Cyber Safety in Remote Aboriginal Communities and Towns

Summary Interim Report

October 2016

Ellie Rennie, Eleanor Hogan & Indigo Holcombe-James
Swinburne Institute for Social Research, Swinburne University of Technology

About this report

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).

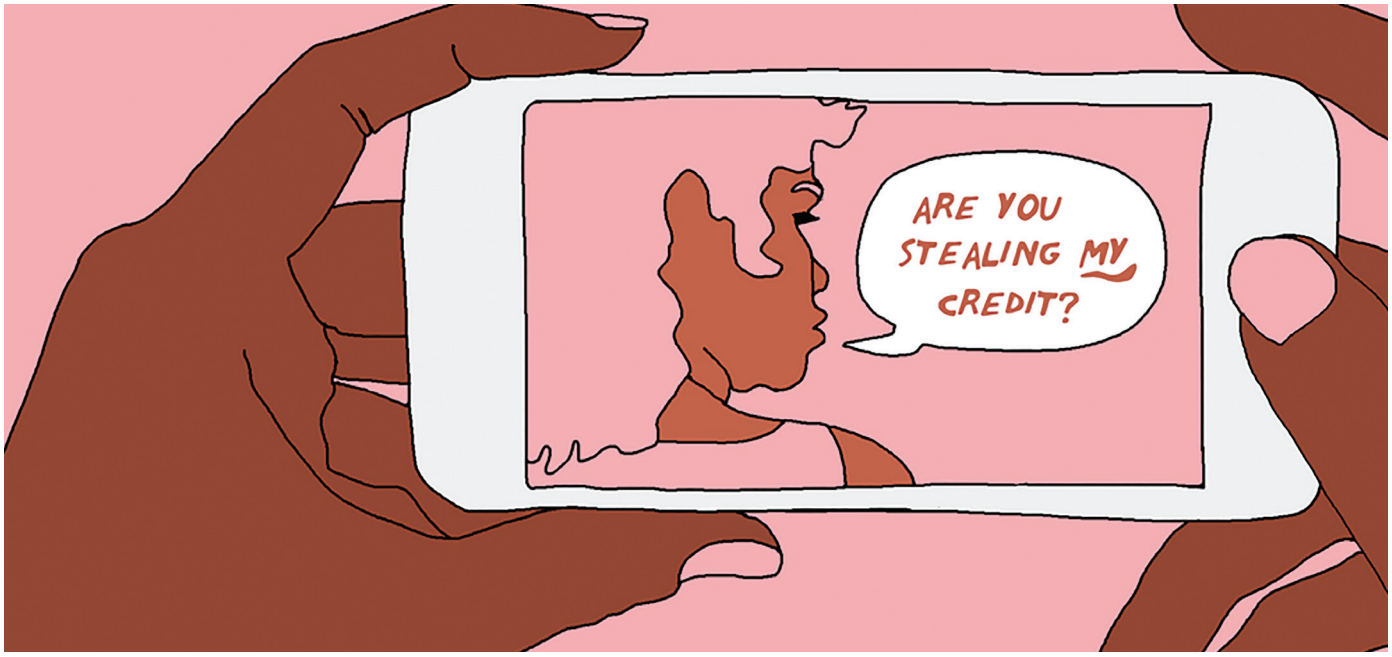
The Swinburne Institute for Social Research is investigating safety and wellbeing as they relate to communication technologies, in remote Aboriginal communities and towns. Telstra is funding the project as an action within the 'Connection and Capability' priority focus area of its Reconciliation Action Plan 2015–18.

This summary report describes the outcomes of the needs-analysis phase of the project, conducted from September 2015 to June 2016, which involved seeking feedback on these issues from a cross-section of Northern Territory 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).

The adoption of 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, 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.

1. 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, may fall within this category.

Revealing photos can 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'.

2. 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 people 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.

3. Financial security and management

Financial security issues, such as identifying scams and fraud, and managing credit and finances, are 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 is free (it is, in fact, charged at 95 cents per day), most likely because there is a grace period after credit runs out, when users can still access AirG before their account is automatically unsubscribed.

Additional findings

4. 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.

5. 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. Community meetings are 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.

6. Digital and cyber safety education and training needs

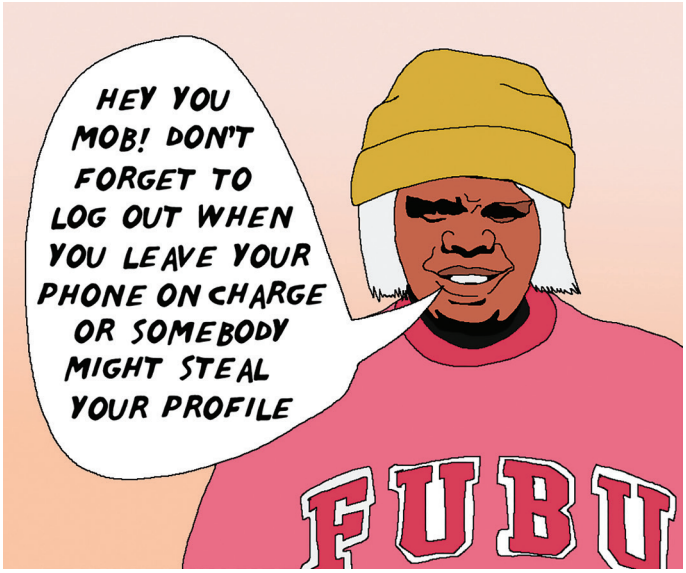
There is a need for straightforward and accessible information, including basic help on using mobile devices and social media accounts.

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'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.

7. 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.



Next steps

The first stage of this research has focused on identifying the scope of cyber safety concerns in remote Northern Territory towns and communities, as well as community awareness and needs. As a direct outcome of our work to date, Swinburne and Telstra will pilot a consumer-oriented website, which will include information on the issues raised in the full report, including keeping phones safe from 'hacking', understanding credit use (including AirG) and finding a device if it goes missing.

In the final stage of the project, we will examine the relationship between cyber safety and lateral violence, as well as community control responses, such as filtering, or turning off internet access when incidents occur. We will also investigate the responsiveness of platforms, and technological developments in areas such as device security. What is the responsibility and capacity of platforms in dealing with cyber safety issues? Can problems related to security and privacy be ameliorated through device security technologies and internet service products?

Cyber safety involves a complex interplay between social norms, wellbeing, device design and available products. Understanding how different strategies interact within the overall social system is important for ensuring that the benefits of internet access are available to all.

References

ACMA—see Australian Communications and Media Authority.

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

AHRC—see Australian Human Rights Commission.

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>.

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

CLC—see Central Land Council.

GIER—see Griffith Institute for Educational Research.

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

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

Hogan, E, 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.

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

Kral, I 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.

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

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

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.

Who we are

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.

The full 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.

www.swinburne.edu.au/research/institute-social-research

Telstra

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. In Australia we provide 16.9 million mobile services, 7.2 million fixed voice services and 3.3 million retail fixed broadband services.

For many years we have been providing products, services and programs to support digital inclusion, including more than $2 billion of customer benefits over the past decade through our Access for Everyone programs.

We believe all Australians should be able to connect, participate and interact safely in the digital world – irrespective of age, income, ability or location – and we recognise the fundamental role Telstra can play in enabling digital and social inclusion.

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

www.telstra.com.au

Acknowledgement

Swinburne University of Technology contributed in-kind researcher time to the project. The partners acknowledge the traditional owners of the regions where this research took place. We thank the individuals and communities involved in this research for their time, knowledge and assistance. Further acknowledgements are provided in the full report.

Visuals in this document developed by Beth Sometimes, a digital designer, who led a cartoon-development workshop with women in Tennant Creek on 23 March 2016 and developed artwork in response.

Suggested citation (Harvard style)
Rennie, E, Hogan, E & Holcombe-James, I 2016, *Cyber safety in remote Northern Territory Aboriginal communities and towns: summary interim report*, Swinburne Institute for Social Research, Melbourne.

DOI for full report:
10.4225/50/578432D317752

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


SWIN
BUR
NE
SWINBURNE
UNIVERSITY OF
TECHNOLOGY