SWINBURNE UNIVERSITY OF TECHNOLOGY

SWINBURNE INSTITUTE FOR SOCIAL RESEARCH

Cyber Safety in Remote Aboriginal Communities and Towns

Interim Report

Ellie Rennie, Eleanor Hogan & Indigo Holcombe-James

Swinburne Institute for Social Research,
Swinburne University of Technology

October 2016

The Swinburne Institute for Social Research

The Swinburne Institute for Social Research focuses on some of Australia's most challenging social, economic and environmental problems, including digital inclusion. We collaborate with industry, government and community partners to extend the evidence base, identify solutions to complex problems and contribute to public debate. With expertise in a range of disciplines including economics, statistics, sociology, history, media studies and political science, the Institute is well known for its innovative work on the social aspects of communications and new media.

This report can be downloaded from the APO Digital Inclusion Collection: http://apo.org.au/collections/digital-inclusion.

Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Institute.

Funding acknowledgement

Telstra funded the research discussed in this report as an action within the 'Connection and Capability' priority focus area of their Reconciliation Action Plan 2015–2018. Swinburne University of Technology contributed in-kind researcher time to the project.

Suggested citation (Harvard style)

Rennie, E, Hogan, E & Holcombe-James, I 2016, *Cyber safety in remote Aboriginal communities and towns: interim report*, Swinburne Institute for Social Research, Melbourne.

DOI: 10.4225/50/578432D317752

Contact details

A/Prof Ellie Rennie, Swinburne Institute for Social Research,
erennie@swin.edu.au, @elinorrennie

Copyright

© Swinburne Institute for Social Research 2016

This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License, see http://creativecommons.org/licenses/by-nc/4.0/.

Contents

List of figures and tables ..... **iv**

About the report **1**

Executive summary **2**

Main findings
Additional findings

1. Literature review **5**

Social media use by Indigenous Australians
Cyber safety concerns in remote communities
Violence and Indigenous communities
Responses to cyber safety
Digital inclusion and cyber safety
Conclusion

2. Research approach and participants **12**

Research locations
Reference Group
Fieldwork overview
Participant groups

3. Internet access and use **15**

Tennant Creek and Elliott
Canteen Creek
Benefits of mobile phones
Benefits of social media

4. Trouble online: inappropriate content **19**

Unwanted comments and language
Teasing, bullying and fighting
Sexting, jealousing, cheating and reputation
False profiles and predatory behaviour
Sharing, smashing and stealing devices
Distraction

5. Privacy and financial security **24**

Credit bullying
Locating phones
Hacking phones and social media accounts
AirG VIP charges
Online scams and fraud

6. Digital literacy **27**

Existing digital capability
Setting passcodes and passwords
Blocking and reporting on social media
Photo tagging
Facebook privacy settings
Death and Facebook profiles
Learning digital literacy
Age and gender

7. Responses to cyber safety issues **33**

Police
Schools
Elders and family
Community meetings
Talking to each other
Individual responsibility
Bans
Creative engagement or plain facts?
Responses to educational videos

8. Conclusion **39**

Cyber safety and digital inclusion
Unique cyber safety concerns related to mobile-only users
Cyberbullying
What can be done

Acknowledgements **41**

List of acronyms **42**

References **43**

List of figures and tables

Figure 1: 'Phone mascot' by Beth Sometimes, developed during the Tennant Creek women's workshop 13

Figure 2: Drawing created by participants during the Tennant Creek women's workshop 18

Figure 3: 'Don't be using my phone' by Beth Sometimes, developed during the Tennant Creek women's workshop 22

Figure 4: 'Are you stealing my credit?' by Beth Sometimes, developed during the Tennant Creek women's workshop 24

Figure 5: 'Fubu' by Beth Sometimes, developed during the Tennant Creek women's workshop 30

Figure 6: How do you learn new things online? 31

Table: Knowledge of passcode and password settings, and social media blocking 28

About the report

In September 2015, the Swinburne Institute for Social Research commenced a two-year research project on safety and wellbeing as they relate to communication technologies, in remote Aboriginal communities and towns. This report provides an overview of findings from the first phase of the project. A final report will be available in mid 2017.

Telstra is funding the project as an action within the 'Connection and Capability' priority focus area of its Reconciliation Action Plan 2015–18. The research has been initiated for the benefit of Indigenous people and is being conducted to inform Telstra's strategy regarding cyber safety for this particular consumer group. It is also intended to inform social and community obligations related to Telstra's recent partnership with the Northern Territory Government to extend mobile phone reception to remote areas, including Indigenous communities.

The first, needs-analysis phase of the project, conducted from September 2015 to June 2016, involved seeking feedback on these issues from a cross-section of Northern Territory (NT) Aboriginal people living in a regional centre, a larger community and a smaller settlement, with different histories of exposure to Information and Communication Technology (ICT).

As described in this report, we found that there are particular mobile phone practices and internet uses occurring among remote Aboriginal people in the Northern Territory leading to identifiable cyber safety problems. Some of these practices, and the resulting issues, appear to be different from those experienced by other segments of the Australian population.

Executive summary

Cyber safety encompasses the protection of internet users from online risks and security breaches, including cyberbullying, identity theft, invasion of privacy, harassment, and exposure to offensive, illegal or inappropriate material (ACMA 2010). While the more dramatic and disturbing aspects of cyber safety are often quick to capture public attention, these are symptomatic of a range of issues related to developing online capacities and 'digital citizenship' (GIER 2011, p. 16).

The adoption of Information and Communication Technologies (ICTs) by remote-living Aboriginal people has been recent and rapid in areas where mobile internet is available (Rennie et al. 2016). Some community members, however, see social media as a threat to community authority and stability, and some remote communities have gone so far as to reject the extension of mobile coverage because of cyber safety concerns.

Cyberbullying that breaches cultural protocols between and within family groups, and that inflames existing conflicts has been documented in academic studies and government reports (AHRC 2011; CLC 2012; Hogan 2014; Hogan et al. 2013; Iten 2014; Kral 2014; Shaw & d'Abbs 2011; Vaarzon-Morel 2014). We know from these reports that middle-aged and older remote Aboriginal people often find cyberbullying distressing and difficult to address. While cyberbullying, in any context, originates from the broader domain of social interaction, remote Indigenous contexts possess unique cultural attributes, alongside geographical isolation, and income and education-related factors, that need to be taken into account in addressing cyber safety.

Main findings

Our research suggests that there are particular mobile phone practices and internet uses among remote Aboriginal people in the Northern Territory that are leading to identifiable cyber safety problems. Some of these practices, and the resulting issues, appear to be different from those experienced by other segments of the Australian population.

Significant aspects of this internet use include:

- Internet access is predominantly mobile-only.
- There is a high level of sharing of devices.
- Prepaid mobile broadband is preferred.
- Facebook and AirG/Divas Chat dominate social media use.

The main cyber safety issues emerging from the research can be grouped into three categories: inappropriate content and comments, privacy issues, and financial security and management.

Inappropriate content and comments

The most frequently reported cyber safety problems include inappropriate images (known as 'noodz' and 'top shots' locally), and abusive or offensive comments and messages ('trash talk'). This activity is occurring on social media platforms Facebook and AirG/Divas Chat, as well as through texting. Inappropriate or offensive use includes swearing, teasing and bullying, which can incite further arguments and fighting offline, particularly when they tie in with existing tension or hostility. The filming of offline fights, which are then shared online, falls within this category.

Participants highlight problems associated with revealing photos, which go against cultural protocols. Some speak of social media being used to make false insinuations about other people's sexual reputation and to cheat on partners. Young women are aware of how false profiles can be created and used for predatory purposes by people they do not know 'in town and out of town'.

Privacy issues

The sharing of devices (sometimes without permission) can lead to privacy issues if social media accounts are not password-protected. 'Hacking' is the local colloquial word for using others' social media accounts or creating false profiles. Many participants do not know, or are unaware of, how to set passcodes and passwords to prevent others from using their social media accounts.

Although sharing devices among kin can have positive outcomes, some women say that they have a second, 'secret' phone that they keep hidden (e.g. under their clothes) for their own use so that others cannot take it. Managing access to phones and accounts can be complicated by Aboriginal family relationships.

Financial security and management

Financial security issues, such as identifying scams and fraud, and managing credit and finances, appear to be significant. 'Credit bullying' occurs when people (usually family members) transfer credit from others' prepaid accounts. Women highlight credit theft as a particularly vexatious issue, especially on unpasscoded phones or when family members have shared passwords.

Another problem involving the sharing of mobile phones is the need to shut down accounts (e.g. banking, Telstra, social media) if a phone is not passcode-protected and goes missing, or is with someone the owner knows but cannot locate. People are unlikely to know about or to access apps like Find My iPhone. These apps require the user to have access to another device, which Aboriginal people living in remote communities and towns are unlikely to own.

Some are using AirG/Divas Chat when their credit has expired and they can no longer access Facebook (AirG is a subscription service based in Canada, which offers access to chat products that can be found via the Telstra Media Mobile Portal). There is a widespread misperception that AirG VIP is free (it is, in fact, charged at 95 cents per day), most likely because there is a 15-day grace period after credit runs out where users can still access AirG before their account is automatically unsubscribed.

Additional findings

Overall digital and cyber safety awareness

People's level of digital capability and cyber safety awareness generally corresponds to the length of time they have had access to the internet, particularly to mobile coverage. There are differences in awareness between age and gender groups, suggesting the need for different approaches and resources for these groups.

Women: Women mostly identify cyber safety as significant, perhaps because 'safety' is (problematically) an issue where they typically exercise greater leadership than men do. Women may also have greater digital capability because of their use of ICT to maintain

family connections and to manage households: women tend to manage BasicsCards, bank accounts, shopping and food. Nevertheless, middle-aged women's digital literacy is probably lower than that of women of similar age (i.e. 35+ years) in non-Indigenous and/or urban populations, and probably similar to that of older women in non-Indigenous and/or urban populations.

Men: Older male participants are less likely to be engaged with cyber safety, and often have lower levels of digital proficiency and cyber safety awareness, compared with women of similar ages. However, young men have a higher level of digital literacy than middle-aged men.

Young people: As among urban, mainstream populations, young people generally display higher levels of digital literacy and are more aware of risks, compared with middle-aged and older people. This indicates that community, school and police programs are successfully conveying information. This is not to say that young people fully avoid these risks, just that they display knowledge.

Managing conflict from online harassment

Some participants prefer to negotiate conflict individually and privately, with other family members and 'cultural way' (according to customary law), before approaching external authorities. Holding community meetings is widely seen as an appropriate forum for providing education and discussing cyber safety issues, or for mediating disputes if families are unable to resolve conflict.

People generally have some knowledge about which external authorities (schoolteachers, police, lawyers, community mediators) to approach and in what situations to approach them about cyber safety issues.

Digital and cyber safety education and training needs

There is a need for straightforward and accessible information, including basic help on using mobile devices and social media accounts.

In particular, people are requesting more information about managing prepaid credit, setting passwords and parental controls, blocking and reporting people on both AirG/Divas Chat and Facebook, and managing privacy settings. Information specific to remote Aboriginal people's cultural issues—such as how to take down a deceased person's Facebook profile—needs to be made readily available. Many desire clear information about AirG VIP's credit and debit arrangements, to counter the widespread misperception that use of this platform is free.

Existing information provided by telecommunications services and social media platforms is often too difficult for remote Indigenous people (particularly middle-aged and older ones) to find or navigate, and a more basic level of English and/or visual mode of delivery is required.

Digital inclusion

Cyber safety has a direct relationship with digital inclusion. Poor understanding of cyber safety, and a lack of mechanisms to address the issues have led some remote communities to reject internet services. However, Aboriginal people, especially within remote areas, experience inequalities and hardships that may be exacerbated if they are not able to access information and services online.

1. Literature review

Cyber safety involves reducing or mitigating social harm related to the use of digital media technologies and applications, including social media. In Australia, cyber safety has been the topic of intense academic and government attention, with significant interventions through the Office of the Children's eSafety Commissioner and the Australian Communications and Media Authority. In mainstream arenas, cyber safety is concerned with the protection of young people, including providing them with sufficient skills to avoid online threats.

A useful summary of the field, produced for the Commissioner for Children and Young People in Western Australia, also emphasises the positive outcomes of social media for young people's wellbeing, recognising that 'digitally mediated mobile, personalised and social communicative practices are now a common feature of everyday life' (Swist et al. 2015; see also Katz et al. 2014; Dooley et al. 2009). Anthony McCosker (2016) observes that the concepts of cyber safety and digital citizenship are centred on social norms and codes, where the role of regulating and managing the digital environment falls to individuals, families and schools.

In this short review of existing literature on the topic, we focus only on cyber safety in remote Aboriginal communities, and consider its relationship to digital inclusion. Very little has been written on cyber safety issues as they are encountered in remote communities. The material that does exist tends to focus on how problems relate to Aboriginal culture and sociality. From these accounts, we know that the kinds of unrest arising through use of social media are challenging established lines of authority in communities, and that cyberbullying is not just experienced by the young, but can also involve adults and families, and occur across multiple communities. There is a possible connection between cyber safety and lateral violence in communities, in that disagreements or accusations that begin on social media can escalate to violent acts before community mediation strategies can be enacted.

As discussed later in this report, some cyber safety issues are the result of particular communication practices in remote communities, including the sharing of devices. Telecommunications infrastructure, products and practices are therefore an important part of the story. We know that Aboriginal people living in remote areas are far more likely to be mobile-only users than other Australians, with respect to not just telephony but also internet use. The preference for mobile devices and mobile broadband services leads to specific cyber safety concerns, as the sharing of mobile phones can have adverse consequences. Moreover, community attempts to manage cyber safety problems can lead to digital exclusion, including restricting access to some services or platforms.

Social media use by Indigenous Australians

The overarching narrative of ICTs in remote Aboriginal communities is one of rapid adoption of social media and mobile devices where there is mobile reception (Brady, Dyson & Asela 2008; Kral 2011, 2014; Rennie et al. 2016). Bronwyn Carlson's work on social media use finds that Facebook has become an everyday, typical activity for Aboriginal people (Carlson 2013; Carlson et al. 2015). Her work is supported by McNair Ingenuity research, released in August 2014, which found that six in ten adult Indigenous Australians used Facebook at the time, compared to 42 per cent of adult Australians nationally. Those

living in the metropolitan areas of the capital cities had the highest use (68 per cent), and those in remote areas the lowest (44 per cent). Even in remote areas, use was slightly above the overall national average (Balogh 2014).

In their meta-analysis of 20 articles, conducted in order to ascertain possibilities for providing health information via social media, Emma Rice and colleagues (2016) found that the literature on social media and Indigenous Australians focuses on four themes. First, social media can be beneficial for *identity expression*, and young Indigenous people are found to be performing their Indigenous identity online (see also Carlson 2013; Lumby 2010). Second, social media also provides a level of perceived *power and control*, in that young people can participate in or create forums and networks that they perceive to be 'theirs', rather than controlled by authority figures or non-Indigenous agents. A related aspect is that social media further enables them to seek out information, on their own terms.

The third theme is *cultural compatibility*, whereby social media's mixed-media forms are better suited to local communication and dialect, by combining text, images, symbols and sounds (see also Kral 2011). Some Facebook pages, such as Warlpiri Chat, are almost exclusively 'in language' (meaning written in an Aboriginal language, Featherstone 2015). Finally, social media is convenient for *maintaining family connections*, particularly with kin who live in other communities or regions. Social media is therefore a site for kinship connectivity and continuity (Lumby 2010).

Cyber safety concerns in remote communities

Research on the negative consequences of social media draws on similar themes. As anthropologist Inge Kral writes, just as the benefits are related to the social and cultural context in which they are embedded, problems are also 'seeded in the norms of the social interactions particular to remote Indigenous sociality' (2014, p. 181). Community concerns arise out of the production and sharing of what is considered to be unregulated content, done without oversight from elders (see also Radoll 2014).

Cyberbullying, jealousing and wrong-way communication

In a survey conducted across six communities as part of her work on cyber safety for the Remote Indigenous Public Internet Access program (Northern Territory, 2010–16), Leyla Iten (2014) found that swearing and arguments were considered the most common problem associated with social media use, accounting for 48 per cent of responses.

Within the 'arguments' category, women in particular identified 'jealousing' to be an issue. Jenny McFarland defines jealousing as actions concerning 'claims or perceived entitlements on relationships between family groups and individuals' (2012, p. 71). Jealousing of this kind is often invoked as a form of provocation in domestic and family violence. She notes that it may also involve rights to country, a car, a house, or other high-status objects. As discussed in this report, jealousing in the form of relationship entitlements can be instigated through online communication (including photographs).

In relation to identity, Petronella Vaarzon-Morel writes that everyday expectations of conforming to and respecting customary law are bypassed through fake profiles; there is a misguided belief that online footprints leave no trace (2014, p. 252). She provides an example from Yuendumu:

> During the period of 'trouble' at Yuendumu, some young Warlpiri created fake identities on Divas Chat to post slanderous messages and spread rumours, denigrating individuals of the opposite faction. Posts concerned allegations of illicit affairs, trumped up 'revelations' about the paternity of particular individuals and descriptions of antisocial behaviours and attributes (Vaarzon-Morel 2014, p. 251).

Perpetrators consider social media to be the arena where they will not be held accountable for their actions. The ability to disregard established lines of authority when communicating on social media appears to be an issue across different regions. Daniel Featherstone observes, in relation to the Ngaanyatjarra and Anangu Pitjantjatjara Yankunytjatjara lands, that elders have expressed concern over 'issues of cyber-bullying, "wrong-way" communication (non-compliance with kinship protocols), and loss of respect for cultural authority as a result of young people's use of ICTs, mobile telephony and social media' (2015, pp. 510–511). 'Wrong-way' communication manifests as flirting and online dating, which becomes problematic within the social order when it goes against kinship-based betrothal demarcations.

Death rites and cyber safety

Customs are challenged not just through overt and hostile posts, but also through the unmanageability of online platforms. In more traditional communities, images of the dead are not circulated and names are not uttered for a certain period. Belongings are thrown away or burnt, and family members will temporarily vacate houses where the dead once lived. In their study of home internet practices, researchers (Rennie et al. 2016) found that social media or applications such as Skype caused distress among some residents as photos and names of deceased family members remained visible on the computer, causing members of the household to stop using the computer until profiles were removed.

While cultural practices are adapting to cope with such online shadows (Kral 2014), stories have emerged of deliberate acts of cultural transgression where profiles of the dead have been created in order to incite or inflame inter-family hostilities. Carlson and colleagues also write of 'RIP trolls', where abusive and racist comments and memes are posted on memorial pages (Carlson et al. 2015, p. 3).

Hate speech

Online hate speech is a serious social harm that is impacting on Aboriginal people. Research into Aboriginal people's use of social media in urban areas has demonstrated that cyberbullying is not just inter-community, it is also intra-community, providing a space 'where Aboriginal people [can] become subject to abuse' (Carlson et al. 2015, p. 3; see also Montgomery 2014). Carlson and colleagues write that although Facebook can be useful in communicating health information, the potential benefits need to be weighed against the challenges, including 'Facebook's potential to contribute to mental ill-health, through facilitating racial abuse and suicide contagion' (2015, p. 11).

A report for the Online Hate Prevention Institute on Aboriginal memes contains an important discussion of the responsibility of platforms in mitigating racism (Oboler 2012). In the case of racist Aboriginal memes, which circulated between June and August 2012,

according to Andre Oboler, Facebook refused to take the images down, determining that they were no more than controversial humour. The report finds that the outcome of such a 'speech rights' decision is that it 'normalises the racist discourse outside of the targeted group and marginalises the victims within society' (Oboler 2012, p. 61). Rice and colleagues write that the 'worldwide application' of social media makes its regulation challenging: 'negative use of social media which undermines identity, control and sense of community and family connection have the potential to be particularly damaging to young people who are already vulnerable' (2016, p. 14).

The responsiveness of platforms in dealing with cyber safety problems in remote communities is an area that warrants further attention. Platforms generally want to avoid becoming what Mike Ananny (2015) has called 'noxious markets'; they attempt to respond to public outrage and repugnance in order to maintain their market. Whether they can know about or deal with issues specific to every cultural group is a significant question.

Violence and Indigenous communities

To date, there has been no in-depth analysis of how violence in communities is related to cyberbullying. However, the types of cyberbullying identified above suggest that social media is a site through which infighting is instigated or exacerbated. It may also be that violence is emerging as a way to resolve disputes that have been initiated through online interactions. As Peter Sutton has observed, in Aboriginal communities conflicts can be a strategy for 'getting subterranean differences out in the open' in order to resolve them (2009, p. 98).

'Lateral violence' is a term used to describe infighting that can take a range of forms, including 'gossip, jealousy, shaming others, verbal and physical attacks, sabotage and bullying' (Clark & Augoustinos 2015, p. 19). Marcia Langton has defined lateral violence as 'the expression of anomie and rage against those who are also victims of vertical violence and entrenched and unequal power relations. Those most at risk of lateral violence in its raw physical form are family members, and in the main, the most vulnerable members of the family: old people, women and children' (2009). Violence in remote communities is generally under-reported (Willis 2011). Even in those incidents that do get reported to police, the role of social media is not necessarily identified, making it impossible to know whether social media is leading to a rise (or otherwise) in lateral violence.

Anthropologists have drawn connections between violence and traditional forms of dispute resolution such as payback (accounts from the 1930s, such as by WEH Stanner, are often cited). Although now worsened by alcohol, 'rates of interpersonal violence were extremely high then also, and marital and sexual relationships and various kinds of jealousies were chief among the prime causes of conflict then as now' (Sutton 2009, p. 99).

McFarland notes that where once payback (including where another family member is 'paid back' in the offender's stead) was supervised and the rules of engagement understood by all, it is now 'far more likely that inappropriate payback will be delivered in an impulsive and opportunistic way, by unauthorised and unsupervised members of the aggrieved family' (2012, p. 81). She further observes that seeing 'culture' as the reason for violence is insufficient, as it is in the places where tradition is most fragile that people are most at risk. The necessary arbitration and resolution is missing in these cases. The relationship of cyber safety to lateral violence is an area that requires further investigation.

Responses to cyber safety

Although social media is a recent and sudden sphere within which established orders are being challenged, it is one part of broader changes to the cultural and social fabric of remote communities. The concerns being voiced are not unlike those expressed during the advent of television (see, for instance, Michaels 1986), which also contained calls for bans and control over communication systems. The difference is that traditionally sanctioned forms of community mediation are struggling to deal with 'wildfires' that are sparked on social media, and that can spread across multiple communities. Local measures, such as community meetings, struggle to deal with fights that occur across multiple places. Kral observes that this is a generational issue, in that the older generation does not have the same technological expertise as the younger:

> Hence, the gerontocratic norms of the past are undergoing a profound disturbance where the patterned habitual practice of elders exercising authority and exerting social control is under challenge. All these factors are coalescing in an environment where the socially sanctioned capacities for conflict resolution are not as evident as they once were (Kral 2014, p. 185).

Vaarzon-Morel writes that some posts are 'directed shamelessly at older people in a clear challenge to authority' (2014, p. 251), provoking anger that can lead to social disruption. She gives the example of conflicts in Yuendumu spreading to Alice Springs through use of mobile phones: 'Whereas older people previously used space between people to defuse conflict, in these examples young people use the mobile phone to reduce space and intensify conflict' (2014, p. 250). Such fights have led more senior residents to call for a ban of social media sites such as AirG/Divas Chat and Facebook.

A Commonwealth inquiry into cyber safety in remote communities concluded that while there are 'protective mechanisms' within Indigenous culture, 'the rollout of new services into remote areas could exacerbate intercommunity conflict while diminishing community capacity to manage such developments' (Joint Select Committee on Cyber-Safety 2013, p. 51).

In her survey of social media and cyber safety, Iten found that night patrols and family or community meetings were viewed as the most appropriate responses to cyberbullying (42 per cent of responses). Women were more likely than men to seek help from police. She notes that in Yuelamu, night patrol was active at the time of the survey, and it was seen as a legitimate mediator in cyber safety in that community. She writes:

> Families in Haasts Bluff expressed that sometimes they will wake up in the morning to be made aware of a fight that started the night previous. The role of night patrol in responding to cyber safety concerns, and understanding how night patrol teams may diffuse and mediate local conflict arising from online communication is worth investigating in order to develop an effective response within their role (Iten 2014, p. 15).

In Tennant Creek, the Council of Elders and Respected Persons (CERP) initiated a 'Divas Cops' program, whereby anonymous people monitored and reported inappropriate behaviour in AirG forums. CERP's intention was for elders to intervene (including banishing individuals from the community for a time), but its program was defunded (Hogan 2014).

A further consequence of cyber safety problems is that some communities have rejected mobile phone infrastructure when the opportunity arose (Radoll 2014), while others are implementing wi-fi networks that can be turned off when problems arise, and blocking social media sites (McFarland & Iten 2016). These should be considered attempts to

reinstitute established lines of authority and mediation. We intend to investigate mediation and other community attempts at cyber safety in our next report.

Digital inclusion and cyber safety

The relationship of cyber safety to digital inclusion is multifaceted. Attempts to deal with social problems arising from the use of ICTs, such as refusing infrastructure or filtering out social networking sites, have a clear impact on digital inclusion, in that the benefits of connectivity are forsaken in order to maintain stability. Wrongdoers are chastised at the expense of all.

At the same time, existing digital inequality may have a systemic relationship to cyber safety, given that the communication ecology of remote communities is limited compared to what other Australian households experience. As discussed in later sections of this report, the way in which people are accessing the internet, combined with particular communication practices, can make individuals more vulnerable to identity theft, privacy breaches and financial hardship arising from telecommunications use.

The high numbers of mobile-only users in remote communities has been attributed to a range of factors, including difficulties in establishing home satellite services, the mobility of Aboriginal families, and the convenience of prepaid plans. The Home Internet in Remote Indigenous Communities project (Rennie et al. 2016) found that the high rates of mobile adoption stemmed from the fact that other services were not meeting the basic needs of remote Aboriginal households, particularly in relation to payment systems, but also regarding installation and subscription processes. If there is no mobile coverage in their home community, rather than accepting the second-best option (satellite internet), residents are instead choosing to go without.

In addition, while households may implement systems for ensuring that home computers are generally not shared beyond immediate household members and close kin, mobile devices can be more difficult to manage, and present particular problems in relation to affordability and privacy. The sharing of devices is likely related to a distinct system of exchange that has carried through from pre-settler times, known as demand sharing (Rennie et al. 2016).

As Jonathan Donner points out, mobile devices have evolved to ‘serve different markets, needs, and use cases’. They include ‘design choices and infrastructure investments created and deployed by technology industries, and influenced by both policymakers and users themselves’ (Donner 2015, p. 61). In remote Aboriginal communities, these design configurations—centred on individual use and portability—will not necessarily play out as originally intended, and the conveniences often associated with mobile devices can become problematic for some people. Digital inclusion thus needs to be considered as part of interrelated consumption patterns, and commercial platform imperatives and products, as well as social practices. Technical advances that enable people to keep their phones and credit safe are a clear area for further research.

Conclusion

Existing studies of cyber safety in remote communities depict some unique issues in addition to those typically associated with other segments of the population (such as offensive language and images). Some of these issues relate to particular dimensions of Aboriginal sociality, including deliberate acts to undermine authority, and crossing into

zones of communication that are considered taboo. Older generations in some communities are struggling to exert authority over social media communication channels. Other communities are taking control in ways that may have adverse consequences for digital inclusion, including refusing communications infrastructure.

2. Research approach and participants

This report covers the first phase of the research, which involved a needs analysis of current awareness and experience of cyber safety issues and strategies at three central Australian sites—Tennant Creek, Elliott and Canteen Creek—from September 2015 to June 2016. These locations were chosen to provide a cross-section of remote central Australian localities—a regional centre, a larger community and a smaller community—with significant Aboriginal populations, varying degrees of remoteness and different histories of internet access.

The rationale behind this approach was to examine the dimensions of cyber safety issues in a sample of remote locations with varying exposure to or no access to mobile coverage, because of the particular cyber safety concerns associated with mobile connectivity. We also wished to explore the relationship between people's history of internet access, level of digital literacy and capacity to deal with cyber safety issues.

Research locations

Tennant Creek is a town of 3000 people, approximately 50 per cent of whom are Aboriginal, and is located some 600 kilometres north of Alice Springs. **Elliott** is a community of 650 people, over half of whom are Indigenous, 750 kilometres north of Alice Springs. Both of these locations are on the Stuart Highway and have had internet access and mobile coverage for almost a decade. Aboriginal groups in both locations have addressed complaints of cyberbullying and related offline conflict in reference to mobile phone technology and social media use, particularly the AirG platform, also known as 'Divas Chat'.

By contrast, **Canteen Creek/Owairtilla** is a small remote community with 180 Indigenous people, 576 kilometres north-east of Alice Springs, 180 kilometres of which is 'off the bitumen', with no mobile coverage and only satellite internet access.

Identifying the communities that might wish to participate in the project, and securing their consent, was a complex process in which we relied on Aboriginal organisations to raise the prospect with community members (see 'Acknowledgements'). We also sought the involvement and advice of government agencies and local community service providers on the project's Reference Group.

Reference Group

The Reference Group consists of representatives from the following organisations: Australian Communications Consumer Action Network (ACCAN); Barkly Regional Arts; Central Australian Aboriginal Legal Aid Service (CAALAS); Central Australian Youth Link Up Service (CAYLUS); Office of the Children's eSafety Commissioner; Indigenous Remote Communications Association (IRCA); NT Community Justice Centre; NT Legal Aid Commission; Red Cross Youth Leadership Group; Papulu Apparr-Kari Language Centre; and Piliyintinji-ki Stronger Families.

The Reference Group is providing overall direction for the project, as well as feedback on the development of research methodology and delivery, and on project outputs such as reports. It also provides a forum for sharing information about relevant policy developments and current cyber safety challenges. The Reference Group plays an important role in

ensuring that the research project is conducted in ways that are ethical and culturally appropriate, particularly concerning cultural protocols relating to remote Aboriginal families and communities, and any potentially sensitive local issues. The initial stages of the project included consultations with a range of individual stakeholders, including some on the Reference Group, listed in Appendix 4 (see the separate Appendices document).

Fieldwork overview

The research design is centred on the principle that the research process should be of benefit to the participants. To achieve this, we developed cyber safety information-sharing workshops, which were intended as a dialogue between the project team (Swinburne and Telstra) and the participants (including the organisations that have facilitated participants' involvement).

For the Tennant Creek component of the research, we worked with Piliyintinji-ki Stronger Families, which provides culturally appropriate services designed to improve the physical, social and emotional health and wellbeing of men, women and children in Tennant Creek; Tennant Creek High School; and Barkly Regional Arts. Workshops took place in Tennant Creek from 21 to 24 March 2016 with Piliyintinji-ki Stronger Families men's and women's groups, and two workshops of boys and girls at Tennant Creek High School, selected by the principal.

From 30 May to 3 June, we held men's and women's workshops in Elliott and a women's workshop in Canteen Creek (men were invited but did not attend). We did not invite young people to participate at these locations.

Figure 1: 'Phone mascot' by Beth Sometimes, developed during the Tennant Creek women's workshop.

The workshop facilitation was adaptive, in that content was changed according to the needs of participants. For instance, the workshops at Stronger Families incorporated privacy-setting information, as participants indicated that this was important to them.

To date, the workshops have been the primary source of information-gathering, and participants have seemed most comfortable sharing their concerns in a group setting. Participants were also given the opportunity to speak one-on-one with a researcher to share concerns or stories privately. A total of 23 structured interviews took place during the fieldwork at Tennant Creek and Elliott in March and May 2016; they were not conducted at Canteen Creek owing to time constraints.

In both the workshops and the one-on-one interviews, participants were informed that they should keep stories generalised and not use names, for ethical and legal reasons. In the interviews, we encouraged people to talk about problems that other people had encountered, rather than their own, as direct questioning can lead to feelings of 'shame' and shut down conversation. We have provided additional quotes by topic in Appendix 3 (see the separate Appendices document).

Participant groups

The Tennant Creek and Elliott fieldwork consisted of separate workshops for men and women because of the sensitive nature of the issues, as well as cultural protocols requiring the genders to congregate separately. Although Tennant Creek High School did not see a particular need for gender division, we chose to speak to the girls and boys separately. Because the boys were only able to participate in one workshop session (owing to football commitments), most of our initial data collection related to the social media practices and concerns of girls. However, the final workshop with the boys at Tennant Creek, and the Elliott men's workshop, in which participants' ages ranged from 18 to 35 years, indicated that young men are using social media in similar ways to young women. We have therefore treated 'young people' as one group for the purposes of this report.

We encountered significant differences in attitudes to cyber safety between the three groups. These differences are important in our analysis of the evidence to date.

Women

Women were mixed users of social media. They were interested in safety generally, with concerns ranging from communication in emergency situations to young people's safety online and community cohesion. Women were facing financial pressure and experiencing cyber safety problems as a result of sharing practices.

Men

Men were not significant users of social media. They used mobile phones mostly for calls to family, friends and service providers. The general attitude among men was that problems are of a 'private' nature and should be dealt with accordingly.

Young people

Young people were high users of social media. While young people presented themselves as experts on cyber safety, and were seemingly across available tools and information, they also encountered some serious cyber safety problems.

Further information on the interviews, including demographics, is given in Appendix 1 (see the separate Appendices document).

3. Internet access and use

> We didn't have any mobile phones when we were growing up. We used public pay phones to communicate between communities, and we would ask whoever answered the pay phone to pass on a message to somebody else in that community. We would also pass on messages if we ran into people in town …
>
> The way that we communicated as young children has totally changed to how young children communicate now. We used to approach people in person, walk over to where they were or look around for them. Now most young people use mobile phones instead.
>
> —Elliott men's group participants

Patterns of internet access, device ownership and payment methods in the research sites corresponded with findings of surveys conducted in Ali Curung in 2013 (Rennie et al. 2016) and by Leyla Iten as part of her work for the Remote Indigenous Public Internet Access program (Iten 2014). Both of these studies recognise that internet access and use varies across communities, and is dependent on infrastructure and related internet retail products.

Tennant Creek and Elliott

Four significant aspects of internet use emerged during the Tennant Creek and Elliott field trips:

- Internet access is predominantly mobile-only.
- There is a high level of sharing of devices.
- Prepaid mobile broadband is preferred.
- Facebook and AirG/Divas Chat dominate social media use.

In interviews, a very high proportion of people who were using the internet said that they used mobile phones to access the internet, and almost half had access to tablet devices. Of those accessing the internet, four in ten people had access to a laptop and two in ten to a desktop. Most were accessing the internet from Next G mobile connections, and some were using a Centrelink computer to access Centrelink services. Only one person reported that they had a satellite internet connection.

Most people used their own device to access the internet, but two-thirds said that they also used someone else's mobile device. When asked if they sometimes let other people use their mobile device, almost three-quarters said that they sometimes let other people use it and only a handful of people reported being the sole user. People described sharing devices most often with family and friends, with a slight bias towards family. The sharing of devices is important in terms of cyber safety problems such as identity theft and 'credit bullying', as discussed below.

Prepaid internet was overwhelmingly the preferred means of payment. Many people we spoke to were not aware that AirG VIP debits a subscription from their account (see '5. Privacy and financial security').

In Tennant Creek and Elliott, around three-quarters of people we spoke to used Facebook. Although people confirmed that AirG/Divas Chat was in use, those in Tennant Creek stated that it was in much greater use among people from remote communities. Some people seemed reluctant to declare that they used AirG/Divas Chat, possibly because it is associated with online dating outside of culturally acceptable arrangements (see '4. Trouble online: inappropriate content'). Other platforms in use included Instagram, Snapchat, Twitter and Messenger, but all at much lower levels. Further details of access in Tennant Creek and Elliott is provided in Appendix 2 (see the separate Appendices document).

Canteen Creek

A different situation existed at Canteen Creek, which did not have mobile broadband, only wi-fi supported by satellite. Wi-fi access was available at the school (with certain sites, including Facebook, blocked) and at the Council office (which includes a public Centrelink terminal). Some households had internet access, and their own laptops or desktop computers, although they reported that speeds were slow. Most people in the community had mobile phones (the local store sold them), which they used when in range. One workshop participant commented, 'Everyone likes to have their own phone so they can access stuff and be more mobile.'

However, the CEO of Canteen Creek Owairtilla Aboriginal Corporation said the community had raised the prospect of getting mobile coverage within the last year because of safety concerns. In the workshop, participants said that the public phones in the community were unreliable: they often didn't work in the wet season; they got damaged; it was sometimes hard to hear the person on the other end; and someone had to search for the person in the community the call was for. Telecommunications access was even worse at outlying outstations that the Owairtilla Aboriginal Corporation oversaw. The CEO said:

> Hatches Creek [80 kilometres from Canteen Creek on unsealed roads] years ago got a public phone, but it needs fixing as sometimes you can ring out and sometimes you cannot. This is urgent, as during wet season we have no communication other than the public phone …
>
> At Kalapitapita [130 kilometres from Canteen Creek on unsealed roads], there are young children and families living there, no communication at all. Come wet season, they are cut off, and if there are any accidents or emergencies, we have no way of helping these people. It is really a huge problem.

In the workshop, participants seemed divided about mobile access—'There is a good side of this and there's also a bad side of it.' But they acknowledged that it could assist with safety and was becoming unavoidable in dealing with online services, such as in the need for SMS code verification to access myGov.

The Canteen Creek Owairtilla Aboriginal Corporation originally refused the extension of coverage because they feared it would be accompanied by problems such as cyberbullying, which had been reported in other locations with mobile access. The community sought to reduce the catalysts for local 'trouble' (e.g. fighting), and had implemented their own prohibitions on alcohol and pornography prior to the Northern Territory Intervention. Participants said that 'cyberbullying is one of the main reasons' for not wanting mobile access. One participant commented, 'People are worried that the internet could make it [trouble] worse. Kids do fight and they will start bullying each other online.' There were rumours that kids were accessing sites such as Divas Chat on some community members' (presumably unprotected) wi-fi or via the mobile signal from Epenarra

at a location 30 kilometres out of the community. However, the CEO said there had not been any fights (cyber-related or otherwise) within the community in the last two years.

Participants said that members of the community used Facebook, which, like participants elsewhere, they saw as being more benign than AirG/Divas Chat—'Other chatlines, that's where the cyberbullying is. Especially AirG.' They mentioned AirG specifically in relation to an incident in Tennant Creek:

> People don't really seem to use AirG here. But when they go to Tennant Creek they do. There was a fight last year, and it wasn't sorted out properly—the parents didn't stop the kids and they didn't have a meeting and come together to stop their kids from fighting. When they went to Tennant Creek they started teasing each other over the chatline.

While some individuals felt that mobile access could be beneficial for Canteen Creek, they felt that 'to move forward the community needs to have the final say' in a forum such as a community meeting:

> I don't disagree about mobile coverage, but I think that before we get it, I think we need to come together as a community and talk about it. And then, have something like this [a *Be deadly online* video] to screen publicly. Have a BBQ or something and then talk about it. Ask the community first, so the community can have the final say. It all comes back to the community. A few people have said that it's a good idea to have coverage, but if everyone comes together then we can get the final answer. We can't just make decisions if our people don't agree.

Benefits of mobile phones

Discussion of the benefits of mobile phones revolved around themes of safety and wellbeing. Participants mentioned the use of mobiles in maintaining connections with family and friends. Participants also described mobile phones as useful for phone and Centrelink banking, looking for jobs, and checking weather and sports scores. Entertainment uses, including playing games, watching videos, listening to music, gambling, and having a camera and a voice recorder were all listed as benefits.

The Tennant Creek men's group said that after accessing YouTube, they used mobile phones mainly for Facebook and calling friends. Participants had heard of, and used, AirG/Divas Chat. While they said they used mobile phones mainly for voice calling (family, friends, Centrelink, doctors and other providers), they mentioned texting when they'd run out of credit, which implies the use of AirG.

Benefits of social media

At Tennant Creek, women identified the main benefit of social media as keeping in touch with friends and family, which was highly valued: 'Sometimes it's good to go on a chatline, to see that person you haven't seen for a while.' One woman said she used Facebook to keep in contact with her sister in Adelaide. In the young people's group, one girl said that she used Facebook to stay in touch with her father in Nhulunbuy.

One woman saw Facebook as a place for expressing your feelings as well as connecting with others: 'Some people need to talk about their feelings on Facebook. I talk about how I feel on Facebook.' Being able to make contact when a car has broken down was raised a number of times, with participants emphasising that sometimes people will need to walk all night if stranded.

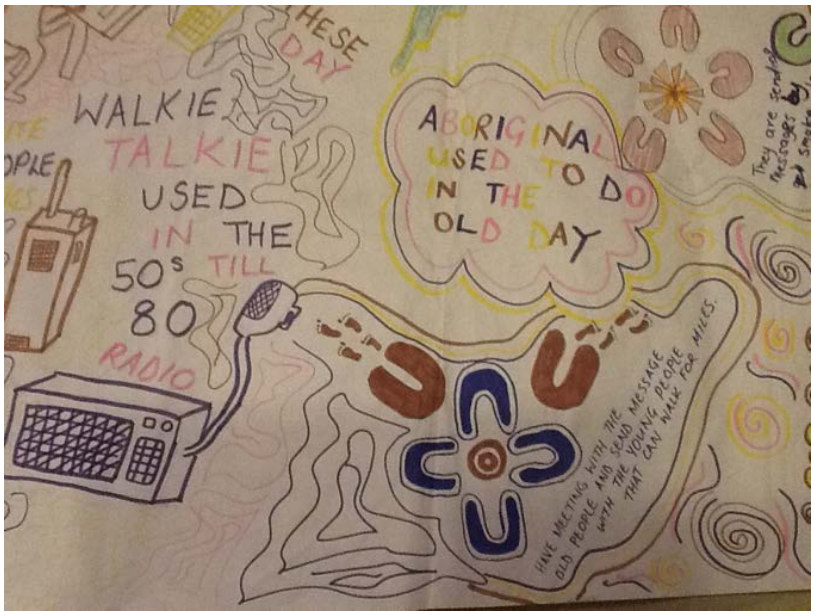

Figure 2: Drawing created by participants during the Tennant Creek women's workshop.

For Aboriginal people living in a remote town such as Tennant Creek, social networking can go beyond socialising into important instances of reconnection. Occasionally, social media is a means for families who have been through enforced or extreme separation to find each other: 'family keeping in contact with children who had been removed from their mothers' was described as one of Facebook's benefits. A woman told a researcher how Facebook had been used to reunite some children who had been removed from their families with family members, although it was too late for them to meet their mother:

> Her nieces and nephews were reunited with her via Facebook. Their father took them away when they were young to South America. The family didn't know where they were. The kids searched for their relative on Facebook and traced them to Tennant Creek. When they made contact, they found that their mother had been killed in a hit and run accident outside one of the town camps only recently.

As the next sections discuss, the benefits of internet access, mobile phones and social media often stem from similar behaviours and uses as do problems online. For instance, some see sharing devices as important for safety, but this practice can also lead to financial abuse such as stealing credit.

4. Trouble online: inappropriate content

> It was better before, when people used pay phones—there is a lot of trouble now on social media.
>
> —Tennant Creek women's group participant

While earlier reports described remote Aboriginal people in central Australia, including Tennant Creek, as being baffled by trouble online (AHRC 2011; CLC 2012; Hogan, Gregory & Thomas 2012; Hogan et al. 2013), most research participants in this study displayed some understanding of what cyber safety issues were and how they occurred.

In response to an interview question asking whether they'd heard of problems caused by people using social media, 32 per cent of respondents (seven out of the 22 asked this question) said 'often', 41 per cent (nine) said 'sometimes', and 23 per cent (five) said 'not at all'. Sixty per cent of people said they worried about other people using social media; 40 per cent said they did not. In discussing what was bad about using social media, only 19 per cent of people asked said that nothing was wrong. One qualified her comments, saying, 'It's not really bad—people have to learn it properly, not silly way, and become responsible and careful of who they have contact with.'

Women and young people had more observations to offer about cyber safety than the men had, probably because of their greater experience of using mobile phones and social media, and consequently higher degree of digital literacy. Some of the men conveyed a sense that they 'heard' cyber safety as a women's issue, perhaps under the general rubric of community safety. Such a correlation would not be surprising, given that Aboriginal women have been highly involved in community safety issues in central Australia over the past few decades, advocating for a greater police presence on the Anangu Pitjantjatjara Yankunytjatjara lands and for an end to family violence (HREOC 2003; McGlade 2012, pp. 97–102; see also Langton 2009). However, any identification of cyber safety as a women's issue puts them in the problematic position of assuming responsibility for managing any negative impacts from other people's behaviour online in the community at large.

The problems most associated with cyber safety were:

- inappropriate content (discussed in this section)
- privacy issues (discussed in '5. Privacy and financial security')
- financial security and management (discussed in '5. Privacy and financial security').

This reflects experience in the mainstream (see, for example, Green et al. 2011, pp. 31–38).

Unwanted comments and language

Receiving unwanted Facebook status updates is not confined to remote Aboriginal populations and often not more than an irritation. However, hostility being expressed through swearing in language was raised as a serious issue. Some male participants said that they had seen swearing in Aboriginal language on AirG, which was problematic as it

was more powerful than using English. Young people sometimes used 'code'—for example, texting language—so older people wouldn't know what they were talking about. One young woman commented, 'AirG does monitor swear words, but people spell their swear words differently so it can get approved [e.g. "fhuk", "fhuka"]. Some use Indigenous language to get it on there. They just go to another level of swearing words.'

One man took himself off Facebook because of the verbal abuse he saw happening there. He considered his family's safety in choosing to withdraw from Facebook. He worried about family photos being put up there: 'Who else is looking at them?' He now just uses telephone calls, face-to-face communication and text messages. Another participant said he was still on Facebook but does not get involved in the arguments people have on there. He blocks people and deletes comments where necessary, to keep himself safe and out of trouble.

Teasing, bullying and fighting

Participants highlighted teasing, bullying and fighting as negative social behaviours, especially in reference to young people. One woman complained about the capacity of social media to magnify gossip and abuse, observing: 'Everybody sees what is being said about people, whether it's true or not.' Some online fighting was becoming more covert: 'Fighting is less on the newsfeed and more in an inbox—private messages—so no-one sees who started it.' However, online fights can spread beyond individuals to the group if not managed.

When the concept of being safe online was introduced in one men's group, participants first spoke about fights featuring Indigenous people being available to view on YouTube. The young men also mentioned the use of social media to organise fights, which were filmed and then uploaded to Facebook: 'People fighting, bullying, teasing, filming and putting up fights online, swearing, dirty words.'

The men said that these fights, which were organised online and offline, were filmed by fellow Aboriginal people. It wasn't clear from participants what the fights were about, and participants did not say anything about wanting to have content removed from YouTube. They said it was 'just fighting' and did not appear overly concerned about the videos or say anything more about this topic.

Sexting, jealousing, cheating and reputation

People described how negative behaviours and outcomes were associated with posting 'rude photos' ('noodz', 'top shots', 'boob shots') and sexual comments (sexting):

> Some girls are taking top shots—cleavage. We know this because they're using them as their profile photos. They're revealing more than what we're meant to do in our culture. We weren't allowed to do that when we were small or a teenager. It's not always public—they are in the bathrooms, and posting photos of kissing their boyfriends.

> Naked photos are a real issue. Very common for teenage girls or boys to post stuff like they are models, you know, like celebrity models. Some wear bikinis, or act like they're porn stars. I have no idea why they do that … maybe to get attention or to get a boy they like. It's like they are making themselves cheaper. Boys would take photos with their tops off, which is kind of okay but not really.

Reputation in a small town was raised as an issue: 'Small town—everyone knows each other, workplace, nurses, child protection, etc.' The potential to slur someone's reputation, even a baby's, was described:

> A teenager has a child, and another one talks [negatively] about that child. How are you going to feel when they are talking about your child as a mother? That's bullying. Judging on who is the kid's dad, who they have been sleeping with. That hurts—only the woman needs to know that.

In Elliott, the men's group said that in a small community such as theirs, people 'would not risk sending naked photos because they would be too scared about everybody seeing them'.

Women discussed a range of problems that could emerge, such as rumours and false insinuations (known as 'jealousing') about other people's sexual behaviour, particularly on social media platforms, and also texting, sometimes leading to fighting:

> Bullying, rumours, if someone takes a photo and they judge it in a different way (misinterpreting photos), if you are sitting with a girl and they will say you are lesbians, or if you are sitting with someone's husband and they will think they are together, causing jealousy.

Participants specifically mentioned Divas Chat as causing problems 'in a wrong way, like swearing, jealousing, fighting in bad way, teasing and cheating on each other'. One woman described how people used Divas Chat to create false profiles and to cheat on their partners: 'Married men going into Divas Chat, texting people. Block them—some I do. Acting like single men but I know these people. Only single men can chat with me.'

While these issues are similar to those that mainstream populations experience through social media use, what was of particular concern was how some people employed AirG to have 'long distance relationships', or more local ones, with people they were not meant to, 'skin-ways': that was eroding traditional protocols for relationships according to specific family affiliations:

> Everyone is connected here … that's why AirG is an issue because they make wrong skin marriages. A person can be your brother here but then on AirG, you can text them like they are your lover.

Participants often perceived Facebook as more benign than AirG, possibly because its focus on 'friends' rather than dating suggests mapping friendship and family networks (to some extent publicly, depending on users' knowledge of privacy settings). For example, participants commented that 'Facebook is okay' and 'Facebook is safer because parents can see what their kids are doing. AirG is more dangerous—it's not real people.' In one discussion group, everyone agreed when a participant commented, 'Other chatlines, that's where the cyberbullying is. Especially AirG.'

However, others observed the use of Facebook to cause problems between partners, and even marriage break ups:

> For example, if a wife logs into the husband's phone and sees that he has connected with other women and she will think, 'What the hell?' Ex-partners can also be lurking about on social media, which can cause problems in marriages.

Another young woman described how her ex-partner harassed her on Facebook, then through texting, to the extent that she bought a new phone:

> I broke up with my ex, and then he was posting stuff about me on Facebook, and I didn't like it, so I blocked and deleted him but he would just keep harassing me by texting me, so I smashed my phone and went to a cheaper phone. I got a new number as well so he can't contact me.

Mobile phones were sometimes used to make 'abusive calls' and, as in the mainstream population, breaking up by mobile was seen as problematic: 'Break-up via mobile not face-to-face which is still a form of bullying. Don't have to face each other.'

False profiles and predatory behaviour

Participants described how some people created false profiles on social media or used someone else's profile to tease others or pick fights, or to make insinuations on dating platforms such as Divas Chat about other people's sexual behaviour (see above).

People also reported the use of fake IDs, where someone finds out another person's password and then logs into their account or phone and sends messages pretending to be that person. For example, boys might use a fake ID when threatening to fight somebody, to cause trouble between two people. Sometimes people find out other people's online banking passwords, too (see '5. Privacy and financial security').

Figure 3: 'Don't be using my phone' by Beth Sometimes, developed during the Tennant Creek women's workshop.

The female high school students were aware of the creation of false profiles, the possibility of 'people talking to you, pretending to be someone else', and the potential to be groomed online by 'paedophiles and child molesters' (information they'd probably received at school). They independently raised the issue of being contacted online by people 'in town and out of town' and said 'men from other countries—maybe get in touch with people in Tennant Creek'. They also described men coming through Tennant Creek, getting in touch with young girls online (it wasn't clear on which platform) and girls having sex in exchange for money, alcohol and drugs. Community workers told similar stories to the researchers in Tennant Creek in 2012, although they named Divas Chat as the platform involved (Hogan, Gregory & Thomas 2012; Hogan 2014).

Some women commented: 'More people are meeting online but what if it's not the person you think it is?' And: 'There are big men preying on young ones, even boys, on the internet. We really need to make sure that our pages are closed and they don't talk to strangers.' One woman found out how to lock her Facebook down so only people she knows can be

added, and she can't get messages from people who aren't her friends. Another said that her 15-year-old daughter had received two messages from men. She observed that dealing with unwelcome contact was difficult for people without the education to do so, and for parents and daughters who did not have a strong relationship:

> I know how to block them; she doesn't. Because we have a good relationship, she told me that we could do it together but if we didn't … what about parents who don't have that relationship, how do they deal with that? They don't know about it and have no education about it. These parents are not educated as much in English and that is an issue.

Sharing, smashing and stealing devices

High school students reported that people sometimes smashed phones because of jealousy. One said that her father used Facebook on the computer because his phone had been smashed. This story corroborates what the school principal had told a researcher earlier: that she used Facebook rather than texting to contact parents and guardians, because phones were often damaged and people could pick up Facebook wherever they had internet access. One middle-aged woman said that she had had five phones: three were taken from her and two she smashed deliberately because people were asking for them.

The swapping, sharing and stealing of mobile phones and other ICT items, especially SIM cards, was flagged as an issue:

> Problems—sometime people sharing, family members—swap the battery, SIM card, memory card. Even earphones. When they see good music, they want to take it.

> Teenagers steal phones and use it to call people, and then the owners get the phone back and they continue getting calls from people and they have to say 'sorry wrong number'!

Some women said that they had a second, 'secret' phone that they kept hidden (e.g. under their clothes) for their own use so that others couldn't take it. One older woman said that she and her husband slept with their phones under their pillows, but other people still took their phones and used them.

Distraction

Distraction—either by inappropriate content or from spending long periods online—was also flagged as an issue. For example, one girl said her parents hated how she was often up late on social media. An older woman commented that she often 'has to tap the table to get kids' attention because they're looking at the phone rather than yarning. You see people in circles all staring at their phone when they would have been yarning before.'

5. Privacy and financial security

> When you're busy, they get your phone and sneak through it—transferring credit from your phone.
>
> —Tennant Creek women's group participant

Privacy concerns, such as the hacking of other people's phones and social media accounts, and the sharing of devices and credit (often without permission), emerged as significant issues for managing ICT use, especially in reference to Aboriginal family relationships. Financial security and management—such as identifying scams and fraud, and managing credit—were also of concern.

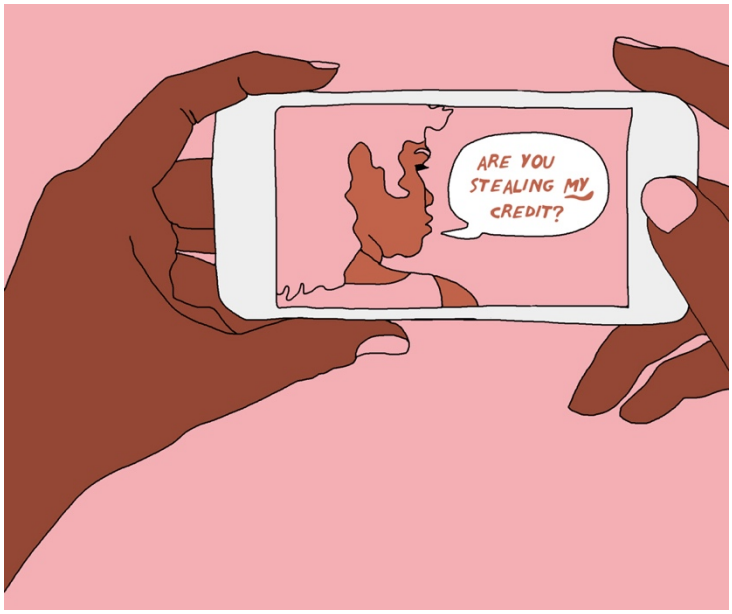

Figure 4: 'Are you stealing my credit?' by Beth Sometimes, developed during the Tennant Creek women's workshop.

Credit bullying

Participants reported that family members transferring credit from prepaid accounts was a particular problem. This happened on unpasscoded phones or when family had shared passcodes. Transferring credit from one prepaid phone to another is relatively simple and has positive uses, such as helping out a friend, or topping up family members' credit when needed. However, this was not always done with the owner's knowledge or consent. The variety of mobile phones, with different methods of setting passcodes on each model, was often an obstacle in this regard (see '6. Digital literacy').

Locating phones

Another problem participants raised with sharing mobile phones was the need to shut down accounts (e.g. banking, Telstra, social media) if their phone was not passcode-protected

and went missing or was with someone they knew but couldn't locate. This can happen on a regular basis when phones are shared and borrowed frequently.

When asked what they would do if they lost their phone, the Elliott men's group said they would buy another phone. One participant responded in detail:

> I would call Telstra and have my number cancelled. I would call Telstra and ask them to track my phone. I wouldn't want anyone else to be using my bank details or accessing my private personal information. We all know how to set passwords on our phones.

People were unlikely to know about or to access apps like Find My iPhone. These apps require you to have access to another device, as well as a Google account or Apple ID. Many people in remote communities do not have easy access to a second device (or personal computer), and workshop participants were generally not aware that they would require an account to trace devices through the Android and iOS platforms.

Hacking phones and social media accounts

The use of other people's phones and social media accounts was identified as a significant security issue, often in relation to the creation of false profiles:

> I wouldn't do internet banking because people can hack in, use your information or ask you for it.

> Hacking is when using someone else's phone or making up false profiles. [It includes] stealing pictures from profiles and commenting or making new profiles with them.

One woman told a story about how her sister took her phone, logged in and posted pretending to be her: 'Can be two family members with same name and can think the other family member is sending bad messages.' Another young woman described her own techniques in cracking people's passwords (their baby's name and their favourite number). Others said that mobile passcodes could be deduced by examining fingerprints on the phone's glass.

A student said that someone had hacked into her mobile phone, presumably because she didn't have a passcode or had shared it, and deleted her messages. Her experience corroborated problems with sharing and passcodes that the women's group reported. One student described how she had once 'loaned' a friend her Facebook password so she could message someone, then later started to get messages on Facebook from people she didn't know.

The lack of and sharing of passcodes and passwords on phones and accounts has implications for people's financial security.

AirG VIP charges

Women's group participants commented: 'People have family on both AirG and Facebook—they say that they use AirG because you need credit for Facebook.' They described the use of AirG as follows:

> Arguments on Facebook, but if you don't have credit then it happens on AirG. Kids in communities that are out of town are using AirG more because they are running out of credit. They would probably use Facebook if they had credit.

Most of the women—and their family and friends, it seems—were unaware that AirG VIP (an instant messenger service) use is charged at 95 cents a day on mobile phones, and that this is deducted from their Telstra prepaid credit. The young men at the high school

also said they used AirG VIP when their credit had expired and they could no longer access Facebook. Ippei Okazaki, Director of the NT Community Justice Centre, who regularly conducts mediation of cyber safety–related conflicts in remote communities, commented:

> There are heaps of Aboriginal users paying VIP … That means about $30 extra on top of Telstra's monthly phone charges. When I let them know, they are often surprised to hear that and wondered why adding $20 credits to their phone does not go far (Okazaki 2016).

Some participants suggested that Telstra could intervene in the situation by stopping AirG from being used without credit (by removing the 15-day grace period), which would make people more aware that AirG VIP is not a free service.

Online scams and fraud

Participants mentioned scams and hoaxes in reference to fears of someone accessing their bank account online:

> Banking on phone is risky … scams and 'dodgy ones', as well as dodgy phone calls and emails, stalkers, 'Dodo'—wanted money out of my account but it was a scam.

One middle-aged woman described how she had lost all of her money to 'Dodo', an online scam, which offered an iPhone for $1 if she provided her bank account details. Other participants were wary of companies offering iPads and laptops through hire-purchase arrangements, because they knew these could be more expensive to pay off over the long term.

A legal aid lawyer also noted the difficulties some remote Aboriginal people had in managing online banking and security, and their vulnerability to fraudulent behaviour. He gave examples of where a relative had accessed a family member's account by knowing the password and other personal details, and passing themselves off successfully as that family member to banking staff.

Similarly, an older woman described a situation in which she had allowed her niece password access to her bank account:

> I made a mistake before with one of my nieces. She wanted me to transfer money out of my account. Then I realised some money was missing from my account—I saw it on account statement and got the bank to stop it.

She protected herself from further incidents like this by only allowing certain people whom she trusted to transfer money on her behalf.

As these stories indicate, concerns about online security that are arising as a result of mobile phone practices mean that some people are missing out on the benefits of online services, including internet banking. Such services are important for people living in remote areas, where alternatives involve travelling long distances or using intermediaries (such as store keepers) who may charge for assistance and keep manual records of people's account numbers, which produces additional security problems (Rennie et al. 2016).

6. Digital literacy

> I want to teach other parents how to make their phones safe for their kids and for themselves.
>
> —Tennant Creek women's group participant

Recently, scholars have critiqued an earlier emphasis in cyber safety research and education on dramatic and disturbing incidences of online harassment, underlining that these are symptomatic of a range of issues that the term 'digital citizenship' encompasses. Griffith University's 2011 evaluation of the ACMA Cybersmart Outreach program, for example, advocated that the current focus on cyber safety be broadened from a 'fear and safety', protectionist paradigm to a celebratory one that embraces an understanding of digital citizenship issues and promotes positive values in online communities, like 'belonging, citizenship, connectedness, collaboration, community' (GIER 2011, p. 16; see also Swist et al. 2015).

The promotion of digital citizenship as a key set of values and activities has been accompanied by an emphasis on the development of digital literacy and capability, particularly for sections of the population likely to be more vulnerable to cyber safety and online security issues—that is, those typically marked by the digital divide, such as older and disadvantaged groups.

This section discusses our observations on digital literacy levels among remote Aboriginal populations, and the potential effectiveness of building digital capability to tackle cyber safety issues.

One of the main indications from the research was that remote Aboriginal participants wanted more information about the use of digital devices and social media to assist with managing cyber safety issues. Whether providing further education and assistance—that is, building digital capability—is all that is required to address cyber safety remains an ongoing area of investigation.

Existing digital capability

In the cyber safety one-on-one interviews, we included three basic questions related to people's capacity to set passcodes and passwords on mobile devices and social media accounts, and capacity to manage online harassment and inappropriate content (blocking and reporting on social media, and using Facebook privacy settings).

Facilitators also raised these issues for discussion in the workshop groups, and offered basic education on mobile phone and social media settings, in response to requests. Differences in knowledge emerged between groups and locations, with some demonstrating, for example, that they knew how to use Facebook settings while others did not know they existed.

In the interviews at Tennant Creek and Elliott, 22 out of 23 people responded to the basic questions about their facility with ICT devices and social media, which are recorded in the table below.

Table: Knowledge of passcode and password settings, and social media blocking

Do you know how to …	Yes (%)	No (%)
… set a passcode or password on a phone or a computer?	82	18
… block or report people on social media?	73	27
… use Facebook privacy settings?	64	36

Source: 22 interviews at Tennant Creek and Elliott.

Setting passcodes and passwords

As described in earlier sections, not knowing how to set passcodes on phones and tablets, as well as passwords on AirG and Facebook accounts, emerged as a significant issue. The lack of this security was associated with credit bullying and with the loss of devices and equipment, music, photos and games. Participants reported instances where their accounts had been hacked, with others sometimes using their social media to send or display inappropriate content. One woman, for example, showed a researcher her AirG account and how her niece had 'been there', posting comments.

When the young people's group was asked what Telstra could do to address cyber safety, they said, 'Put a password on AirG.'[1] In Elliott, male participants said that some people in the community didn't know how to operate their wi-fi privacy settings, so others stole their wi-fi. This can happen with a hotspot from an individual's phone, or the wi-fi at the Council building in the community, or the wi-fi at the Eldorado Motel in Tennant Creek. Sometimes children sit outside the motel in the street late at night accessing the Eldorado wi-fi on their phones.

Blocking and reporting on social media

Knowledge of how to block and report people varied within and between groups, and between different platforms (AirG/Divas Chat and Facebook). For example, in Elliott, most participants said they knew how to block people on Facebook.

An older woman described how she had blocked people when they were swearing or sending nasty messages on Facebook, and deleted material on AirG: 'Need to stop messages immediately on Divas Chat—people really going off on Divas Chat.' She gave an example of how she'd told a nephew she would delete his messages if he kept on posting nasty things:

> Once I've been doing that, other people don't do it so much. If people use bad language—I send them a private message, saying that's bad language or say, if there's something you want to talk about, tell me proper.

She had also found the Facebook page of the New South Wales chiropractor who'd been charged with harassing Nova Peris online and posted comments, saying, 'You can't treat an Indigenous woman like that.'

1. A password and username is required to log in to AirG/Divas Chat. However, users must sign out of the service each time to prompt this security setting.

Another woman suggested that Telstra close accounts of repeat offenders on AirG:[2]

> If someone is being reported all the time could Telstra close their account on them? If more than three people report the same status they should get suspended for a week—that way they learn.

During discussions in Tennant Creek, it became apparent that many people were unaware of how to block and report people on AirG and Facebook, and how to use privacy settings. The exceptions were some (younger) participants; a 30-something woman said, 'Sometimes you block or ignore … Sometimes I accept when I know that person. Even scams when they ask for money, I just block them.' The men observed, however, that blocking people on social media could be problematic because you had obligations to people culturally.

Taking down fake AirG accounts can be difficult. Ippei Okazaki from the NT Community Justice Centre commented:

> We receive weekly requests to shut down fake or hacked AirG accounts from [one] community alone. Unfortunately, AirG in Canada are not as co-operative as they could be when impacted families contact the 1800 number. AirG requests people put their complaint in an email, at which point people ring me out of frustration. They are frustrated as they do not have an email account or they are such infrequent email users engagement becomes problematic due to forgotten email passwords or not checking follow up email from AirG (Okazaki 2016).

Photo tagging

High school students were aware of how tagging photos could be problematic on Facebook: 'If you post something on Facebook when you're young, it can follow you the rest of your life.' Snapchat and Instagram were specifically mentioned here: 'You can screenshot Snapchat. It's always in the background—hard to delete things [from the internet].'

They also described being tagged in porn shots without their permission: 'Some people tag you in porn shots, say "do you like that?" It's disgusting, they should have shame.' One girl said she'd been tagged in a porn shot: 'It was disgusting and I deleted it.' Another girl had received a porn shot, but she thought the boy who sent it had had his account hacked. Not all the students in the group were aware of how to un-tag photographs on social media. Young men were concerned about photos leaving a trail and being found out later (a 'digital footprint').

Facebook privacy settings

When the Tennant Creek women's group were asked if they knew there were different types of friend settings on Facebook, they said, 'No—it's all open to the public.' One woman commented to a researcher that 'Facebook needed a tiny padlock'. The researcher showed her that Facebook indeed had a tiny padlock where you could do a 'privacy check-up', which the woman hadn't known about.

Some mothers observed that they didn't have access to their daughter's Facebook, indicating that the younger generation knew how to use privacy settings. Some of the

---

2. User behaviour complaints are handled immediately after being received by AirG. Repeat offenders receive a permanent ban by AirG; however, this does not stop an individual simply creating a new profile.

young men said that the Australian Federal Police had done training using the interactive ThinkUKnow Australia program (Australian Federal Police 2009).

Facebook privacy settings were generally seen as difficult to navigate, especially on a phone; some middle-aged and older people also found the typeface hard to read. However, in Elliott, most male and female participants demonstrated a thorough knowledge of the use of privacy settings, and the possible consequences of sharing private and personal information on Facebook. An older woman explained in detail to the researchers how she had set up a private family page on Facebook with over 60 members, for relatives across the country to share messages.

When asked how they'd learned to navigate Facebook settings, the women's group said that there were a couple of 'unofficial Facebook gurus' that everyone went to for help. Some survey respondents described how they acted as ad hoc digital champions, helping family and friends with Facebook and other online activities:

> I help with issues on Facebook—how to make it private, how to lock photos and get permission to tag. Family members know that I'm good at phones, it just kind of passes on around here …
>
> Many times, I help my grandmother with Facebook … she has an iPhone and can be better than me with using it. I help my family mainly and workplace. Friends sometimes.

This kind of activity suggests how in a relatively small location with about ten years of mobile phone and internet access, some community members may play an informal role in improving others' digital literacy and facility.

Figure 5: 'Fubu' by Beth Sometimes, developed during the Tennant Creek women's workshop.

Death and Facebook profiles

Another issue some participants raised regarding Facebook was how to take down someone's profile after they had died: 'Death—if someone dies, and others don't know how to delete the profile.' People were unsure how to remove someone's profile in this instance and found Facebook's processes difficult to navigate. While handling a deceased friend's or relative's profile is also an issue for non-Indigenous Facebook users, it has particular

urgency for remote Aboriginal people because of cultural restrictions on naming or representing a deceased person, especially during the immediate period following their death (see '1. Literature review').

Learning digital literacy

Most interviewees said that they worked out how to do things online themselves, followed by being shown by family members (a sister, a daughter, a friend and a 13-year-old were mentioned). Comments about how people taught themselves included: 'get on the internet to work it out … work out a lot of things we don't know'; 'I have to read about it myself … I'm a newcomer to it, I have to learn more things.'

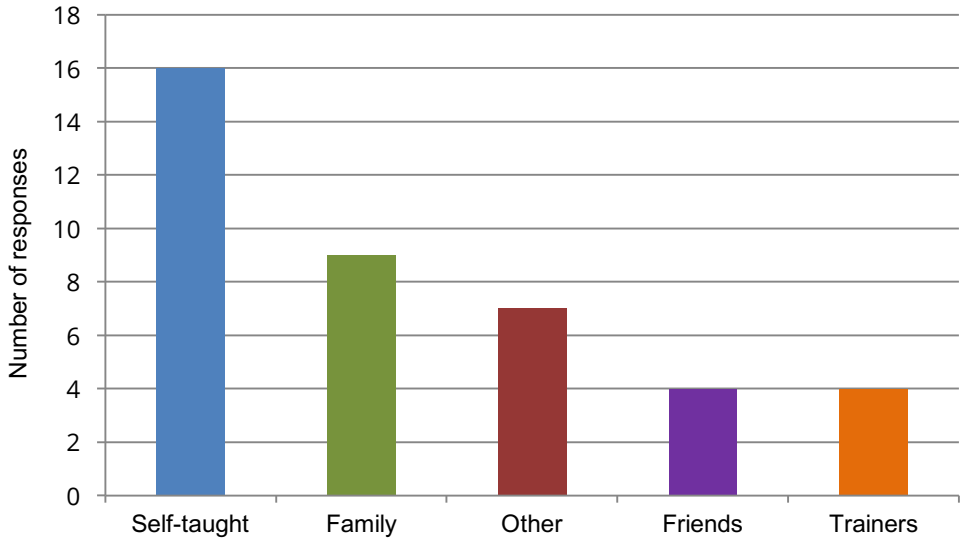

Figure 6: How do you learn new things online? *Source: 22 interviews.*

When asked what they would like to learn how to do online, interviewees said: pay bills; repair vehicles; write English; use privacy settings; use Facebook, Divas Chat and email; use general computing functions; use YouTube; check the weather and the news—'what's going on overseas'. One participant mentioned difficulties navigating myGov: 'myGov. Requires a lot of information. Was on yesterday for a long time trying to work it out.' Three respondents said they didn't want to learn how to do anything on the internet/computer/phone, and two were not sure.

Three-quarters of interviewees said they helped other people use the internet for purposes such as using Centrelink and online banking. Family members were mentioned several times, as well as friends, for example: 'A lot. My partner, sister, mother-in-law, father-in-law, cousin, dad, auntie.'

Several interviewees said they did not help others online. One explained: 'I do my own banking. I don't like to get in other people's problems—I like to be by myself, not sticking my nose in other people's problems.'

Age and gender

How digitally literate the different age and gender groups were, and whether this had implications for delivering information and training emerged as specific areas of

investigation. As in mainstream populations, young people generally appeared more sophisticated in their knowledge and use of digital technology and social media than adult research participants. For example, high school girls knew how to use wi-fi on an iPhone to access iCloud. They used phones for emergency calls and to contact friends and family by text. They observed that it's 'not really phones that are the problem, but what's on them [apps]'.

The students were aware of the potential for false profiles, and online fraud and hoaxes. They had heard of the 'Dodo' scam, and said that you could tell if something was a scam if it was 'too cheap' or 'too good to be true'. They mentioned concerns about having phone and social media accounts hacked, and people not knowing how to use privacy settings. However, they displayed their digital proficiency by saying you could tell if a Facebook profile was fake if someone unknown to you asked your age or sent you photos, or had two accounts with the same name, and that you shouldn't add strangers as Facebook friends. They also knew that you shouldn't disclose your location and you should turn geotagging off to avoid being traceable.

When students were asked in the group discussion how they dealt with problems online, or if they had suggestions about how to do so, they said:

> Turn your wi-fi off or switch your phone off. Turn off notifications so you won't get distracted. Put phone somewhere else. Put it in flight mode.
>
> Go out bush and sit down—but sometimes there's wi-fi out there. At Devils Marbles, they have it. It's dumb.
>
> It's off at different times … They should turn it [wi-fi] off at 8 pm.

One girl said her parents took her phone for a week because she got in trouble on AirG, then gave it back to her with a new password. She also destroyed her SIM card, and only got a new one after having time out.

When young men at the high school were asked what advice they would give to a younger sister about being safe online, they suggested: 'Don't talk to strangers online, don't add people on social media you don't know, don't use AirG until you're 18, and don't share passwords. If a phone gets broken, buy a new one. Shops should ask people for ID when you buy phones and SIM cards.'

Nevertheless, although the students' responses indicated a reasonable degree of digital proficiency, it wasn't clear how effective they were in implementing these strategies.

In Tennant Creek, the students perceived adult men as being less digitally literate, saying that their fathers and uncles often used mobile phones just for calling people rather than texting or going on Facebook. These perceptions were borne out by the male participants' feedback. Two (out of 12) men said the subject of cyber safety was totally new to them. Most of the men's group had heard the term cyber safety but didn't know much about it. Adult male participants found the concept of having an online versus an offline identity, or of acting differently face-to-face versus online, too complex, which probably reflects their usage of mobile phones mainly for voice calling.

However, younger males in the school group displayed similar levels of digital literacy and cyber safety awareness to what the girls showed. This finding was repeated at Elliott, where the men participating in the workshop were relatively young (18 to 35 years) and had a high level of digital literacy. These findings from younger males indicated that this was a generational difference rather than a gender bias towards online participation.

7. Responses to cyber safety issues

> Let the school know—principal and teachers—what to expect from kids, why they're not at school and when they're playing up—it's because of the community conflicts caused by the internet.
>
> —Tennant Creek women's group participant

Interviewees and workshop participants were asked whom they would approach for help—elders, youth workers, teachers, the police, someone else, or no-one—if social media was causing troubles in their community. There was no consensus about the best ways of responding to local cyberbullying. Participants expressed some preference for trying to resolve conflicts related to social media with the individuals involved and with relevant family members first, then taking issues to a broader community meeting if they could not be resolved by families or had wider ramifications.

One person said she 'wouldn't know what to tell younger kids because they don't listen—let them find out themselves'. A middle-aged woman pointed to the complex bind of digital proficiency and cultural issues for adults seeking to address trouble online among young people: 'Can't talk to my brother or my nephew cultural way—only nieces. Sometimes you know something's happened but you're not sure how to talk to them.' Some saw enlisting the assistance of external authorities (police, teachers, lawyers) as appropriate if relevant to the situation (e.g. if cyberbullying occurred at school) or if other avenues had failed to resolve conflict online and offline. Police were most often mentioned in the 22 interviewee responses to this question (half of responses), followed by parents and family members (just over one-third), and elders (one-third). Several responses referred to school and teachers.

Police

One respondent saw cyber safety issues as entirely a police matter:

> The police—they assist us from there. No-one else from phone department here, we need one based here. To help people, to teach them. How to face things if they come across bad things on the internet. Whether to tell/report or leave it alone. Need someone to set the grounds here about who to pull in to sort it out before it becomes a big issue. So people can learn the difference, they think it's simple but it's hard to get yourself out of. Problem goes on but you are stuck in the middle.

A woman remembered the Australian Federal Police (AFP) 'looking at the whole of the NT' several years ago 'to keep an eye on it [cyberbullying] when the trouble started with young ones on AirG'. She nominated the AFP as part of her strategy for responding to cyber safety locally:

> Get the AFP to come out and talk to our community and our elders about cyberbullying—people can translate. Community members, they can interpret.

Another participant observed that the relationship between online fighting and conflict between different families made it difficult to address, but suggested that approaching the police would not be viewed positively in the community, presumably because of negative contact with the justice system:

> Online violence maps to families—if you have a little clan family you can't stand up to a big clan family. And people say you're frightened if you go to the police, which people really hate.

Schools

A student described trouble online as a matter for schools to adjudicate initially before it's referred to parents and police:

> Normally gets raised at the school and they do it—because it usually gets brought into the schools. Students tell teachers where it started. Teachers have a meeting and if it goes too far they get the police in. Or parents.

This response appears to reflect knowledge and possibly experience of an existing procedure for handling cyberbullying at school.

When students were asked in the group discussion how they would deal with problems on social media, they suggested approaching the people involved directly: 'Go and explain yourself to them.' If the problems continued, they said to 'tell a parent', or deal with it 'by talking to your family', or go to the principal if it's someone at school. The young men said, however, that nothing happened when cyberbullying was reported to teachers: that they don't know how to respond to the issue and in most cases no action is taken.

Some older women believed that schools should play a role:

> High schools need to have a process on how to be safe. They teach them how to make an account and they shouldn't teach them until they are older, after school.

Another was critical of the digital literacy training that schools deliver and the age at which students receive it:

> Not teaching basic steps at school. They are not adults, should have been a lead-up where they are more at Year 11 and 12. Teaching them to use it too early for internet access.

But another doubted that what students learned at school had any impact on their online behaviour:

> What schools teach them doesn't make any difference. They don't understand the consequences. They think it's fun but don't understand the consequences. Need to be taught properly—got to stage where fighting physically. Young girl got hit over the head and was unconscious, police had to be called in because of something someone had written on the internet. She placed charges.

One interviewee advocated education for young people and adults on several fronts:

> Should be lessons taught at high school or Grade 6 as they know how to use [social media] from that age. Also through women's and men's group sessions, women's refuge, men's counselling at BRADAAG, prisoners—all need to learn these things. [Someone might] get out of prison and might stalk a person. Not how you should approach a person, and kids need to stop with the nudity. Need to know at high school that half-naked body is bad attention. Brochures are needed. Clinics—people go talk to doctors about it.

Elders and family

Among interviewees, approaching elders was often recommended in relation to their capacity to organise and mediate meetings between family members:

> Elders. Have a community meeting.
> Take to elders, they get family together. Sometimes police. Also parents, and stepbrothers.
> Bring elders and the families of the people in the fight together.

Some women said that 'kids will misbehave and nothing that elders or parents say will make a difference'. A woman who'd been involved in the Tennant Creek Council of Elders and Respected Persons (CERP) when they tried to use 'Divas Cops'—a system where some young people were appointed to report anyone causing trouble online to the elders—to address cyberbullying said it didn't work because the elders would tell the kids to stop but they wouldn't.

Canteen Creek participants said it was the responsibility of individual families to resolve issues such as online and offline fighting: 'It starts at home, you know, and if parents don't discipline their kids it can get out of hand and they can tease and bully whoever.' And: 'But it still comes down to the parents—whatever the parent does, if they stop the kids from fighting and sort problems out, things like this won't happen.'

Community meetings

In the communities, people suggested that a meeting would be an appropriate forum for addressing and providing education about cyber safety. The Elliott men's group gave detailed directions for holding such a meeting:

> It is really important that we have a community meeting to teach married couples and parents that they have to teach their children and take responsibility for things that they are sharing on social media. To organise a meeting like this you should involve the Elliott Women's Shelter, the Elliott police station, the Sport and Rec. Centre, the Council, the Clinic, the school also … Drug and Alcohol at the Clinic. It would be good to bring a footy player or a musician to speak as well so that people listen. A lawyer could talk about social media and the law. We also think a representative from a technology company should be there to talk about the good and bad sides of technology.

Canteen Creek, which did not have a police presence, had a strong sense of local governance. When asked what they did if families were unable to resolve conflicts, they said, 'It's the community's responsibility. Everyone comes together to sort it out.' As discussed in '3. Internet access and use', they thought a community meeting should occur to discuss the introduction of mobile coverage and to watch educational cyber safety videos: 'the community can come together and have a community meeting and watch the show' and 'to move forward the community needs to have the final say'.

Similarly, someone in the women's group stated: 'Brochures need to go to Clinic, refuge, CLC, high schools, training centres, work (can get bullied by colleagues too).'

During a group discussion, a senior woman said:

> We need to go out to the communities and talk to people to tell them to stop doing it. They need to be told with a translator, that the police should come … It needs to happen in communities because the fighting (even killing) is happening there and the police can't stop it.

Talking to each other

When asked to make suggestions about how people can relate to each other on social media, some participants emphasised the need for positive and respectful communication on social media: 'Just tell them good way' and 'Kindly, kind words, share stories and culture with other different communities.' And: 'Not to use abusive or offensive words and to respect each other because respect comes both ways. Build a relationship (not romantic but friendly) with each other where you can talk to each other openly and honestly and with love (not romantic).' Another endorsed the idea of meeting with families offline to discuss online issues: 'We need to talk to the families about it not through the internet—it has to be face-to-face contact, sitting down, liaising with other people. Don't want the distractions.'

When women were asked for suggestions about how to get young girls to think about their reputation online, they replied: 'It's really hard' and 'It's about respecting yourself.' One woman suggested that people needed to develop empathy online: 'It's about understanding another person's feelings—get to know her. You think you know them [on Facebook] but you don't. Facebook—some people don't know each other but they want to be friends.'

Individual responsibility

Several participants included themselves in potential responses to cyberbullying, working in conjunction with other people—'Yes! Myself, police, elders and other family members.' Others saw dealing with conflict as a private or autonomous matter, like the participant who didn't like 'sticking her nose in other people's business'. For example:

> Just myself. I'd make them understand.
> Work it out myself. Other people should too.
> If it's a family member, would tell them not to do it. Would let friends sort it out themselves.

This divided response was evident, for example, among the Tennant Creek men: some said they would report offensive content or bullying to the police, but others said they would 'work it out themselves' rather than go to the school or the police.

Bans

Some older and middle-aged women favoured a ban on the use of mobile phones and social media for people under 18 years, although one pointed out that kids will just borrow other people's phones or 'even go to the town library' to use the internet. This observation was borne out by discussion with the young people's group, who listed all the places where free wi-fi was available in town.

The notion of using restrictions to deal with difficult behaviour is common in remote contexts, such as in the use of alcohol bans, which Canteen Creek community members applied prior to the implementation of restrictions by state, territory and Commonwealth governments. The call to ban the extension of mobile coverage to prevent cyber safety issues in remote communities reflects this rationale, as do to a lesser extent wi-fi hotspot management strategies, which are sometimes implemented by communities themselves, in other instances managed by external agencies with the communities' permission (McFarland & Iten 2016).

Such levers are not available to Aboriginal people living in regional centres, which increasingly rely on the internet to connect them to external services and agencies, and to stimulate social, economic and tourism opportunities (such as the provision of wi-fi at the

Devils Marbles). As well as not being a particularly manageable solution in towns and cities, banning and prohibiting under-age mobile phone and social media use has the additional drawback of restricting opportunities for young people, especially in disadvantaged areas, to develop digital literacy.

Creative engagement or plain facts?

The use of artwork and other creative practices, such as making music or film clips, is often presented as an effective and culturally appropriate way of engaging with Aboriginal people, because of the emphasis on creative practices as an integral aspect of cultural transmission (Rennie 2013). An assumption sometimes operates that educational material will communicate more effectively to Aboriginal people if it employs aspects of their language, idioms and culture, or is at least framed in a 'two-way' format: that is, a dialogue between Aboriginal and non-Aboriginal cultures. As Harper et al. (2012, p. 46) observe, such concerns in educational contexts 'reflect a well-founded consideration that Indigenous students experience real educational difficulties that can be related to cultural difference'.

We found that opinions are divided on which approaches work best in relation to cyber safety education. At the February 2016 Reference Group meeting, some members suggested that local content that remote Aboriginal people developed themselves was the most effective way of engaging them in cyber safety education. Others claimed that it was 'candy flossing' cyber safety, which was fundamentally an issue of lateral violence. While creative content might be entertaining and so forth, they argued, it does not address serious issues, such as youth suicide and assaults, which can emerge from cyberbullying. Instead, people needed to be presented with the plain facts about cyber safety.

As part of the research workshops, we provided opportunities for participants to sample Aboriginal and non-Aboriginal cyber safety resources to gain some indications about what strategies and material communicated the issues most effectively with remote Aboriginal groups. At the Tennant Creek workshops, we trialled the use of two resources: Codey Avatar, a locally developed online cyber safety education tool; and *Photograph*, a non-Aboriginal film about sexting at school. We employed a digital designer with extensive experience in central Australia to work with the women to develop artwork based on the workshop content. Because the digital designer is female, she was only able to work with the women's group. We showed the B2M *Strong choices—cyber safety* (B2M 2012) and *Be deadly online* (Office of the Children's eSafety Commissioner 2014) videos to the Elliott and Canteen Creek groups.

The digital designer, Beth Sometimes, explained how messages about situations involving cyber safety could become the basis for cartoons, and produced poster and comic book scenarios based on the participants' artwork (some reproduced in this report). Although the women enjoyed participating in these activities and were impressed by the artist's cartoon-style representation of their messages, there was not any sense that educational traction was gained by presenting activities in this format.

Responses to educational videos

Responses from young people indicated that they had been exposed to cyber safety educational material, including some clips we suggested showing to them, and had found it effective. When asked what videos they had seen before about online safety, young participants in Tennant Creek said that training from the local police (ThinkUKnow) was

good and they remembered the content. The Elliott men thought they'd already seen the *Be deadly online* and B2M clips, and felt confident discussing cyber safety issues without such prompts.

While participants often indicated that they found cyber safety education videos shown at the workshops entertaining or informative, they generally said the material would be more appropriate for younger, often primary school age groups. Additionally, some participants enjoyed creative activity as a form of engagement, but it was not necessarily more effective as an engagement tool than direct training and discussion.

At Canteen Creek, the women seemed embarrassed by the language (swearing) opening one clip but nodded at some of its messages. They said: 'I think if we were to get internet, people would need this kind of information' and 'Young ones need to know about the messages. And good education about it—it might make people deal with stuff the right way.' Some also expressed concern about whether showing films about issues such as sexting, particularly if they were not current concerns in the community, might give people ideas about things they could do online. When they were asked what age groups would benefit from seeing the videos, they suggested as young as primary school—'11-year-olds use Divas Chat'—and that the educational videos should be screened as part of a community meeting about cyber safety.

This feedback suggests that participants thought there was some place for cyber safety education, especially within a school or community meeting and in response to local issues (such as trouble, or the introduction of mobile coverage). Schools (which go up to Year 8) in the two smaller communities were eager for the researchers to leave behind USB sticks with copies of cyber safety education videos.

Ippei Okazaki, Director of the NT Community Justice Centre, suggested that educational videos about cyber safety may lack efficacy because remote community members are suffering from an educational 'fatigue', as they have been subjected to numerous government campaigns on 'problem issues'. He observed:

> The ACMA and ThinkUKnow YouTube videos I have shown in the community have not really resonated with the people I have shown. They are too accustomed to competing government campaigns for no smoking, gambling, domestic violence, obesity, brushing teeth.

He commented:

> Sitting down and physically showing my phone or printing screen dumps appears to get more of a reaction. Especially when people post using fake profiles of the elders or dead people. However, I concede this is labour-intensive and does not reach a wide audience (Okazaki 2016).

This observation concurs with feedback generally from adult participants that they preferred to have simple and direct 'hands on' information about managing AirG and Facebook usage, setting passwords and parental controls. Other suggestions included producing film clips of a pair of hands demonstrating various activities on social media (e.g. setting passwords and privacy settings) without 'voicing' the instructions in English or translating the instructions into different local Aboriginal languages. As a further output of this project, the research team is currently developing a website with basic information on credit use, passcodes and passwords, social media settings and how to locate lost devices. The comic artwork produced during the workshops is being utilised in the design.

8. Conclusion

Our task in the first stage of this project was to identify the kinds of cyber safety issues that are arising in remote Northern Territory towns and communities and to consider the implications for digital inclusion. The next stage of the project will examine how community, technology and consumer solutions might help address cyber safety concerns.

Cyber safety and digital inclusion

In remote Northern Territory towns and communities, cyber safety is inseparable from digital inclusion. Cyber safety is concerned with the direct consequences of internet use and how individuals and families manage online threats. However, the management or avoidance of online threats can result in restrictions on internet access, cutting people off from the full opportunities and benefits that come with internet use.

As the Canteen Creek experience illustrates, some communities have chosen to go without mobile infrastructure in order to avoid cyber safety problems that have arisen elsewhere (see also Papunya's deliberations on this issue, in Hogan et al. 2013). Other communities are using wi-fi filters, and resorting to temporary wi-fi 'blackouts' when inappropriate use occurs, or when fights break out as a result of social media interactions (McFarland & Iten 2016).

Although such measures demonstrate the strength of customary Aboriginal protocols and mediation strategies—whereby elders are working to maintain community cohesion—they can come at a cost. Rejecting or suspending internet access may result in other hardships, as more services are moving online. The benefits of mobile phones and internet identified by participants in this study—entertainment, financial management, maintenance of family connections, online shopping and government services, and access to information—are significant for all Australians, but especially for those who are living remotely, for whom the face-to-face alternatives are costly and time-consuming.

Unique cyber safety concerns related to mobile-only users

As we discussed in '1. Literature review', the connection between digital inclusion and cyber safety occurs at the level of communication practices. Aboriginal people in remote communities are making particular communication choices as a result of the products and infrastructure available to them (see also Rennie et al. 2016). The result is that Aboriginal people in remote areas are more likely than other Australians to be 'mobile-only' internet users, without fixed home internet connections or the convergent, 'polymedia' (Madianou & Miller 2012) experience that is assumed to exist in the majority of Australian homes.

When combined with sharing practices, mobile-only use can result in particular cyber safety concerns. In this report, we have identified privacy and security risks that arise when devices are shared, including: access to private information in social media accounts, bullying related to use of others' social media accounts, and financial vulnerability arising from insecure internet banking. Importantly, these risks are a disincentive for people to use services (such as internet banking) that might otherwise be of benefit to them.

Cyberbullying

Inappropriate or offensive content, including hate speech, was identified as producing negative feelings and social rifts in remote communities (as it does elsewhere). In remote communities, there is a relationship between conflict online and conflict offline, such as 'jealousing' disputes and difficulties navigating family avoidance relationships. Conflict offline can be initiated and/or exacerbated by online conflict. In addition, cyberbullying becomes particularly problematic when it challenges cultural law and authority. For instance, identity breaches (hacking and false profiles) are sometimes committed as a deliberate challenge to community cohesion.

What can be done

In the first stage of this research, we employed educational resources within our workshops to prompt discussion and to try to understand the level of existing cyber safety awareness. We found that the level of awareness differed across groups and communities, and that there is still a need and a desire for education programs. Overall, participants wanted simple, direct and accessible information about the use of digital devices and social media, to assist with cyber safety issues. Swinburne is developing a website based on this feedback, which will include information on issues discussed in this report, including keeping phones safe from hacking, understanding credit use (including AirG VIP) and finding a device if it goes missing.

As discussed in this report, some communities are successfully using community forums to avoid conflict and violence. However, in relation to cyber safety, existing strategies for mitigating conflict and resolving disputes are not necessarily workable, owing to the rapid spread of information, often across multiple communities. Many participants nonetheless stated that they preferred to negotiate conflict individually, with other family members and 'cultural way', before approaching external authorities. We plan to investigate community mediation in our next report, as well as community wi-fi control responses, such as filtering, or turning off internet access when incidents occur.

Finally, the issue of platforms and technologies requires further research. What is the responsibility and capacity of platforms in dealing with cyber safety issues? It may also be the case that particular problems, such as those related to security and privacy, could be at least partially ameliorated through device security technologies and internet service products. Cyber safety involves a complex interplay of social norms, wellbeing, device design, and the social responsibilities and responsiveness of commercial providers and platforms. Understanding different strategies, and how these interact within the overall system, is important for understanding how the harms of internet use can be reduced, and the benefits maximised.

Acknowledgements

Identifying the communities that might wish to participate in the project, and securing their consent, was a complex process. We relied on Reference Group members to suggest potential sites and local organisations to raise the prospect with community members. Kathy Burns at Barkly Regional Arts helped by providing advice about possible sites and relevant community organisations and representatives to contact. With the assistance of Marie Murfet, Leisha Booth and George Butler at Piliyintinji-ki Stronger Families, and Maisie Flood at Tennant Creek High School, we carried out the first phase of the research in Tennant Creek. Senior woman Heather Wilson and School Attendance Officer Josiah Nuggett assisted our team in facilitating men's and women's workshops in Elliott. Margaret Cowie, CEO of Owairtilla Aboriginal Corporation, and Estelle Mick organised a workshop to discuss cyber safety with the researchers.

Dale Wakefield, former Executive Officer of Alice Springs Women's Shelter, was engaged to facilitate the women's workshops at Tennant Creek and Elliott. Beth Sometimes, a digital designer, led a cartoon-development workshop with the Tennant Creek women on 23 March 2016 and developed artwork in response. Mark Sulikowski, Telstra's Senior Advisor in Indigenous Digital Capability, facilitated the men's workshops. Dale Wakefield and Mark Sulikowski also led workshops with female and male students respectively at Tennant Creek High School. Micheil Paton from the Central Australian Aboriginal Family Legal Unit (CAAFLU) in Alice Springs facilitated and conducted surveys at the men's group at Elliott. Eleanor Hogan led the workshop discussion at Canteen Creek. Eleanor Hogan and Ellie Rennie interviewed members of the women's and young people's groups in Tennant Creek, and Indigo Holcombe-James and Eleanor Hogan surveyed women in Elliott.

List of acronyms

ACCAN	Australian Communications Consumer Action Network
ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AHRC	Australian Human Rights Commission
AIATSIS	Australian Institute of Aboriginal and Torres Strait Islander Studies
ARC	Australian Research Council
ATSI	Aboriginal and Torres Strait Islander
BRADAAG	Barkly Region Alcohol and Drug Abuse Advisory Group
CAAFLU	Central Australian Aboriginal Family Legal Unit
CAALAS	Central Australian Aboriginal Legal Aid Service
CAYLUS	Central Australian Youth Link Up Service
CERP	Council of Elders and Respected Persons (Tennant Creek)
CLC	Central Land Council
HREOC	Human Rights and Equal Opportunity Commission (now Australian Human Rights Commission)
ICT	Information and Communication Technology
IRCA	Indigenous Remote Communications Association
NT	Northern Territory
NTER	Northern Territory National Emergency Response
RIPIA	Remote Indigenous Public Internet Access
SUHREC	Swinburne University Human Research Ethics Committee

References

ACMA—*see* Australian Communications and Media Authority.

AHRC—*see* Australian Human Rights Commission.

Ananny, M 2015, 'From noxious to public? Tracing ethical dynamics of social media platform conversions', *Social Media + Society*, vol. 1, no. 1, pp. 1–3.

Australian Communications and Media Authority 2010, *Cybersmart parents: connecting parents to cybersafety resources*, Commonwealth of Australia, Canberra.

Australian Federal Police 2009, *Think U Know*, viewed 30 May 2016, <http://www.thinkuknow.org.au/site/>.

Australian Human Rights Commission 2011, *Social justice report 2011*, Commonwealth of Australia, viewed 21 June 2016, <https://www.humanrights.gov.au/our-work/aboriginal-and-torres-strait-islander-social-justice/publications/social-justice-report-3>.

B2M 2012, *Strong choices—cyber safety*, Skinnyfish Music, Stuart Park Northern Territory, viewed 30 May 2016, <https://www.youtube.com/watch?v=nPrJ3ngblYY>.

Balogh, M 2014, 'Indigenous Australia addicted to Facebook', media release, 25 August, McNair Ingenuity Research, Crows Nest.

Brady, F, Dyson, LE & Asela, T 2008, 'Indigenous adoption of mobile phones and oral culture', in F Sudweeks, H Hrachovec & C Ess (eds), *Cultural attitudes towards technology and communication*, Murdoch University, Perth, pp. 384–398.

Carlson, B 2013, 'The new frontier: emergent Indigenous identities and social media', in M Harris, M Nakata & B Carlson (eds), *The politics of identity: emerging Indigeneity*, University of Technology E-Press, Sydney, pp. 147–168.

——, Farrelly, T, Frazer, R & Borthwick, F 2015, 'Mediating tragedy: Facebook, Aboriginal peoples and suicide', *Australasian Journal of Information Systems*, vol. 19, pp. 1–15.

Central Land Council 2012, 'Divas Chat causing social chaos', *Land Rights News Central Australia*, April, pp. 5, 24.

Clark, Y & Augoustinos, M 2015, 'What's in a name? Lateral violence within the Aboriginal community in Adelaide', *The Australian Community Psychologist*, vol. 27, no. 2, pp. 19–35.

CLC—*see* Central Land Council.

Donner, J 2015, *After access: inclusion, development, and a more mobile internet*, MIT Press, Cambridge, MA.

Dooley J, Thomas, L, Falconer, S, Cross, D & Waters, S 2011, *Educational evaluation of Cybersmart Detectives: final report*, prepared for the Australian Communications and Media Authority by the Child Health Promotion Research Centre, Edith Cowan University, viewed 30 June 2016, <http://www.acma.gov.au/theACMA/cybersmart-detectives-report>.

Featherstone, D 2015, 'Connected, creative and cultural communities: developing an integrated approach to policy and evaluation for remote Australian Indigenous media and communications', Doctor of Philosophy thesis, Communications, Murdoch University, Perth.

GIER—*see* Griffith Institute for Educational Research.

Green, L, Brady, D, Ólafsson, K, Hartley, J & Lumby C 2011, *Risks and safety for Australian children on the internet: full findings from the* AU Kids Online *survey of 9–16 year olds and their parents*, ARC Centre of Excellence for Creative Industries and Innovation, Brisbane.

Griffith Institute for Educational Research 2011, *The ACMA Cybersmart Outreach program evaluation*, Griffith University, Nathan, Queensland.

Harper, H, Helmer, J, Lea, T, Chalkiti, K, Emmett, S & Wolgemuth, J 2012, 'ABRACADABRA for magic under which conditions? Case studies of a web-based literacy intervention in the Northern Territory', *Australian Journal of Language and Literacy*, vol. 35, no. 1, pp. 33–50.

Hogan, E 2014, 'Behind the mulga curtain', *Inside Story*, 11 July, viewed 30 June 2016, <http://insidestory.org.au/behind-the-mulga-curtain>.

——, Gregory, R & Thomas, J 2012, *Papunya Internet and Computer Centre report*, Swinburne Institute for Social Research, Melbourne.

——, Rennie, E, Crouch, A, Wright, A, Gregory, R & Thomas, J 2013, *Submission to the inquiry into issues surrounding cyber-safety for Indigenous Australians*, Swinburne Institute for Social Research, Melbourne.

HREOC—*see* Human Rights and Equal Opportunity Commission.

Human Rights and Equal Opportunity Commission 2003, *Social justice report 2003*, Commonwealth of Australia, viewed 21 June 2016, <https://www.humanrights.gov.au/our-work/aboriginal-and-torres-strait-islander-social-justice/publications/social-justice-report-10>.

Iten, L 2014, *Southern RIPIA sites cyber safety program report*, Northern Territory Library & Central Australian Youth Link Up Service, Alice Springs.

Joint Select Committee on Cyber-Safety 2013, *Issues surrounding cyber-safety for Indigenous Australians*, Commonwealth of Australia, Canberra.

Katz, I, Keeley, M, Spears, B, Taddeo, C, Swirski, T & Bates, S 2014, *Research on youth exposure to, and management of, cyberbullying incidents in Australia: synthesis report*, Social Policy Research Centre, UNSW, Sydney.

Kral, I 2011, 'Youth media as cultural practice: remote Indigenous youth speaking out loud', *Australian Aboriginal Studies*, vol. 1, pp. 4–16.

—— 2014, 'Shifting perceptions, shifting identities: communication technologies and the altered social, cultural and linguistic ecology in a remote Indigenous context', *The Australian Journal of Anthropology*, vol. 25, pp. 171–189.

Langton, M 2009, 'The end of "big men" politics', *Griffith Review*, no. 22, viewed 21 June 2016, <https://griffithreview.com/articles/the-end-of-big-men-politics/>.

Lumby, BL 2010, 'Cyber-Indigeneity: Urban Indigenous identity on Facebook', *The Australian Journal of Indigenous Education*, vol. 39, supplement, pp. 68–75.

Madianou, M & Miller D 2012, 'Polymedia: towards a new theory of digital media in interpersonal communication', *International Journal of Cultural Studies*, vol. 16, no. 2, pp. 169–187.

McCosker, A 2016, 'Managing digital citizenship: cyber safety as three layers of control', in A McCosker, S Vivienne & A Johns (eds), *Negotiating digital citizenship: control, contest and culture*, Rowman & Littlefield, Lanham, MD (forthcoming).

McFarland (née Turner-Walker), J 2012, 'Clash of the paradigms: night patrols in remote central Australia', M. Crim. Justice thesis, University of Western Australia, Perth.

—— & Iten, L 2016, 'Community management of public internet wifi hotspots', paper presented to Broadband for the Bush Forum V, 8–9 July, Brisbane.

McGlade, H 2012, *Our greatest challenge: Aboriginal children and human rights*, Aboriginal Studies Press, Canberra.

Michaels, E 1986, *The Aboriginal invention of television in Central Australia, 1982–1986*, Australian Institute of Aboriginal Studies, Canberra.

Montgomery, H 2014, 'The internet: the benefits, problems and legal difficulties for Indigenous Australians', *Indigenous Law Bulletin*, vol. 8, no. 14, pp. 19–23.

Oboler, A 2012, *Aboriginal memes and online hate*, Online Hate Prevention Institute, Melbourne, viewed 30 June 2016, <http://ohpi.org.au/aboriginal-memes-and-online-hate/>.

Office of the Children's eSafety Commissioner 2014, *Be deadly online*, viewed 30 May 2016, <https://www.youtube.com/watch?v=3iOBMU-UirQ>.

Okazaki, I 2016, Personal communications, 15 & 17 May.

Olsen, P 2013, 'Teenagers say goodbye to Facebook and hello to messenger apps', *The Guardian*, 10 November, viewed 3 June 2015, <http://www.theguardian.com/technology/2013/nov/10/teenagers-messenger-apps-facebook-exodus>.

Radoll, P 2014, 'Cyber safety and Indigenous youth', *Indigenous Law Bulletin*, vol. 8, no. 12, pp. 11–14.

Rangaswamy, N & Nair, S 2010, 'The mobile phone store ecology in a Mumbai slum community: hybrid networks for enterprise', *Information Technologies & International Development*, vol. 6, no. 3, pp. 51–65.

Rennie, E 2013, 'Co-creative media in remote Indigenous communities', *Cultural Science*, vol. 6, no. 1, pp. 22–36.

——, Hogan, E, Gregory, R, Crouch, A, Wright, A & Thomas, J 2016, *Internet on the outstation: the digital divide and remote Aboriginal communities,* Institute of Network Cultures, Amsterdam.

Rice, ES, Haynes, E, Royce, P & Thompson, SC 2016, 'Social media and digital technology use among Indigenous young people in Australia: a literature review', *International Journal for Equity in Health,* vol. 15, no. 81, pp. 1–16.

Robinson, G 1997, 'Families, generations, self: conflict, loyalty, and recognition in an Australian Aboriginal society', *Ethos*, vol. 25, no. 3, pp. 303–332.

Schmidt, J-H 2014, 'Twitter and the rise of personal publics', in K Weller, A Bruns, J Burgess, M Mahrt & C Puschmann (eds), *Twitter and society*, Peter Lang, New York, pp. 3–14.

Shaw, G & d'Abbs, P 2011, *Community safety and wellbeing research study: consolidated report*, Department of Families, Housing, Community Services and Indigenous Affairs, Canberra.

Sutton, P 2009, *The politics of suffering: Indigenous Australia and the end of the liberal consensus*, Melbourne University Publishing, Carlton.

Swist, T, Collin, P, McCormack, J & Third, A 2015, *Social media and the wellbeing of children and young people: a literature review*, prepared for the Commissioner for Children and Young People, Perth.

Vaarzon-Morel, P 2014, 'Pointing the phone: transforming technologies and social relations among Warlpiri', *The Australian Journal of Anthropology*, vol. 25, no. 2, pp. 239–255.

Willis, M 2011, 'Non-disclosure of violence in Australian Indigenous communities', *Trends & Issues in Crime and Criminal Justice*, no. 405, Australian Institute of Criminology, Canberra, viewed 30 June 2016, <http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi405.html>.