Cyber Safety in Remote Aboriginal Communities
Summary Report
June 2018

Ellie Rennie, Tyson Yunkaporta, Indigo Holcombe-James
Digital Ethnography Research Centre, RMIT University

DOI:10.4225/50/5afcbbe7c483

Overview and summary of findings

Cyber safety involves avoiding or removing harms that might occur because of online communication, including cyberbullying, identity theft, harassment and scams (Swist, Collin, McCormack & Third, 2015; see also Katz et al., 2014; Dooley et al., 2009). Learning and applying certain digital skills is often seen as a means of achieving cyber safety. Taking measures to protect others from harm—especially children—is also part of the cyber safety effort.

In this report, we look at issues that fall under the umbrella of cyber safety, and the particular kinds of outcomes that are occurring in remote Aboriginal communities and towns. Some of the standard strategies for avoiding harm are failing in these contexts, and the resulting problems can affect many people.

We focus on two issues. Firstly, the tools and platform features for managing online privacy do not necessarily accord with the relatedness that characterises social life in Aboriginal communities. Secondly, the circulation of “fight videos” appears to be a phenomenon that can perpetuate violence. While there are cultural explanations for how privacy issues and conflict unfold in these communities, this can change or be amplified through certain attributes of platforms and devices. Seeing cyber safety as a set of skills or behaviours is therefore insufficient in this context. Both Indigenous governance and platform governance need to be considered when addressing these issues, taking into account the ways in which user practices are leading to particular outcomes.

Understanding how conflict and harm are occurring is important for both community safety and digital inclusion. Negative experiences, such as identity violations and unauthorised access to financial accounts, are causing some people to avoid using services (such as online banking), while others are facing increased costs associated with data credit theft and the need to regularly replace lost, borrowed, or damaged devices. In attempting to mediate conflict, some communities and organisations are choosing to control access to Wi-Fi and computer centres.
Findings

As outlined in our Interim Report (Rennie et al., 2016a), the particulars of how people in remote Aboriginal communities access the internet provide important context to the research findings. Internet access is predominantly mobile-only in these communities, and pre-paid credit is preferred to post-paid billing. Facebook and AirG/Divas Chat dominate social media use, although Snapchat is also popular with children. With this in mind, we found that:

- In the communities and towns where our research took place, people were not necessarily using device and platform settings in ways that might help them avoid online harm. Social obligations can influence how people use devices, and this can lead to problems with privacy. For example, the sharing of devices (sometimes without permission) can lead to privacy issues.
- Inappropriate or offensive use included “swearing” (see page 13), teasing, and bullying, which can incite further arguments and fighting offline, particularly when tied to prior hostility, or when communication breaches cultural protocols. When conflicts occur online, we heard, they can escalate quickly.
- The filming of offline fights, which are then shared online, was a cause for concern amongst some community members, who saw them as perpetuating hostilities that might otherwise get resolved.
- Fight videos are wrongly portrayed as riots or gang-style violence by the mainstream media. We show that these fights need to be understood within the historical context of remote Australia, including traditional forms of dispute resolution and Outback amateur boxing. Social media platforms amplify these fights and bring them to a wider audience, which may result in hate speech. Current platform moderation methods appear to be insufficient.
- Financial security needs, such as identifying scams and fraud, and managing credit and finances, are significant. Financial literacy programs should consider addressing cyber safety issues as part of the training they provide.
- A participant’s level of digital capability and cyber safety awareness generally corresponded to the length of time they had been using the internet. We found differences in awareness between age and gender groups, suggesting the need for different approaches and resources for these groups. There is an ongoing need for straightforward, accessible devices and social media accounts. Older people in particular were not confident with devices. Others were aware of how to manage prepaid credit, set passwords and passlocks, block and report people on AirG/Divas Chat and Facebook, and adjust device privacy settings. The fact that some people knew how to use device privacy settings, but were choosing not to, indicates the differences between online privacy and Aboriginal notions of privacy. However, practices are constantly changing in response to technology.

This report identifies several approaches to addressing cyber safety in Aboriginal communities:

- Mediation of various kinds is generally accepted as necessary to avoid further conflict. Mediation that includes community Elders was considered most effective. Older people in particular may need digital skills training in order to feel empowered to manage problems.
- Identifying “trusted flaggers” within communities and organisations to work with social media companies may produce better moderation outcomes on certain types of content.
- Other measures currently being enacted include temporary removal of internet access, either by controlling when and where services are available, or by removing trouble-makers from the community.

About the research

The research took place over two years in Central Australia and Cape York (in far north Queensland). We used qualitative research methods, including workshops with men, women and high school students, as well as interviews with people working in services that encounter cyber safety issues. Ethnographic methods, together with Indigenous standpoint theory, were used for the Cape York component. At the conclusion of the project’s research phase, resources and time were dedicated to producing podcasts, in collaboration with remote Indigenous media organisations, to educate people in remote communities about cyber safety. These productions, along with an additional episode produced by RMIT, can be found at http://apo.org.au/node/172076.

We thank the communities where the research took place, and recognise the Traditional Owners of the lands we visited over the course of the project. Telstra funded the research and podcasts as an action within the “Connection and Capability” priority focus area of its Reconciliation Action Plan 2015–18.

References


