Cyber Safety in Remote Aboriginal Communities

Final Report

June 2018

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

RMIT UNIVERSITY

About the authors

Associate Professor Ellie Rennie

Associate Professor Ellie Rennie is a Principal Research Fellow at RMIT University's Digital Ethnography Research Centre (Technology, Communications and Policy Lab), investigating digital inclusion and the social dynamics of technological change. She has authored or co-authored four books including: Using Media for Social Innovation (2018), and Internet on the Outstation: The digital divide and remote Aboriginal communities (2016).

Dr Tyson Yunkaporta

Dr Tyson Yunkaporta is an academic, educator, Indigenous thinker, maker (traditional wood carving), author, arts critic, and researcher. He is Apalech clan (west cape) with ties in the south, born-country is Melbourne and adoptive and community/cultural ties all over, from Western NSW to Perth.

Indigo Holcombe-James

Indigo Holcombe-James is a PhD candidate at the RMIT Digital Ethnography Research Centre (Technology, Communication and Policy Lab). She researches digital inclusion and cultural institutions.

DOI 10.4225/50/5afcbbe7c4833

Suggested citation (APA):

Rennie, E., T. Yunkaporta & I. Holcombe-James (2018).
Cyber Safety in Remote Aboriginal Communities: Final Report. Melbourne: Digital Ethnography Research Centre, RMIT University.

Contents

Index of tables

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*.

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 information, including basic help with using mobile 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.

Introduction

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, 2016b; Brady et al, 2008; Kral, 2011, 2014).

Mobile devices are life changing; not only do they help overcome some of the difficulties of living in geographically remote areas (such as transport coordination and access to services), but social media applications also provide a means for people to easily stay in touch with family living in disparate locations.

However, cyber safety issues are limiting some of the benefits of internet use. When people find it difficult to manage their online privacy, or find themselves in social conflict as a result of social media interactions, it can make them less willing to take up online opportunities. In the first stage of this research we heard of various instances where people were avoiding opening internet banking accounts, finding themselves without credit because others were accessing their device, or falling victim to malicious online abuse from anonymous perpetrators.[1]

In this report, we look at why people in these remote communities are experiencing negative outcomes from internet use, possibly with greater frequency than other population groups. We explore the reasons, ranging from rules governing communication within kinship classificatory systems, to social obligations around shared devices and credit. Importantly, when cyber safety problems arise in remote communities the consequences can be serious and may involve many people.

Some of these consequences are difficult to assess. Physical conflict, for instance, can signify social breakdown, or it can be an attempt to reinstate social order in accordance with traditional modes of dispute resolution. Moreover, cyber safety is not simply a matter of individual or group behaviours. Technology design also plays a part, in terms of how devices and platforms enable or restrict agency, and prioritise or demote certain content. Looking at the intersection of social norms, values and sociotechnical regimes can help inform strategies to address social harm through communication technology.

Existing knowledge of social media use in remote communities and towns

We know from other studies that Facebook and other social media platforms have become an everyday activity for Aboriginal people (Carlson, 2013; Carlson et al, 2015). A survey by McNair Ingenuity Research and the Indigenous Remote Communications Association (IRCA)[2] found that 51 per cent of people living in remote areas of Australia use Facebook to access information, and 17 per cent use AirG (McNair & IRCA, 2016). Social media is convenient for *maintaining family connections*, particularly with family who live in other communities or regions. Social media is therefore a site for kinship connectivity and continuity (Lumby, 2010). Social media's mixed-media forms are said to be suited to local communication and dialect, by combining text, images, symbols, and sounds (Kral, 2011).

The few published studies on social media use in remote Aboriginal communities also identify particular problems. Some of these issues relate to 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.

Conflict can arise from the production and sharing of what is considered to be unregulated content, done without oversight from community Elders (Radoll, 2014). In relation to identity, Vaarzon-Morel (2014) looked at how everyday expectations of conforming to and respecting customary law are bypassed through the use of fake online profiles. Elders from the Ngaanyatjarra and Anangu Pitjantjatjara Yankunytjatjara lands have expressed concern over "wrong way" communication involving flirting and online dating, which becomes problematic within the social order when it goes against kinship-based betrothal demarcations (Featherstone, 2015). Cyberbullying that breaches cultural protocols between and within family groups, or that inflames existing conflicts, has also been documented in academic studies and government reports (Central Land Council, 2012; Hogan, 2014; Hogan et al, 2013; Iten, 2014; Kral, 2014; Shaw & d'Abbs, 2011; Vaarzon-Morel, 2014).

A more comprehensive overview of the existing research on social media and cyber safety in remote communities can be found in our Interim Report (Rennie et al, 2016a). In this Final Report we draw on academic literature from three specific areas that informed our work: network privacy (Section 1.2), violence and dispute resolution (Section 2.1), and platform governance (Section 3.1).

Structure of the report

In Part 1 of this report, we address the specific issue of privacy. Privacy, which can be understood as "boundary control", competes with other values in every society. We look at the concept of relatedness in Aboriginal culture and how privacy settings on phones and social media platforms do not necessarily accommodate situations where social obligations take priority over individual autonomy. Part 2 looks at the consequences of online conflict. We were told of instances where misbehaviour by children led to inter-family feuds and physical fights, sometimes involving many people.

In Part 3 we discuss how these conflicts are potentially made worse through the filming of fights, which are then shared on social media platforms. Fight videos may be perpetuating violence, making it more difficult for disputes to be managed and resolved. Part 4 discusses various approaches to overcoming these harms, including face-to-face mediation strategies, moderation via social media platforms, and management at the level of telecommunications products and infrastructures. Finally, in Part 5, we discuss some of the challenges with conducting qualitative research on cyber safety in remote communities.[3]

1 Findings related to the benefits of mobile devices and internet use are outlined in our Interim Report from the project. See Rennie et al, 2016a.

2 Now known as First Nations Media Australia.

3 For those seeking a complete account of the project findings, we recommend reading this current report in conjunction with the 2016 report (Rennie et al, 2016a).

Part 1: Privacy

1.1 Privacy and cyber safety

The concept of cyber safety is premised on the assumption that particular strategies and behaviours need to be adopted in order to stop or minimise harm. We found that most people in the communities we visited were aware of device settings and how to use them. Despite this, people were still experiencing the kinds of problems we identified in our Interim Report (Rennie et al, 2016a), including: devices and profiles being used by others, people being subjected to unwarranted accusations or unwelcome posts, and financial vulnerability when others used or asked for credit.

If what is occurring is not a knowledge issue, then cyber safety – either as a definition of the problem, or as a strategy – is an insufficient concept for approaching the dynamics of digital communication in remote Aboriginal communities. Following the Interim Report, our research shifted to examining *why* typical ways of managing online communication were failing in these communities.

One answer involves privacy. In Aboriginal communities, people's obligations to others in their networks can take priority over their own needs. Social expectations and norms can thwart typical strategies for avoiding online conflict, including device management. People are therefore considering a trade-off between two scenarios – one in which they use devices and settings as they were designed to be used in order to protect themselves from harm, and another where they abandon these strategies to meet obligations to others, forgoing control in the process.

1.2 Privacy as boundary work

Privacy is best understood as the practice of making oneself open or closed to others. Privacy scholar Christena Nippert-Eng (2008) uses the term "boundary work" to describe strategies and practices that individuals develop to create, maintain and modify what they consider to be private. In online environments, such strategies might include the use of device and platform settings, but can also involve self-monitoring and self-disclosure as ways to consciously construct an online identity to share with others. While these strategies are not confined to online communication, technology alters how these self-disclosure behaviours unfold. We also internalise social surveillance differently in online contexts. For example, teens are known to post cryptic messages that peers can decipher, but which remain opaque to parents (boyd, 2014; Marwick, 2012). Strategies for privacy therefore require constant maintenance and negotiation (Ito et al, 2008), and can involve difficult choices. Helen Nissenbaum writes that when information technologies violate the flow of information that sustains relationships and activities (maintaining or balancing competing interests), the consequences can be serious, "disrupting the very fabric of social life" (2009, 3).

Following this, we set out to understand how the sociotechnical systems of mobile devices and social media are interacting with conceptions of privacy in remote Aboriginal communities. We found that a form of boundary work is being enacted, but that it does not accord with the privacy controls embedded in social media platforms and devices.

1.3 Method

The research for this stage of the project took place in two locations. The first location was a large community in far north Queensland's Cape York region (which we refer to as Community A).[4] This community has had mobile coverage for many years. The second location was a community in Central Australia (referred to as Community B).[5]

The first stage of this research, intended to scope the issues, involved workshops and group discussion. In the second stage, we undertook a more ethnographic approach. The data collection for this stage was carried out by research team member Yunkaporta, who has close ties in the community and experience navigating the complexities of the insider–outsider tensions that occur at the interface of Indigenous and academic knowledge systems. The research involved informal conversations with community members on the broad topic of cyber safety, conducted over a two-week period, supplemented by five in-depth interviews (with three women and two men). These interviews were conducted and transcribed in Cape York Creole and Aboriginal language (presented as such below, and explained in the surrounding text). As part of Yunkaporta's Indigenous standpoint methodology, data analysis was executed through "yarns" with family and knowledge-keepers, deep reflection, and the carving of symbols on a traditional wooden object before translation into standard English print forms (see Appendix). The data was also analysed as a group (by the report authors) in relation to technology design and use.

1.4 Demanding and sharing mobile devices

Device sharing was common in both Community A and Community B, despite widespread awareness that giving a device to someone else might lead to problems. As outlined in our Interim Report (Rennie et al, 2016a), 80 per cent of the Central Australia interviewees (n=17) used their own device, but 57 per cent (n=12) said they also used someone else's. Most respondents (72 per cent, n=13), in answer to a question about sharing devices, said they sometimes let other people use their device. Some spoke of their devices being taken or stolen, but in many instances, devices were given to another person on request.

The Cape York interviewees suggested that problems often start when devices are shared. The borrower might use the phone for deliberate mischief, or unintentionally use it in ways the owner might find problematic. For example, a senior man in Cape York used the words "borrow" and "to give", suggesting permissioned use of devices by non-owners:

> **Participant 3:** *Why they don't own that phones some them might together, borrow it. To give someone that might cause problem also. That's where you know where they abuse it that can cause problem or, we need to find some sort of a way that how we can educate our people not to misuse this phone.*

Here, the Elder's solution was not to stop others from borrowing phones, or to set a pin number to restrict access, but rather to educate the borrower on appropriate use.

4 The Cape York community chose not to be named in this research. As such, throughout this report, we refer to this community as Community A.

5 The community in Central Australia is also not named here: we refer to this community as Community B throughout this report.

Another man (Participant 5) described the difficulties he experienced in managing his mobile phone. He was distressed that after his daughter used his phone, he could then "see" her boyfriend inside the phone: "I don't wanna see you boyfriend inside that mobile phone now but from him he might ring me, bother me," he explained. In any other situation, he would avoid a daughter's boyfriend, as some forms of contact with in-law groups may breach kinship rules. Even if it were not the man's fault if he saw the boyfriend's name in his phone, or spoke to him accidentally, he would still be accountable under customary law. We learnt that what was commonly described as people "smashing" their own phones can occur in response to such accidental "wrong way" communication. Kinship can also work the other way: a group of men in Community B observed that blocking people on social media could be problematic, because they had obligations to people and blocking would cause offense.

Not everyone felt these obligations or responded in these ways. However, even when avoidance relationships were not a factor, other expectations could still impact on the device owner. One middle-aged woman living in Community B said she had owned five of her phones in recent years; three were taken from her, and two she destroyed deliberately because people were asking for them. A senior woman said that she and her husband slept with their phones under their pillows, but this did not always prevent much younger people from taking them.

Taking the time to set or change the security options on a device is, on the surface, more straightforward than tactics such as hiding that device. People were mostly aware of how to adjust security options, but chose not to. The vast majority of interviewees confirmed that they *did* know how to set a passcode or password on a device (82 per cent, n=18). In the workshops, however, women said that kids would find ways to get into phones, including reading fingerprints left on phone screens as a means of deciphering pin numbers, while others suggested that they felt obliged to share their pin with other people.

A Torres Strait Islander woman living and working in the Cape York community (Participant 4) revealed that although she owned a phone, she could not use it as it was locked (rendered inaccessible) after her kids tried and failed to guess her pin. According to the woman, being locked out of devices was common in the community, and resulted in some people regularly discarding locked phones and buying new ones. She said that other people she knew had given up on using pins, suggesting they were either unaware of how to unlock a device, or found dealing with retail service providers too onerous.

1.5 Hacking

A young woman (Participant 1) described her experience of being "hacked", by which she meant someone had used her social media account without her permission:

> *You get hacked, someone hack your phone, cause a lot of trouble. It happened to me last year, someone hacked my Facebook and I don't know who was sending um, like texting this one boy, and I got into trouble. That girl came to me at the shop and just—she just hit me. Punched me. Yeah. "You was texting my man!" I said, "What? I didn't," and when I went back online I seen this text message. I said "What? I didn't do that!"*

After describing the above incident (in which someone had impersonated her within the Facebook messenger application), the young woman went on to give other examples of similar incidents happening to people she knew. She then stated that "Divas is more worse than Facebook." When asked why the Divas Chat application was worse than Facebook, she explained:

> *Because Facebook you have to put your real name. But Divas you can put any name you want to and wherever you're from and where you [...], but some teenagers will put from Brisbane and other names like "bad boy" or something and then they will swear other people they know from here but they doing it here and they say it's me calling other girls name. That's why they couldn't find out who was doing that round here – who was swearing dead people and that. They went to the police and said can you call the [telecommunications provider] and find out whose number is that but they couldn't find out.*

The woman was describing people creating profiles on Divas Chat and using them to "swear" another person whilst remaining anonymous. As discussed further in Section 2.1, in this context "to swear" is different from using bad or rude language. "Swearing" is almost akin to a curse, an indecent assault that must be answered with vigorous aggression. When asked if this form of teasing was happening at the same level as it was before the widespread adoption of the internet, the interviewee said that it was now worse, and attributed that to the fact that it was done anonymously:

> **Interviewer:** *So is it just the same teasing as before, before the phones, before the internet, or is it like worse teasing?*
>
> **Participant:** *Worse teasing.*
>
> **Interviewer:** *Like worse kind of teasing.*
>
> **Participant:** *Yeah now. Than before.*
>
> **Interviewer:** *And how come, what is it that makes it worse? Like how come they doing it worse?*
>
> **Participant:** *Because see they don't, they won't find out who that person.*

She also explained that people are likely to have non-Indigenous friends on Facebook, "so people they don't swear on Facebook". According to Ellison and colleagues, privacy can mean "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" (Ellison et al, 2011: 20; Westin, 1967). In the young woman's account, individuals were losing the ability to control their reputation on Divas Chat, yet regulating their reputation on Facebook. This observation demonstrates how platform governance – in particular the rules and moderation systems created by social media companies – can have direct outcomes for users (see also Section 3.7).

1.6 Autonomy and relatedness

The problems discussed above stem, at least in part, from two competing systems of privacy: the tools available to manage information through technology are in tension with, and thwarted by, media practices stemming from social norms among the group. The technological tools – passwords and passlocks, and blocking people through social media privacy settings – were being ignored or abandoned by some. People were experiencing hardship because they found it difficult to manage devices, including who had access to their accounts. The apparent gap between privacy concerns and behaviours may be linked to how the notion of relatedness in Aboriginal culture differs from personhood as understood in Western cultures.

As Marwick and boyd (2018) note, while "privacy law and privacy technology are significantly intertwined [...] most work in this area is distinctly Western" (2008: 1159). As a result, "although privacy and surveillance affect different populations in disparate ways, they are often treated as monolithic concepts by journalists, privacy advocates, and researchers" (Marwick & boyd, 2018: 1159). In this section, we work towards untangling these factors.[6]

The autonomy of the individual is a core concept of the Western paradigm of rights, in that entitlements are accorded to all human beings (natural rights), as a necessary means of achieving maximum social good. Aside from the institutional construction of privacy within law and state, the primacy of the individual also manifests through moral and social codes, including an emphasis on self-preservation and the pursuit of power and recognition – the self-fashioning person (Glaskin, 2012). When privacy is defined as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" (Vitak et al, 2011: 20), it places the autonomous self at the centre.

For Aboriginal knowledge systems, the individual is subsumed within the social, defined by kinship and clan membership. In this context privacy, as the selective control of access to the self (as per Altman, 1977), still occurs, but the self might also be defined by connections to others. Systems of avoidance, regulation of contacts, and separation between women and men at times, are boundaries where infringement has consequences. Anthropologists working in different regions of Australia have described this as a social order that is characterized by "relatedness" (for a full discussion see Rennie, Yunkaporta & Holcombe-James, 2018).

We do not wish to overdraw the distinction between autonomy and relatedness. In Western (non-Indigenous) systems, while the notion of privacy involves the protection or preservation of the individual, it also enforces rules of civility and social norms (Post, 1989). The concept of privacy as enacted through law tort therefore acknowledges that individuals' privacy needs are inseparable from social life.

Melford Spiro warns against describing the Western self as "autonomous, egocentric, context-independent, and the like", as this approach can conflate cultural attributes with political concepts of individualism. He contends that "there is much more differentiation, individuation, and autonomy in the putative non-Western self, and much more dependence and interdependence in the putative Western self, than these binary types allow" (Spiro, 1993: 117). Expressions of autonomy are, and have been, expected and accepted in Aboriginal social relations. Cultural change is also loosening the degree to which obligations determine the distribution of material goods and resources. However, where relatedness still influences social norms, it can manifest in difficulties when people try to manage devices and online privacy.

As these examples show, the sharing of devices among kin in particular can result in established, longstanding codes being stressed or broken, including boundaries that determine whom people are allowed to communicate with. At the same time, sharing is a feature of relatedness, and refusal can have negative consequences. Writing in the 1990s, David Martin noted that for the Wik Mungkan people of Cape York, a refusal to share, or a perceived inadequacy of sharing, is a denial of relatedness or of "one's rights and interests in that relatedness, and a denial of a set of norms and values understood and represented as axiomatic" (Martin, 1993: 36). Sharing and exchange are thus a means by which the social order is enacted and maintained.

As relatedness is differentiated, degrees of obligation vary, which may explain the seeming complexity of these localised mobile device practices to outsiders. Moreover, people use tactics to avoid demands; actions such as hiding devices in clothing are a means of denying without committing outright refusal. Some contemporary objects may also be deemed exempt from demand sharing (Macdonald, 2000). We observed this in our Interim Report (Rennie et al, 2016a), where we noted that mobile devices and credit seem to be in a grey zone where denial (and hence autonomy) might eventually be exerted. Two women in Cape York described their interactions over phone credit. The first (Participant 1), in her twenties, had begun denying requests:

> *Last year all the girls were at boarding school like family they used to text me, "Sis can I get credit off you just two dollar," they would text you their numbers, "Please," like beg you. I was like sending them credit but then I said, "No I can't place my credit on yous."*

Participant 2, a woman in her thirties, said she had previously asked others for credit ("I used to be like that!"), but added, "Somebody buy me credit I'll pay it back," suggesting that for her, reciprocity around credit is symmetrical, and therefore more closely aligns with non-Indigenous sharing systems.

6 For further information on how privacy is a Western construct, and how it interacts with non-Western contexts, we suggest reading the recent special section "Privacy at the Margins" in the International Journal of Communication, 12 (2018).

1.7 Summary

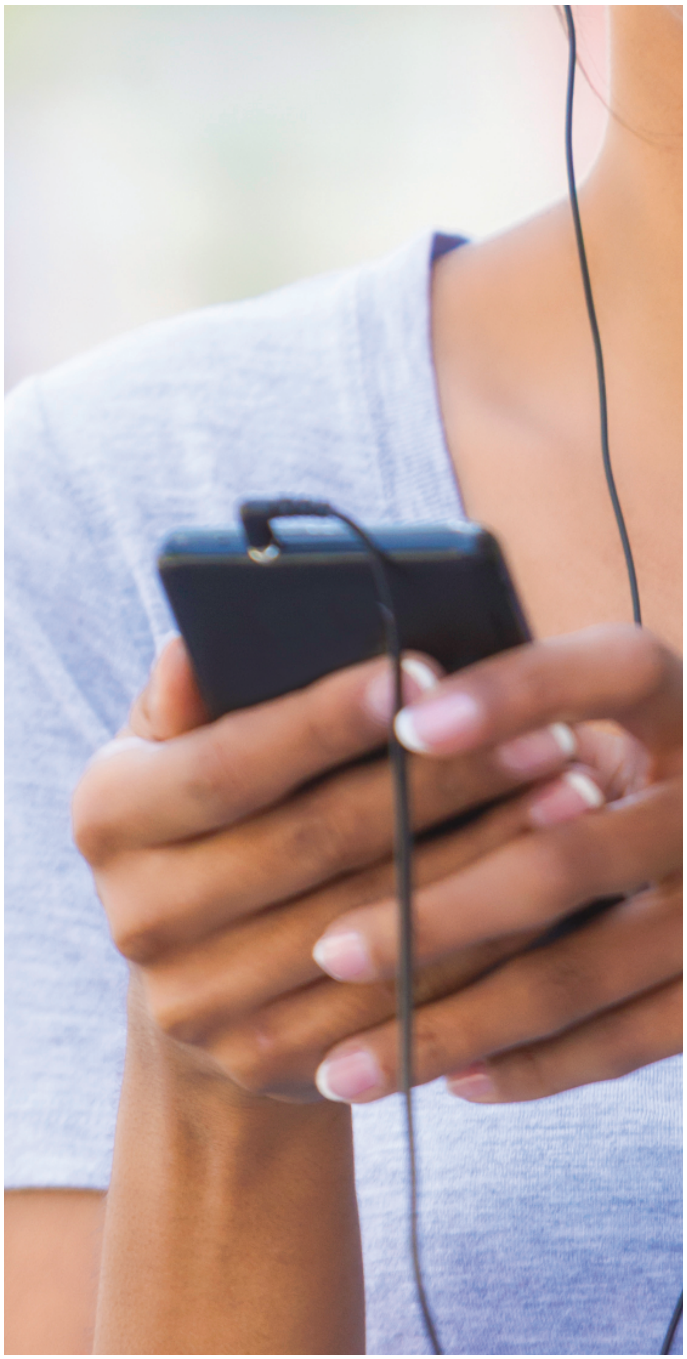
Privacy issues assume a different order and nature in remote Aboriginal communities, because the sociotechnical frameworks of online platforms and devices institute an individualistic notion of privacy that does not accord with the relatedness that characterises Aboriginal sociality. While some material objects may be deemed exempt from demand sharing obligations, including mobile devices and other communication technologies, the boundary work that individuals employ to maintain privacy online is nonetheless influenced by these norms.

Privacy issues in these communities include:

- people using others' social media and financial accounts, sometimes without their knowledge;
- users transferring credit from one device to another without the owner's knowledge;
- the owner of a device receiving unwanted calls and texts intended for the prior borrower, which can be problematic due to culturally mandated avoidance relationships.

Jessica Vitak and Jinyoung Kim write that an extreme privacy management strategy is possible at the account level by "deactivating/reactivating one's account or creating multiple accounts" (2014: np). However, they write that such strategies are not likely to be a common practice amongst US graduate students, due to the high management costs. While the management costs are just as high for those living in remote Aboriginal communities (for instance not being contactable at the same number), the pressures and demands associated with relatedness are seemingly higher, as people in these communities seem to replace SIM cards and phones more frequently than other groups do. However, practices are changing and some people are choosing not to share devices.

Our findings also suggest that standard digital literacy approaches to cyber safety are not adequate for resolving these privacy concerns. In both Central Australia and Cape York, many community members we spoke to knew how to use basic technology settings (including pin numbers and blocking people on social media), but found these strategies to be insufficient or onerous in the face of social obligations. Moreover, when devices are shared, the rules governing communication within the kinship classificatory system can be rendered unworkable through phones and social media, leaving users at a loss as to how to honour both obligations and avoidances at the same time.



Part 2: Consequences

2.1 When disputes move offline

During a conversation in Cape York, one man (Participant 5) said in hushed tones, "They bin swear like dead people aa'." He was describing a particularly dramatic incident that had taken place on social media. Traditionally, "swearing", teasing and the subsequent fights were always highly ritualised, including songs and dances followed by stylised and theatrical combat designed to release aggression and settle tensions, while minimising harm. Participants were always highly visible and accountable for their words and actions. However, in this incident – in which the perpetrator was safely anonymous, and was thus able to blame others for the transgression (using a fake profile) – the double taboo of publicly saying the name of a deceased person while also "swearing" them proved to be an explosive innovation, with disastrous consequences for the community.

In this instance, we heard that family members confronted the people who had been blamed for the transgression, who then responded with greater outrage at being falsely accused. The conflict quickly escalated from the cheeky disruptions of children to a full-blown community feud, with violence involving many people. While young people committed the acts, other family members became involved in the dispute.

A male Elder (Participant 3) commented:

> *Yes and they just misuse the phone and they abusing each other and sometimes one person go away from the group and he or she start you know ringing and start abusing and that's where the problem comes in. And they start blaming each other.*

In using the phrase "go away from the group", the Elder was suggesting an "alone" behaviour, akin to walking down a track unaccompanied, which traditionally – and still today – is a behaviour equated with intent to do black magic or sorcery. Sickness and misfortune that occurs after a person exhibits such solitary behaviours may result in that person being accused of doing "ma' wop" (sorcery) with evil intent. Platforms such as Divas Chat, which enable people to "hide" their identities, are viewed suspiciously by Elders, as users are stepping outside of their social ties, which are in turn connected into ancestral order.

The consequences of such actions can have broader community repercussions. Referring to the fights that occurred after this incident, a young woman said, "Someone can get hurt or someone can get killed just from misusing [phones]." She continued, "I can't leave my phone anywhere. You can't trust these kids, they'll take it and misuse it."

Another woman from Community A described how a boy had impersonated a girl from another family and was "swearing" his own family:

> **Participant 1:** *Someone was swearing some family and that person swearing and saying like another girl's name and the family goes to that family and say, "You swearing" and they say, "It's not me." But one time they did find out. It wasn't a girl swearing, it was a boy. That boy was acting like a girl. And he was swearing his own family. He was the one who causing the fight.*
>
> **Interviewer:** *What happened?*
>
> **Participant 1:** *They took him to mediation.*
>
> **Interviewer:** *But only after they made like big fights and all that.*
>
> **Participant 1:** *Yeah.*
>
> **Interviewer:** *So what happened with the big fights, how did they go, spread out to how many people?*
>
> **Participant 1:** *Lots of people. Men folks were fighting, ladies were fighting.*
>
> **Interviewer:** *All over or just like lots?*
>
> **Participant 1:** *Two families. [Long pause.] Yeah. So that's a bad one there.*

In our Cape York fieldwork, all participants viewed the fights described above as a threat to community cohesion, and all were adamant that fighting incidents had increased as a result of online communication.

In many instances, the fights extend beyond those who committed the original offense and the person at whom it was directed. While the initial communication is often between children (jealousy among adults being the other major type of contributing event), the receiver's kin will seek retribution from members of the opposing family. While this explains how a matter can escalate into a community problem, it also demonstrates that while online communication can be used to undermine relatedness (to "go off alone"), relatedness reasserts itself in the response, albeit in an unsanctioned fashion. Young people from Community B described it in the following manner:

> **Male Participant:** *It leads to fighting, somebody said something about somebody... it just carries on and on: "You said this about me on Facebook, you said that about my cousin on Facebook". Sometimes it doesn't stop, it just carries on for months and months.*
>
> **Female Participant:** *The whole family?*
>
> **Male Participant:** *And the more it carries on the more people get involved in it. Some people they don't even have a phone but they hear and they see from other family members.*

The sharing of fight videos online (see Part 3 of this report) might be a contributing factor, whereby conflict is acted out in public, making allegiances visible and thereby reaffirming connectedness, albeit through unacceptable behaviour in the eyes of Elders. But as the male participant in this dialogue points out, conflict can also impact on those who don't use social media.

Young people from Community B told us that fights were more likely to occur during football weekends. These fights can stem from long-standing hostilities:

> *They got families living at the town camps down here. So when they have problems down there they come into [Community B] and find each other here and then fight here instead of going back where they came from. They come onto other people's country and start problems round here and that's not right... They come for the football. Since footy started it's sorta been fighting and all that, because they been fighting in their community, but they move to another community. So they come to [Community B] to take players to play and they meet up, and they meet at the front here and start the fight and it gets bigger and bigger and with family members coming from other communities.*

However, the young people also pointed out that some fights are caused by alcohol. Posting on social media when inebriated can lead to physical violence:

> **Female participant:** *They probably go drinking and then they go to that person and say, "What you been saying about me on Facebook – I'll bash you... You talk to me face to face." And the other lady will say, "I'll wait until you are sober", but the other lady will keep going.*
>
> **Male Participant 1:** *You see that a lot of times around here in [Community B].*
>
> **Male Participant 2:** *"If they see you up in town and they are sober they just walk past you."*

As this conversation reflects, one difficulty in understanding and addressing cyber safety is that it can be hard to separate out what is the result of platform governance, or particular types of online communication, from what is caused by other factors. The young people referred to fights that stemmed from things said online, but implied that those involved would have been less confrontational if alcohol was not a factor.

2.2 Technology assisted coercive control

When people spoke of jealousy on social media, they were sometimes referring to fights over a person:

> *Well since living here they just been fighting, fight after fight, and it wasn't, it wasn't actually men, it was just women. Like yeah, more women saying things to one another and they having a fight. What are they fighting about and they would be like they said something on chat, they said something on Facebook, you know, "This fulla texted this fulla."*

However, some also referred to jealousy within relationships. A young man admitted that he had recently been "in trouble for domestic violence, breaking in and drinking, hanging around with the wrong people", which he said was "because of AirG" (presumably communicating with these "wrong people" via that platform).[7]

Mobile devices and apps can play a part in domestic violence. A study by the Domestic Violence Resource Centre Victoria (Woodlock, 2017)[8] found that intimate partner stalking is often carried out via messaging (over two thirds of victims surveyed in the study experienced this form of stalking), as well as via social media, or GPS (over half experienced this form of stalking). The authors conclude that mobile devices and social media platforms are providing perpetrators with new means of carrying out coercive control (in the case of GPS), and making it easier to intrude on a victim's daily activities, leading to a greater frequency of abuse.

Molly Dragiewicz and colleagues (2018) suggest the term "Technology Assisted Coercive Control" to describe how domestic violence can be both amplified and ameliorated by the regulations and actions of social media companies. For example, while platforms can make it easier to inflict coercive control, they are also developing policies and mechanisms to address some forms of harassment committed by intimate partners, such as removing images when image-based abuse is reported.

7 While we heard about coercive control via mobile phones within our research regions – people following or threatening partners – we did not have ethical clearance to delve into specific cases.

8 Over 90 per cent of participants in the Woodlock study identified as Anglo-Australian.

Part 3: Fight videos

During interviews with our research participants in Central Australia, we heard that some communications on social media platforms were resulting in physical confrontations involving many community members. In addition, local staff in the justice, education and social work sectors had noticed some people were filming fights and posting the footage on YouTube and other social media and video platforms.

In 2017 and 2018, the production and distribution of fight videos in remote Australian communities and towns attracted mainstream media attention. The media coverage, which depicted these fights as being akin to riots or gang violence, was itself a cause for concern for residents, who saw the reporting as sensationalist. The circulation of fights on social media was damaging the reputation of these towns and communities, and potentially that of their Aboriginal custodians. This was the case in the Central Australian community we worked with for this study. As noted, throughout this report we refer to this community as "Community B".

A number of anthropologists have written about violence within Aboriginal groups prior to the advent of social media. In this previous research, group fights were linked back to traditional forms of conflict resolution, as "clearly structured activities, patterned and predicted by cultural rules" (Burbank, 1994: 4). The same scholars, however, acknowledge that not all fights serve such a purpose (see Section 3.6). Historically, boxing events have also been a feature of Outback towns for both Indigenous and non-Indigenous residents. There is a connection between these two more ordered displays of violence and the fights depicted in the videos, as well as clear points of departure.

One differentiating factor, which we focus on this report, is the role of social media platforms in perpetuating violence. These platforms have evolved into elaborate technical systems that amplify some types of content over others through algorithmic and search design. In interviews, we heard that social media might inhibit conflict resolution. For example, platforms may play a part in exacerbating tension (if not the physical aspects of violence) through the ways in which they prioritise content. In Section 3.7, we discuss the extent to which online moderation approaches might curtail the circulation of fight videos, thus reducing their social influence.

Our aim in investigating the fight videos was to understand the role of social media in relation to these fights, and to determine what can be learnt from the videos of the violence itself. To do this we tried to replicate how users themselves might encounter the videos when searching within the platforms. In terms of the social media elements, we analysed the number and frequency of videos, the extent of their circulation, viewership size, and instances where content moderation had occurred. We tried to understand who was making the videos and how many people were posting them. With respect to the violence depicted, we undertook content analysis of the footage, looking for recurring features in the fights themselves, including the number of people present, and the gender and age of participants.

The key findings are as follows:

- In Community B, a basic YouTube search mostly uncovered fight videos produced in the previous two years (up to October 2017). However, some videos were five years old. The most recent video had been posted four months prior to the research. For ethical reasons, we were not able to determine the extent to which videos are shared on private Facebook pages.
- Some moderation of content is occurring. Over a six-week period, two videos (of the 40 we analysed) that were previously unrestricted became age-restricted to viewers.
- The vast majority of fights seem to follow particular rules. The presence of a large number of people does not signify unruliness, but rather that a fight is being monitored and will be broken up if the violence escalates. The presence of bystanders also suggests fights are a well-understood public spectacle.
- Children are sometimes involved, either as creators of the videos, or as spectators. Children were also seen play-fighting in some videos.
- Of the 40 fight videos we analysed, 24 were from the town named in the search term, and 16 were from elsewhere in Australia.
- The 40 videos were published from 21 different accounts. One account was responsible for publishing 15 of the videos. While comments on the platform suggest that some accounts belong to community members, at least one account seemed to be run by an outsider and motivated by racial prejudice.
- Fight videos have been added to YouTube "playlists"[9], with 25 playlists containing fight videos appearing through a standard search. These playlists contain a high proportion of restricted or removed content (21 per cent), and include fight videos from elsewhere in remote Australia and abroad (in amongst non-fight video content).

Given that Aboriginal communities may not want to attract attention to these videos, there were ethical considerations in undertaking this research. Our decision to proceed followed consultation with our reference committee, whose members stated that they would benefit from insights into platform governance, including the effectiveness of flagging or reporting content. A structured analysis also serves to hold the media to account for unethical news reporting.

9 A YouTube playlist is a curated list of videos chosen and compiled by a particular user.

3.1 Research method

The following methods were used to understand the nature of these videos, and the ways in which community fights are tied up with social media platform culpability and responsibility.

To create the data set we performed searches of YouTube, as well as public Facebook groups. For the YouTube component of the research, we aimed for a minimum of 50 fight videos in order of ranking (or all fight videos if our search returned less than 50). For Facebook, we conducted a basic search within the platform. While fight videos are likely to be shared on personal Facebook pages (known as "profiles"), for privacy reasons we did not investigate personal pages. The Facebook dataset was therefore small in comparison to the YouTube dataset.

Our analysis involved the researchers working as a group to find, watch, and analyse videos on a single computer over the course of one day, and noting metadata associated with the videos, such as views and upload date. The decision to watch and analyse the videos over a day was designed to reflect the assumed practices of platform users: as Freeman and Chapman (2007) argue, "few users would look at >50 videos" on any particular day (207–8; see also Keelan et al, 2007; Gao et al, 2013).[10] In addition, we were interested in understanding not only how these videos intersected with issues of cyber safety from the perspective of their community of origin, but also how they intersected with the practices of use on the platform.

Ethical considerations, along with YouTube's Terms of Service, set boundaries around the scope of the research. As articulated in point 5B of YouTube's "Your Use of Content" guidelines, the platform does not allow users to download any content unless a download link appears. In addition, users are not permitted to copy content, which makes content analysis of large datasets difficult.[11] Accordingly, we devised the following processes for data collection:

1. conducting a search of YouTube, using only the name of the town and the word "fights". We used an incognito browser to minimise algorithmic bias in the search results and repeated the search on multiple devices;
2. categorising by genre the first 50–100 videos to appear as a result of the search;
3. checking individual accounts that were posting multiple fight videos to determine whether the account was primarily used for this purpose;
4. analysing playlists with a view to investigating the social curation of fight videos; and
5. conducting searches under related terms, including just the name of the town. This enabled us to understand the likelihood of fight videos appearing when a user was not necessarily looking for them.

The search yielded three playlists and one duplicate video in the top 50, which we discounted from our analysis. The final number of videos in our content analysis dataset was 55. After this point, the search was failing to display videos related to the "fight video" search term. For the comparison searches, we searched just the name of the town, substituted the name of the town, and searched broader search terms including "fight videos Australia" and "Outback fight videos". We did not perform content analysis on these search results, but looked for differences between the search results, in particular whether fight videos appeared or not.

While we were interested in understanding how users were encountering the platform and these videos, we were also sensitive to the algorithmic biases that follow each of us across the internet. In an attempt to avoid these, we performed our searches on an Incognito Google Chrome window on a university computer. This measure had other consequences, however. For example, unless you log in to Google or YouTube through a user profile, access to videos that have been reported and then made age restricted is disallowed. To get around this, we adopted a combination of using the accessible information (such as thumbnail images and textual descriptions), and using a logged-in Google Chrome browser to search for the specific video and watching it there.

As Lavanya Sunder (2016) notes, some YouTube values are "dynamic", such as views, or likes (2016: 2). Accordingly, the data we collected is valid on the day of its analysis. However, we did revisit the dataset six weeks later to note the number of views in order to determine the rate of increase (see Section 3.4).

Table 1: Data points gathered

Video Content	YouTube-derived data
Number of bystanders	Video name
Number of people directly involved in physical conflict	Uploader account name
Number of people visibly filming the physical conflict	Number of views
Location (whether inside, outside, on main road, etc.)	Number of likes, dislikes
Evidence of any observable 'rules' (such as bystander intervention, or audible comments from bystanders)	Comments
	Number of followers for uploader account

10 While snowball sampling on YouTube should ordinarily follow the platform's "recommended" videos (Sunder 2016: 2), due to this project's geographic focus we decided to engage with the search results instead of following recommended videos. We did, however, run searches with similar words, including abbreviations. This did not drastically change the search results.

11 YouTube's Terms of Service state: "You shall not copy, reproduce, make available online or electronically transmit, publish, adapt, distribute, transmit, broadcast, display, sell, license, or otherwise exploit any Content for any other purposes without the prior written consent of YouTube or the respective licensors of the Content. YouTube and its licensors reserve all rights not expressly granted in and to the Service and the Content" (YouTube, 2010).

Our analysis of the videos' content was based in textual analysis. Cultural studies research positions all cultural practices as texts that can be read for meaning – that is, as an avenue to understand the context from which that text was produced (Fürsich, 2009). Textual analysis is an empirical method that involves deconstructing a text and "examining the formal internal features and contextual location of a text to ascertain what readings or meanings can be obtained from it" (Hartley, 2002: 227). The method we applied to the videos therefore involved "reading" the content for common or dominant signifiers. As with any reading, this requires that the researchers take an interpretive position; the subjectivity of the researcher is unavoidable. However, as John Hartley points out, textual analysis is not intended to find the exact meaning of a text, but to "understand the variety of meanings made possible by a text" (2002: 227).

To structure our textual analysis, we listed common elements, coded the videos, and looked for frequency of occurrences as well as variations between videos. The 55 videos were watched in a continuous sitting over one day, by three researchers in the same room (plus one note-taker), using a single computer. The team included one researcher (Yunkaporta) with specific expertise in the area of Indigenous knowledge and governance systems.

The fourth stage of the research involved categorising videos found in the playlists. In doing this, we were interested in understanding what Thanh Kieu and colleagues (2015) describe as social curation: a process of "aggregating, organising and sharing the content created by others to add context, narrative and meaning" (2015: 415). We searched for "[Community B] fights", filtered the results for playlists, then documented the following information:

1. The account name, or curator, associated with the playlist.
2. Number of Community B fight videos.
3. Number of non-Community B fight videos.
4. Any locations specified in these non-Community B fight videos (in order to identify how widespread or not the practice is, or might be). Videos that identified both Community B and other communities (a recurring practice that we observed seems to indicate cross-community conflict) were marked as both a non-Community B and a Community B video.
5. Categorising the other videos in each playlist (for example, music video, movie trailer).
6. Quantifying these.
7. Noting the presence and number of deleted videos.
8. Repeat until saturation.

In total, we looked at 25 playlists containing fight videos before we reached a point where playlists were failing to show any fight videos. Finally, we also conducted a focus group with young people (aged 18–30 years), and observed a cyber safety training session run by a legal organisation at a local high school.

3.2 Search results

Of the 55 videos obtained and analysed from the search "Community B fights", over three quarters of them (42) depicted some degree of violence. One of these 42 videos featured a formal sporting event (boxing at a "tent fight", discussed in Section 3.6), and one was a compilation of international street fights. While these latter two videos provided important points of comparison in our analysis, they did not fit the definition of what we set out to observe.

The remaining 40 videos depicting violence all appeared to be fights involving women, men, girls, and boys that were filmed on mobile devices by onlookers in remote Australian communities and towns. In the discussion below, we use the term "fight videos" when referring to these 40 videos. In addition to the 55 videos, three playlists also appeared in the top 60 search results.[12]

The most recent fight video was published four months prior to the date of our analysis (October 2017). As shown in Table 2, the vast majority of fight videos that appeared in the search results (37) were published in 2016 and 2017, with only three videos dating from previous years (two in late 2012, and one in 2015, all ranked in the bottom quartile). The presence of these earlier videos demonstrates that this is not necessarily a recent phenomenon. It is possible that there were more videos from earlier years, but these have been buried by the search algorithm.

Half of the fight videos (20) we analysed were identified as being filmed in Community B, or involving people from that town (as indicated in video titles and descriptions). Others included locations elsewhere in the Northern Territory, as well as in the Kimberley and Cape York.

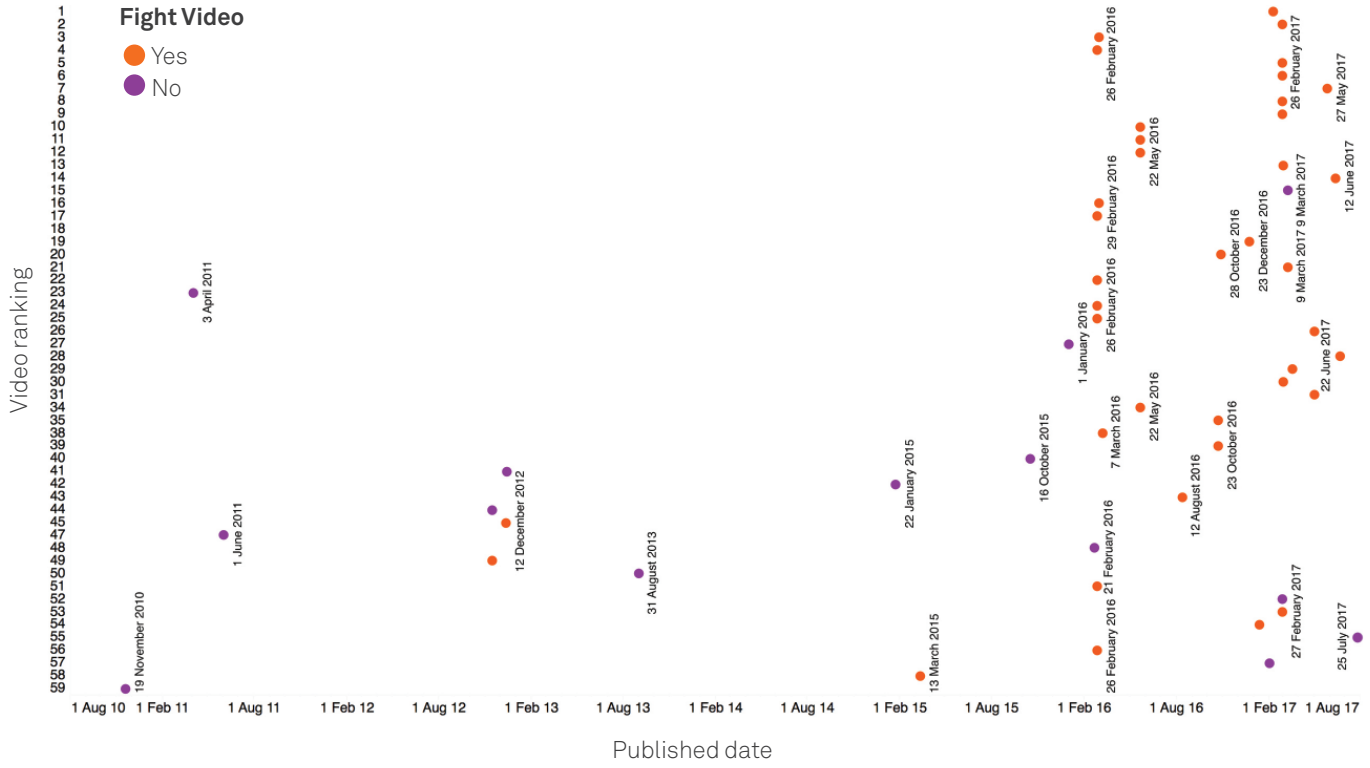
In amongst these videos were 14 videos that related to the name of the town only. One was a music video by an Aboriginal hip-hop artist. Others included videos of community events, digital stories, and travel vlogs.

As stated above, we conducted similar searches in order to understand the importance of place names. A search for the term "fight videos Australia" yields clips of pub brawls and street fights from mainstream media coverage, as well as wildlife videos ("Koala brawl"). The term "Outback fights" yields a higher proportion of tent fight videos. The local name of the town is therefore important in how publishers and viewers identify these videos.

A search of "[Community B] fights" on Facebook yielded links to fight videos on a platform called FunTVKids, along with eight other video sharing sites.

12 One video also appeared twice, resulting in 59 search results in the dataset.

Table 2: Search results by published date (excluding playlists)



3.3 Content analysis

There is much that cannot be known from watching these videos. The videos give no indication of why the fight commenced – such as whether the participants were fighting to defend honour, to resolve a dispute, or for sport. A mix of motivations likely underpins the fights. The fights are clearly a recognisable if not predictable activity, within which various relationships and motives may coalesce. Bystanders' typical reactions, the frequent presence of children, and the lack of collateral damage (to things or bystanders) all suggest a level of community acceptance that fights occur.

3.3.1 Video production values

These fight videos are best described as "user-generated content", in that they were filmed by non-professionals, using handheld devices. The fight videos we analysed were mostly of short duration: half of them (20) were between one and three minutes long. Of the remainder, nine videos were less than one minute long, nine were between three and five minutes long, and two were of more than five minutes long. As with much user-generated content, the videos were of poor quality. Most appeared to be unedited, raw footage created by a witness to the event acting opportunistically. While searches for fight videos using other town names yielded fight videos with some notable production elements (for example, footage that was titled and edited to music), the research dataset only contained two videos with these features, and YouTube had removed the music on one for copyright reasons.

Other aspects of the filming process can be gleaned from the videos. For example, it was common to see footage being shot with multiple mobile devices when large crowds of spectators were present (often with children filming – see Section 3.3.6). Two fights were repeated in the sample, but had been filmed on different devices – one fight across three videos, the other across two videos. We assessed that these fights were therefore considered a spectacle worthy of sharing, and that filming them was not considered to be an out-of-the-ordinary activity. However, some fights appeared to be captured covertly: one video creator was hiding behind a tree, while another was holding the camera at her/his side. In two instances the fight participants asked the person to stop filming, as the following dialogue illustrates:

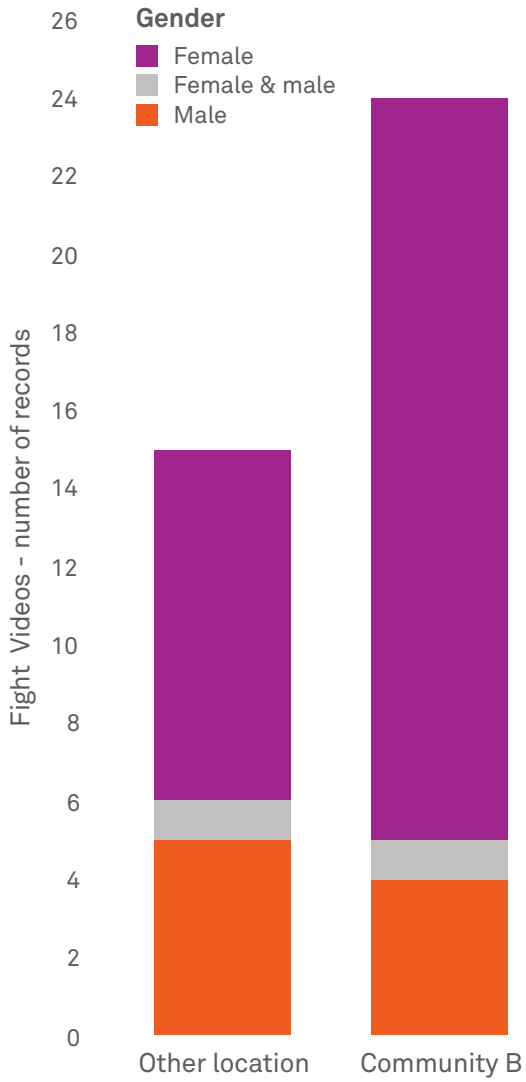
> *"You should stop recording."*
>
> *"I think I shouldn't."*
>
> *"I think you should."*
>
> *"No-one tells me what to do."*

3.3.2 Setting

Most of the videos we analysed were shot in daylight, with only two filmed at night. Both of the night scenes involved fights between teenage girls, with a small number of bystanders lighting the scene using the torch setting on their mobile devices.

Most fights took place in a public location, typically on a street or another outdoor public place such as a basketball court. One exception was an enactment of a fight performed by young girls and filmed indoors.

Table 3: Number of records, gender of participants



3.3.3 Who is fighting?

In our sample, women and girls were shown fighting more frequently than men; 27 of 40 videos involve women or girls, with 16 of these set in Community B. Men or boys were fighting in 11 videos, four of which were filmed in Community B. In addition, two videos portrayed both men and women fighting (but never with each other). When women were fighting, the spectators were usually women and children, although not exclusively.

In 11 of the 40 fight videos we analysed, two or more fights were occurring. In these instances, the video commenced by focusing on one fight then turned to a different fight that had broken out on the sidelines. It is possible that these fights depict some kind of inter-family hostility.

In some instances, a fight video would start with young people fighting, but older people would then begin fighting each other too. When more than one fight was observable, there were almost always 20 or more spectators present.

Three of the videos featured fights between two different communities (framed in terms of Community X "vs" Community Y), as indicated in either the video title or description. In our interviews, some people suggested that fights often coincide with football events, as this is when people from different places come together.

The fact that some participants show resistance to being filmed indicates that those directly involved in the fighting might see it as a private matter, be conscious of the legal consequences of fighting in a public place, or be aware that filming might get them in trouble with parents/Elders/the law.

3.3.4 Style of fighting

In almost all the videos we analysed, the participants adopted a boxing stance and struck with their fists. No weapons were used. The fights appeared to end before anyone was seriously hurt.

Only one video from Australia showed fighting that resulted in blood being drawn. The video is from the Kimberley, and was shot in a town identified only as "Blood City":

> *The fighters are two athletic-looking young men. One young man strikes the other and then steps back, boxing style. One man talks in language, while the fighter with the bloody nose can be heard saying, "I'm alright!" He walks back into the fight, which moves onto the road. When one fighter is down the other stops and moves away until his opponent is ready to resume the fight. While there are clear boxing rules in evidence, the fighters are also displaying anger; the man that strikes can be heard saying "You lucky I don't King it", and "I'll kick-box you". The fight ends with the injured man lying on the road in a pose of surrender, with others standing around him to make sure the opponent doesn't approach again* (researcher's observational notes).

By comparison, the international fight video showed blood and more extreme violence. This video was a compilation of both organised and spontaneous fights from the USA. The fights in this footage were racialised, with captions describing those pictured as "Nazis" and "Aztecs". The video commences with the words "top most brutal attacks no weapons" followed by a warning that it contains content that some viewers may find disturbing (this was edited into the video by the producer, rather than being a YouTube disclaimer). In contrast to all the other videos on our list, the fighting in this video was severe and callous, and no one stepped in to stop the violence or protect the participants.

In the Australian fight videos, there were clear instances when the rules were broken. The two obvious violations were hair-pulling amongst women, or when someone ended up on the ground. In 11 of the videos, spectators pulled the fight participants apart when one or both of these breaches occurred. For example, when women engaged in hair-pulling, bystanders became referees and were heard saying "Fair go, no pulling hair", or similar. Hair-pulling occurred in 9 of the 40 videos. In some videos the fight was paused as a woman re-tied her hair, even when no hair-pulling had occurred. Fights where people end up on the ground were stopped by bystanders, often with multiple people stepping in to intervene.

Some fights were clearly pre-organised, such as this one between teenage girls:

> *One of the fighters stops and then drinks and wipes her face with a washer, says "Don't fucking grab my hair". Fight recommences on road. Again, "Keep on, [name]. Fair go, no pulling hair too." She again stops to pour water on face and uses towel, handed to her by her support crew (researcher's observational notes).*

One video was more disturbing than the others in the dataset. In this video there were signs that the women involved were intoxicated, and that the fight was spontaneous. The violence was more confronting. Our notes, taken while watching the video, described it as follows:

> *The setting is behind some houses – less public than others. Alcohol is a factor; at least one person is holding a bottle of some description. There is a noticeable "winding up" of the fist as a woman punches another. The bystanders (approximately eight women) are more vocal than in other videos. The fight ends up on the ground. Someone steps in to intervene and the person behind camera starts yelling in language as well as "Back off, back off" and "You get up now". Close filming. A bystander is physically dragging the fighters away but the kicking and punching while on the ground continues; it's like a beating, an abuse, not a performance fight* (researcher's observational notes).

The video had twice the number of dislikes as likes, and the single comment was a profanity directed at the person who posted the footage, suggesting a betrayal of social codes in doing so.

3.3.5 Role of bystanders

Half of the videos in our sample featured more than 10 spectators or bystanders (including 11 videos with 30 or more). In some cases, people seemed to be fortuitously close by, while in others they were more likely deliberate witnesses to the fight. In many videos the bystanders created a kind of boundary around the fight.

Interestingly, unlike other fight videos (such as the international fight video found in the search results), no obvious collateral damage occurred in the Australian fight videos. Small children and babies were sometimes fairly close to the action, and parents did not seem concerned that they might get injured. This possibly reinforces the idea that many of these fights were considered to be "good fights", where the rules will be upheld.

As mentioned above, when more than one fight breaks out in a single video, this may represent inter-family hostility, or some kind of inter-group hostility (such as football violence – an almost global phenomenon). These videos were the ones more likely to be represented as "riots" in the media. However, the presence of a large number of spectators can indicate a more controlled type of violence than is the case with a small group. Only fights with 10 or more bystanders were broken up when things got out of hand. Of those with less than 10 bystanders (14 videos), the bystanders did not break up the fight, although injury was not apparent in most of these cases.

3.3.6 Children

In 11 instances, children could be seen filming the fights on cameras, or heard speaking in the background as they filmed on a mobile device. Young people are therefore implicated in the filming of the videos, if not in subsequently posting them on YouTube. Children were present as bystanders in at least 16 of the videos, and in many cases a significant number of children were present.

In some videos it was apparent that children were play-fighting, mimicking the behaviour of the older participants. During our interviews with young people in Community B, one young woman stated that a local man had been organising fights between young people for the purpose of making and distributing videos. While violence is always a learnt behaviour, what is significant here is that the videos themselves are a conduit for this learning process.

3.4 Metadata analysis

By "metadata" we mean information that is found on the social media or video platform, including comments, likes and dislikes, views, and restricted content. Metadata provides some indication of how the videos are received, and how platform governance might work to promote or limit content to audiences (Rieder et al, 2018).

3.4.1 Views

In total, the fight videos had been viewed over 326,000 times (combined total) at the time the analysis took place (in October 2017). The highest-viewed fight video had been watched over 25,000 times by this date, while the average number of views was 7543. Between October and December 2017 (a six-week interval), views of the fight videos (combined total) increased by 14 per cent.

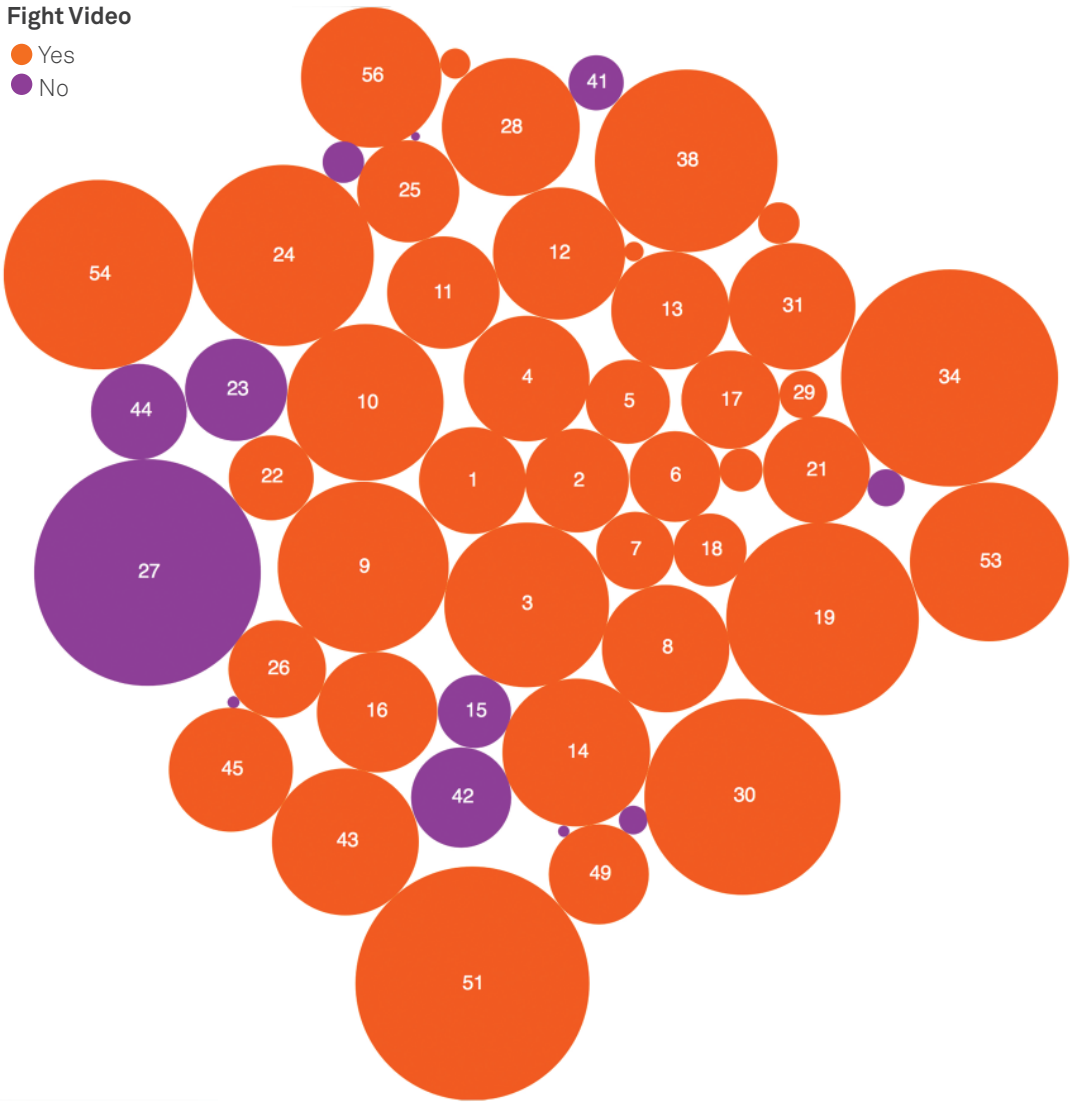
3.4.2 Likes, dislikes and comments

On the day of analysis, the combined total of likes for the 40 fight videos was 303, compared with 115 dislikes. The highest number of likes for a single video was 44, for a video of two young women fighting that was published in mid-2016 (this video also received 20 dislikes). The average number of likes per video was eight, compared with an average of three dislikes.

Only three of the 40 videos we analysed had more dislikes than likes. The comments on one of them suggests this video should not have been posted, as it depicts a particularly violent social breakdown (this video is described in Section 3.3.6), while the other two were probably "disliked" due to the poor quality of the footage. Over half (24 of the 40) of the fight videos had one or more comment, with a combined total of 95 comments. Of the 40 videos we analysed, 16 had no comments, three had 10–13 comments, five had 5–10 comments, and 16 had less than five comments.

The comments fall into three broad categories: hate speech, video quality, and commentary on the fight or the individual fighters. The majority of comments (45) were commentary on the fight or fighters. A typical comment was "[Name] can't stand her ground"; "lol. [Name] got smashed"; or "This is how girls are supposed to fight – no pulling hair" (adapted for ethical reasons). In a comment thread for one video a platform user challenged another user to a confrontation, and the other person accepted the challenge. Comments relating to video quality (6) expressed frustration at poor-quality footage, such as "Why are these all filmed on potatoes?"

Table 4: Data by rank (occurrence in the search), and number of views.



3.4.3 Hate speech

Hate speech was found in the comments section of eight different videos, six of which were fight videos, and two that were not. One video was a music video by a local Aboriginal hip-hop artist and singer, while the other was the tent boxing video. In a few instances, platform users took on the perpetrators of hate speech.

User accounts can also be a vehicle for hate speech. For instance, one account professed to be from an Aboriginal man, but used a derogatory racial term in his account name and offered a "free box of VB" (a brand of beer) to subscribers.

3.4.4 Restricted content

Four videos were restricted as of December 2017. Interestingly, two of these were not restricted when we viewed them in October (at which time they were first and second in the search rankings by relevance), despite both having been uploaded in February 2017. Both were uploaded by same account, and both purported to be from Community B. Another significant similarity is that there were between 30–50 bystanders in each video. In addition, one video had a disclaimer that the audio had been removed due to copyright infringement, which was possibly an automated response (see Section 3.7).

Of the two videos that were already restricted in October 2017, one was from Community B, and the other purportedly from a nearby community. The two videos were published from different accounts. The Community B video depicts an organised fight between teenage girls. The video that purportedly came from the nearby community in fact seems to depict the same fight; it appeared in a different video that was unrestricted, higher up in the rankings, and uploaded by a separate account. The second video was not restricted content, demonstrating the randomness of what is restricted and what is not.

3.5 Playlists

Playlists reveal the social curation efforts of platform users. In some instances, the curation might not be for an audience, but for the curator's own purposes. We observed that some playlists appeared to be gradually built up as repositories of videos for later viewing, much like a collection of bookmarks, as they exhibited clustering around a topic according to the curator's interests at that time.

We analysed 25 playlists, which we sourced by using the same search term used for the content analysis dataset ("Community B fights"), but filtering for playlists only; beyond this, the playlists failed to show fight videos. These 25 playlists contained 3115 videos. Of these 3115 videos, 49 were professional fight videos and around 10 per cent were fight videos from Australian communities and towns. Approximately 70 of the 361 videos referred to Community B.

Analysing the playlists also provided us with some insight into the social curation efforts of the platform itself. The YouTube platform curates its own playlists. These playlists contained fight videos that were in our search dataset. For instance, a playlist titled "popular videos – Community B", made up of 200 videos, contained 21 fight videos from Community B and one from another community in the region.

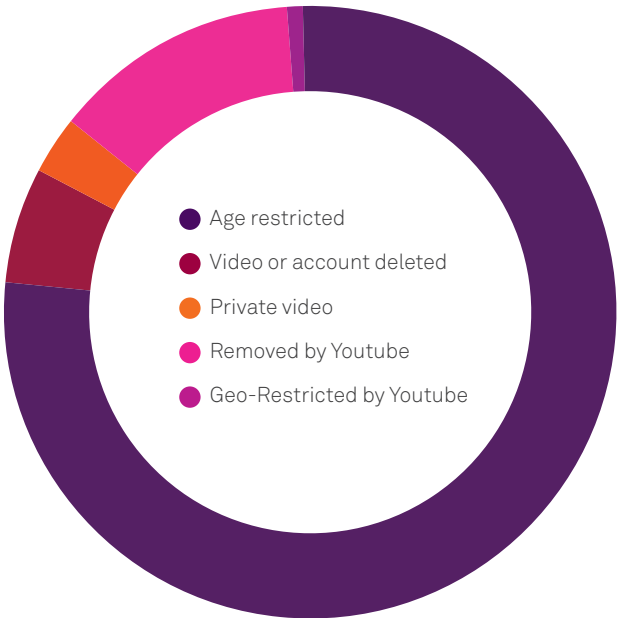
Playlists unintentionally make visible the moderation efforts that occur on the YouTube platform. If a video that has been published directly by a user (not in a playlist) gets removed by YouTube, that video can no longer be seen and leaves no obvious trace. This, however, turns out not to be the case with playlists, where instead a placeholder appears onscreen to indicate where content has been deleted. Due to this platform feature we were able to see that a total of 659 videos (21.6 per cent of the 3115 videos included in the analysed playlists) had been subject to moderation. Table 5 shows that videos are much more likely to be restricted than removed (323 were age restricted; 22 account or video was removed; 13 were private videos; 58 were removed by YouTube; 3 were geo-restricted).

It is important to note that once a video has been removed, we can no longer determine whether it was in fact a fight video. However, the high level of moderation does demonstrate that those curating the playlists had chosen content that went against the platform's Terms of Service, some of which may have been fight videos.

In summary, playlists demonstrate that the fight videos we analysed were being curated in with other content, including fights from other Australian places and overseas. The high number of fight videos from other Australian towns and communities shows that this is a broad phenomenon, rather than being local to the town named in our search term.

This curation of the Australian fight videos may indicate that there is a cultural meme status attached to fight videos, a status that may be international in reach. One theory is that fight videos have an audience that seeks out spectacle and difference, which is not necessarily a local audience. The YouTube platform's own playlists demonstrate that its algorithms are promoting fight videos.

Table 5: Breakdown of restricted and deleted videos by form of moderation



3.6 Violence and Indigenous communities

It has been estimated that Indigenous Australians experience violence at two to five times the rate of other Australians, and possibly at higher rates in some communities (Wills, 2011). The term "lateral violence" is often used to describe infighting amongst members of a particular community, and can include "gossip, jealousy, shaming others, verbal and physical attacks, sabotage and bullying" (Clark, & Augoustinos 2015: 19). As suggested in our Interim Report (Rennie et al, 2016a), violence that occurs as a consequence of online communication meets this definition of lateral violence. Lateral violence is also sometimes discussed in relation to people's power, for example as stemming from frustration and anger in circumstances of marginalisation or oppression (Langton, 1988). As such, the kinds of hate speech identified in this report may be a contributing factor to lateral violence.

Interviewees suggested to us that the fights are usually the result of jealousy, gossip, or long-term family hostilities. It is impossible to confirm this from the videos themselves. What we can say is that these displays of violence are public (particularly when they occur in a group situation), and that the act of filming a fight and posting a video to a public platform was a frequent activity in 2016 and 2017. The high number of fight videos also suggests that fighting has a particular significance for those producing the videos, and possibly for those participating in this form of violence.

Fights have received a significant amount of attention from the field of anthropology, as a window into the role of violence within a social structure. Marcia Langton points out that some of these scholarly accounts are "constrained by prudery" (1988: 202) – told through the lens of a different moral stance. W.E.H. Stanner grappled with this in his 1968 Boyer Lecture, concluding that the Aboriginal approach involved an acceptance of people as aggressive. The ritualisation of fighting was a way to "control, approve and enjoy", and importantly to limit, that aspect of human nature (Stanner, 1968/2009: 209). He also noted that such restraint was abandoned when "passions got out of hand" (201).

Our observation that some fights appeared to be rule-based – in terms of fighting style and location – while others overstepped these boundaries is thus on a trajectory with these anthropological accounts. The presence or absence of bystanders, and the extent to which bystanders intervene, is also a focus of the pre-YouTube studies mentioned above. Gaynor Macdonald, writing of the Wiradjari people in the 1980s, observed that a fight was an event in which the whole community might participate. The presence of spectators who could become protagonists in a fight is noted in many such accounts.

> *A "good fight", as opposed to "fooling round" or "fightin dirty", would take place in an area symbolically set aside from daily living. In the past this would be up at the back gates of the Aboriginal station, known as the mission, or in a clearing by the railway bridge just along from the mission. There are still favoured spots today-near particular street lights, in a natural or created clearing such as a carpark (Macdonald, 1988: 181).*

Moreover, fights are spoken of openly, as though the telling of a fight story is a way to place events in a social order (Burbank, 1994). Victoria Burbank writes: "Whatever people's motives for talking about aggression and for talking about aggression to me, I think it reasonable to say that aggressive interactions generate great interest" (Burbank, 1994: 8). In terms of the fight videos, it is possible that putting fight videos on a public platform such as YouTube is undertaken and accepted in a similar way – if not encouraged, then at least not hidden.

The issue of continuity and change cannot, however, be ignored. While there are clear parallels between the fights featured in anthropological accounts, those earlier stories may reflect social orders that are now under strain. David Martin, writing of the Wik people from Cape York in the 1990s, noted that aggression and violence "may well have resonated with certain deeply sedimented cultural views and practices, but its massive and chronic scale and domination of the social, intellectual and emotional agendas were an entirely contemporary phenomena" (Martin, 1993: 143). Rather than being a continuation of conflict resolution methods, fight videos may be a symptom of the erosion of traditional practices and rules. Or they may have become a cultural meme that responds to the affordances of the technology, a way to build audience, kept alive from outside interest rather than internal group need.

It can be difficult to know from the videos alone whether authority was present during filming – for example, community leaders whose presence may implicitly sanction the fights – or what occurs after the video stops. We therefore refrain from drawing too many connections between fights that have been detailed in historical accounts and those that are now viewable on social media platforms. Moreover, as McFarland (2012) points out, it may be the case that violence occurs more frequently in places where tradition is at risk, where authority does not intervene, and where disputes are not resolved. As young people in the focus group pointed out, disputes continue to replay and even spread on social media, making resolution difficult.

Finally, the fight videos need to be considered beyond the context of the internal group dynamics from which they originate. Fights might be a form of defiance against the white system, in that they represent a refusal to play by imposed laws. The effect of their documentation, however, is increased bureaucracy and policing.

Through their media circulation the fights also become about place, and how a place is perceived by those within the group and those outside of it. Gillian Cowlishaw (2004) has written in detail about how such fights can be misconstrued as riots by the local non-Indigenous population and media. Cowlishaw's work draws attention to the politics of place, and how stigma, status, and power (both Aboriginal and non-Indigenous), not just culture, are part of the story of fights. The hate speech comments on the fight videos are a direct expression of this, in that they represent a racialised form of blame for "ruining" place.

The racialised reception of the fight videos is further highlighted by the presence of the tent fight video in the dataset. The comments on this video contained hate speech against the Aboriginal boxer. Tent fights are glorified, structured performances in their own right (Hooper, 2009; Brophy & Williams, 2014; McLennan, 2007). We stumbled across a documentary series about tent fights on YouTube. The video, from 2008, describes the "end of an era" due to governments in Victoria, Tasmania and New South Wales imposing rules on tent fights, including compulsory use of a boxing ring, and fights occurring only once a month.

In an interview, the so-called last remaining boxing tent owner, Fred Brophy, baulks at the imposition of safety standards: "If I do that they will put me in the same category as professional boxing and it's not, it's a show – it's a side show." He states, "When I go, it's a bit of Australia that's going to go as well" (Overlander.tv, 2008). The documentary claims that tent boxing is an Australian man's rite of passage (women amateur boxers who also participate in Fred Brophy's fights are absent from this account). The cultural history of tent fights in remote Australia may explain the boxing technique adopted by Aboriginal fight video participants. If this is the case, then the videos and the fights themselves sit within a complex cultural history of Indigenous and settler relationships.

3.7 Platform governance

Social media platforms such as Facebook, YouTube, and Twitter provide people with the means to share content, including user-generated content. These platforms allow users a high degree of freedom, and describe themselves as conduits between creators and audiences (Johnson, 2017: 19). However, when content posted to such platforms oversteps moral boundaries, the platforms face criticism from both regulators and users. Platforms therefore attempt to manage the massive volume of content that appears on their sites on a continuous basis, whilst preserving participatory features. For instance, Facebook reviews 6.5 million reports a week relating to potentially fake accounts (Hopkins, 2017), and YouTube "receives 275, 000 flags a day for review across all types of content".[13] In a recent submission to the 2018 Australian Senate Inquiry on cyberbullying and Australian law,[14] Mia Garlick (Facebook Director of Policy, Australia and New Zealand) and Antigone Davis (Facebook Director, Global Safety) wrote that Facebook receives "millions of reports each week" and has "a community operations team working 24/7 to review and action reports as quickly as possible" (Garlick & David, 2017: 3). However, Facebook's moderators are reportedly overwhelmed, and have only 10 seconds to make a decision on whether to ignore, escalate, or delete a post (Hopkins, 2017).

For content such as fight videos, understanding how these governance processes work sheds light on where these videos sit in relation to broader community standards, as well as how they circulate. Furthermore, these videos, and the policies and algorithms that determine their circulation, have become part of a now-widespread concern over the power of platforms in shaping public sentiment, and the social and political consequences that flow from that power.

Platforms manage content by issuing rules that users are expected to abide by. Known as "Terms of Service" or "community standards", these rules typically prohibit the following:

- "Sexual content and pornography
- Representations of violence and obscenity
- Harassment of other users
- Hate speech
- Representations of or promotion of self-harm
- Representations of or promotion of illegal activity, particularly drug use" (Gillespie, 2017: 14).

While these standards are similar across platforms, the consequences of overstepping them are not uniform. Facebook's submission to the Senate Committee did not specifically discuss fight videos, but in responding to one of the Inquiry's terms of reference (the broadcasting of assaults and other crimes via social media platforms)[15] , it did detail the platform's responses to the use of "Live Videos" – content that is filmed and uploaded in real time – in relation to violence. Content that "celebrates or glorifies violence" is removed, and the use of Live Videos to "facilitate criminal activity that causes physical harm to people or animals" is prohibited. If a Live Video is reported and requires an immediate response – for example, if there is "a genuine risk of physical harm or direct threats to public safety" – Facebook will notify law enforcement agencies (Garlick & David, 2017: 9). Neither YouTube nor Google (YouTube's parent company) made a public submission to the Inquiry.

3.7.1 Flagging and reporting

Platforms implement rules using various methods, including: allowing users to flag/report content; enabling community moderation within groups; and employing staff who assess "flags" and take action when they deem content to be inappropriate. In addition, platforms use machine learning and geoblocking or filtering software to identify harmful content, and use algorithms to filter content according to individuals' preferences (Milosevic, 2015).

Again, according to Facebook's 2017 submission to the 2018 Senate Inquiry, "all reports [received by Facebook] are reviewed and actioned by real people, who undergo extensive training when they join, and who are regularly trained and tested beyond this initial training... Given the increasing volume of content being shared (and consequently also reported)... we do use automation to assist our community operations team in implementing our policies and in some limited cases to prevent the resharing of nonviolating content" (Garlick & David, 2017: 3).

The flowcharts overleaf detail the possible outcomes for a reported Facebook post, and draw on Tarleton Gillespie's (2012: n.p.) analysis of a leaked Facebook moderation manual: According to Gillespie (2012), Facebook actively monitors user content (not just content that has been flagged), while YouTube "claim[s] to wait for their users to flag before they weigh in" (np).

Online moderation is not a new phenomenon: it has been occurring since the emergence of early internet discussion lists. What has changed is the scale at which it happens. As the scale of moderation has increased, so too has its opacity. Moderation is generally undertaken by small teams of staff who oversee policy-making and enforcement, and are difficult for users to reach directly. Facebook users, for example, are encouraged to report problematic user behavior, but are not provided with the criteria against which that content is assessed by the platform's moderators (Crawford & Gillespie 2014; Heins, 2014). These assessment criteria can alter based on geographic location.

13 Buskiewicz, Managing Director, DIGI, Committee Hansard, 9 February 2018: 47; as cited in Senate Report, 2018: 54.

14 Senate Inquiry: Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying, 2018.

15 See Senate Report, 2018: 1

Gillespie (2017) identifies two forms of moderation: 1) where users flag, or report, problematic content, which is then forwarded to the platform for a final decision; or 2) where mechanisms are provided for users to rate or block content, which enables the platform to filter "towards those who want to see it, and away from those who don't" (2017: 17–18). For each of these approaches, there are two choices on what then happens to the content in question: either it is deleted, or it is marked as problematic and users are assisted to avoid it (whether through an age restriction, or a warning that the content is sensitive).

Each method has both positives and negatives. Removing problematic content enables a platform to send a particular message to its users: an implicit statement that the platform's managers are decisive, and do not tolerate such content. This can be beneficial from a public relations perspective, in that potential advertisers can avoid association with negative content and/or users. On the other hand, as Gillespie notes, content removal is a "blunt instrument… [that] runs counter to the principles promised… open participation, unencumbered interaction, and the protection of speech" (Gillespie, 2017: 20–1). People who choose to flag content may be politically motivated, or may not understand the context of the post/video. In addition, banning a user doesn't simply curb current behavior; it also bans that user's future posts.

Moreover, content removal can have negative results when carried out in error. For example, in early 2018, a female Aboriginal blogger created a Facebook post with a screenshot of hate speech she had *received*, in order to expose the racism she was being subjected to via the platform. In response, Facebook imposed a temporary ban on her account, as her post was deemed to contravene community standards. She commented on her blog: "Banned. For 3 days. For showing the world the racist hate speech that was levelled at me… This is some Class A victim blaming bullshit" (A Dingo Named Gerald, 2018). In the case of this blogger, it is possible that the post was picked up by an algorithm rather than flagged by another user.

As discussed in Section 3.5, approximately half of the moderated fight videos in the playlists we studied were given an age restriction, rather than being removed. Filtering or restricting who can view particular content is less invasive than removal, but can leave platforms open to criticism for being too permissive, or for encouraging anti-social and harmful actions.

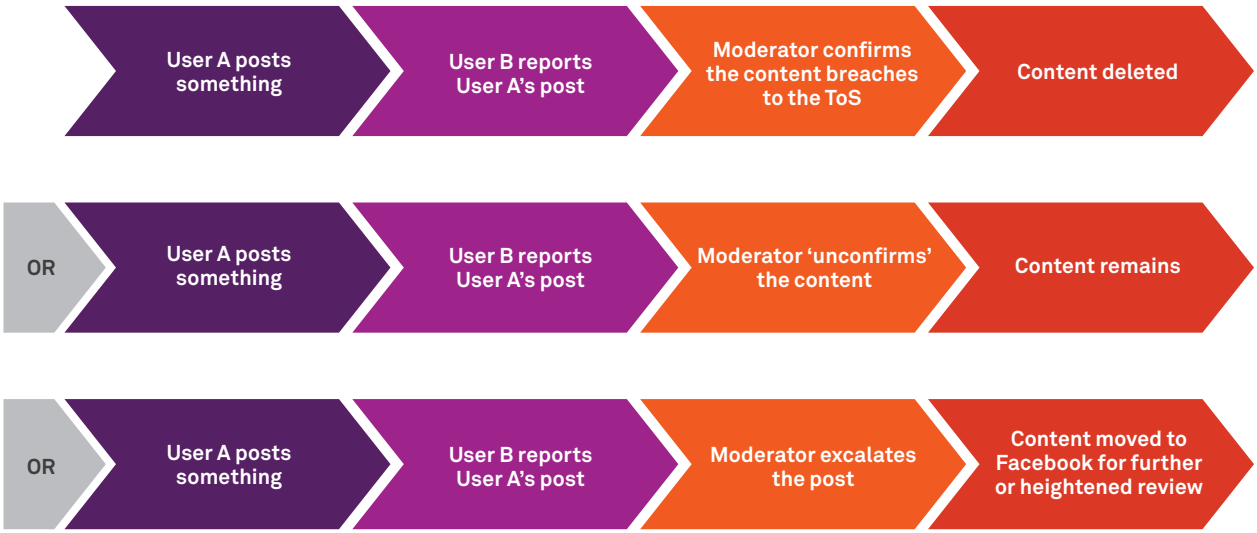
In May 2017, *the Guardian* reported on over 100 leaked training manuals and documents relating to Facebook's moderation processes. The leaked documents revealed the difficult decisions platform staff must make. Moderators' guidelines included the following passage:

> *Videos of violent deaths, while marked as disturbing, do not always have to be deleted because they can help create awareness of issues such as mental illness. Some photos of non-sexual physical abuse and bullying of children do not have to be deleted or "actioned" unless there is a sadistic or celebratory element (Hopkins, 2017).*

The report also revealed that Facebook allows livestreaming of attempts to self-harm because it "doesn't want to censor or punish people in distress" (Hopkins, 2017). Danielle Citron and Helen Norton summarise the dilemma for online platforms:

> *Intermediaries' voluntary actions can educate users about acceptable behaviour. Their inaction in the face of online hate plays a similar role: intermediaries' silence can send a powerful message that targeted group members are second-class citizens (Citron & Norton, 2011: 1441).*

Table 6: Possible Facebook moderation outcomes (as per Gillespie, 2012)



3.7.2 Hate speech moderation

Anat Ben-David and Ariadna Matamoros-Fernandez (2016), in examining the distribution of hate speech on Facebook, trace the platform's definition of hate speech through its Terms of Service. Facebook users, upon signing up to the platform, agree to "not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence" (Facebook, ndb, Section 3, para. 7, cited in Ben-David & Matamoros-Fernandez, 2016: 1168). But Facebook also "distinguishes between humorous and serious speech, and advocates for the freedom to challenge ideas, institutions and practices" (Ben-David & Matamoros-Fernandez, 2016: 1169). For these researchers, this means social media platforms now "define what hate speech is, set the accepted rules of conduct, and act on them" (2016: 1168; see also Citron & Norton, 2011).

3.7.3 Legal contexts

A significant body of legal scholarship and practice has focused on whether and how online platforms should be responsible for content posted by their users. As this literature points out, the Terms of Service for both Facebook and YouTube are inherently connected to US legislation and legal precedent. Other countries, including Australia, have legislated to bring platforms' actions into line with national expectations of acceptability.

In the mid-1990s, US policymakers were struggling with how to regulate illicit content on the internet, including both the users who were posting this content, and the platforms they were posting it to. Increasingly, charges of libel, privacy violation and hate speech were directed at platforms, rather than individuals. In 1996, the *US Communication Decency Act* (CDA) was passed in an attempt to ameliorate emergent problematic digital practices. As a result of the CDA, social media platforms – referred to as digital intermediaries – were granted immunity from civil liability for content published by third parties.

Although the CDA was deemed unconstitutional in 1997, aspects of the law survived. One of these remnants (Section 230), created what is commonly referred to as a "safe harbour", which states that platforms are not liable for the acts of their users, because they are not understood as publishers (Gillespie, 2017; see also Mueller, 2015). This understanding relies on the "content/conduit" distinction in US telecommunications legislation, which distinguishes between publishers who provide information and distributors that circulate information produced by others. As digital intermediaries, online platforms therefore remain statutorily immunised from liability, even if they are notified of potentially problematic content, and/or remove that content (Johnson, 2017: 18; Citron & Norton, 2011). As Tarleton Gillespie (2017) notes, this means that not only are platforms *not* required to intervene, but that if they do, there is no standard "effective policing" that they can be held to (2017: 5-6). Platforms are obliged to remove content only when it infringes on the copyright of others, or where it violates criminal law, including images of child abuse.

Beyond the US context, regulatory frameworks are less lenient. While digital intermediaries have broad immunity in the US, in the EU (along with Russia, and some South American countries) they are offered "conditional liability". This means online platforms are not liable for their users' posts, "as long as they have no 'actual knowledge' of, and did not produce or initiate the illegal or illicit material"; and that they must respond to requests from the government and/or courts to remove particular content (Mackinnon et al, 2015). The UK *Terrorism Act* (2006) requires platforms to comply with a takedown request within two days, or they are deemed to have endorsed that content (Gillespie, 2017: 9–10). In China and some Middle Eastern countries, online platforms are subject to "strict liability", which requires companies like YouTube to "prevent the circulation of illicit or unlawful content... [by] removing or censoring, often in direct cooperation with the government" (MacKinnon et al, 2015: 50). In addition, some nations, including several in sub-Saharan Africa, have "not instituted laws articulating the responsibilities of Internet intermediaries in any form, leaving intermediaries there uncertain about what they might or might not be liable for" (Gillespie, 2017: 6–7).

While the way social media platforms operate is influenced by government laws and policies, some scholars see this as impinging on their duty to protect freedom of expression, including Article 19 of the *UN Declaration of Human Rights*, and the 2012 resolution that offline rights should also be protected online. For example, states can require digital intermediaries to hand over users' data for the purposes of surveillance. Platforms do not necessarily report transparently on how they respond to government or corporate requests, let alone make public their own internal decision-making around Terms of Service issues (Mackinnon et al, 2015).

In Australia, the *Enhancing Online Safety Act* (2015) was created to establish a complaints mechanism for Australian children experiencing serious cyberbullying, and gives the eSafety Commissioner the power to investigate such complaints (Office of the eSafety Commissioner, n.d.-a). As a result of the Act, the eSafety Commissioner may issue a notice to a social media service requesting or requiring that the service remove the material. The Commissioner may also issue an end-user notice to an individual who posts cyberbullying material, requesting that the material be taken down; that the person desist from cyberbullying activity; and/or that the person apologise to the child who was targeted (for further information, see Office of the eSafety Commissioner, n.d.-b; Office of the eSafety Commissioner, n.d.-c). The Commissioner has a range of enforcement powers for dealing with non-compliance, including issuing formal warnings, accepting enforceable undertakings, and seeking injunctions. With its focus on education and awareness raising, the Commissioner may also work with schools, parents, and the police to stop cyberbullying. The Commissioner also administers the Online Content Scheme (*Broadcasting Services Act 1992*, schedules 5 and 7), which is designed to protect consumers, particularly children, from harmful and inappropriate material through a complaints-based mechanism for illegal and offensive online content (child sexual abuse material is illegal in Australia, and is dealt with by the eSafety Commissioner in collaboration with law enforcement agencies and the global network INHOPE). The eSafety Commissioner thus acts as a "safety net when a social media services [sic] does not consider a report made to them under their reporting tool to amount to a breach of their terms of use" (Office of the eSafety Commissioner, n.d.-d: 7).

The Senate Report (2018) on the *Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying* was released on 28 March 2018. The E-Safety Commissioner expanded on the role outlined above stating that: "... report[ing] to the social media sites... [is] the most expeditious way of getting [content removed]. But if the content doesn't come down within 48 hours, [people] can come to us... A lot of the moderators, depending on the platform, may have 30 seconds or a minute to look at the reports as they come in. They're dealing with huge volumes and they often miss context."[16]

Details from the Senate Report (2018), and from submissions to the Inquiry preceding it, have been cited throughout this section. While the report acknowledges that Aboriginal and Torres Strait Islander people are particularly likely to experience technology-facilitated abuse,[17] little detail is provided as to how this can differ from other contexts.

3.8 Mainstream media ethics

Finally, ethical reporting by news outlets might help address the wider community perceptions and reactions to the fight videos, including hate speech. One outlet published an article about a Facebook page that was being used to share fight videos, drawing attention to the fight videos and associated hate speech on the news outlet's own Facebook page.[18] An article in the same publication in April 2017 stated that young women were involved in "brutal street fights" while dozens of bystanders cheered from the sidelines. Earlier this year, a different publication recycled these concerns, reporting them alongside articles about a recent child abuse case and questioning tourism funding for the town.

The articles were problematic on a number of levels: first, all three either linked to or auto-played fight videos while purporting to discourage their circulation. Reporters discussed the fights as being akin to riots or gang behaviour, with one journalist seemingly questioning government investment in the town. Followers of one outlet's Facebook page posted hate speech on the page – proof that the articles were themselves guilty of inciting a form of violence. These incidents highlight that the issue of fight videos is not simply a "problem" caused by Aboriginal people in remote communities, but one that involves inter-racial assumptions, media moral panic, and platform governance.

16 Inman Grant, eSafety Commissioner, Committee Hansard, 9 February 2018: 62; as cited in Senate Report, 2018: 47.

17 Queensland Family and Child Commission, Submission 8: 2–3; as cited in Senate Report, 2018: 15; Australian Women Against Violence Alliance, Submission 14: 2; as cited in Senate Report, 2018: 24, 36; eSafety Office, correspondence received 23 March 2018: 4; as cited in Senate Report, 2018: 49.

18 These articles have not been named, or cited, for ethical reasons.

Part 4: Responses

4.1 Individual responses to online harms

In the first stage of the project, we asked 22 participants if they knew how to block or report other people on social media. Most responded that they did know how to block or report (73 per cent). We then asked who they would approach for help if there were "troubles in your community caused by Facebook/Divas Chat/WhatsApp etc." Possibly due to the wording of the question, no participants responded that they would contact the platforms (through flagging/reporting) or the eSafety Commissioner. Responses, in order of frequency, included approaching Elders (or another family authority), police, teachers, attempting to sort it out directly ("myself"), and lawyers. However, one participant suggested that a local "phone department" was necessary and described a hypothetical authority with responsibilities not unlike those of the Office of the eSafety Commissioner:

> *To help people, to teach them how to face things if they come across bad things on the internet, and 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.*

Some young people from Community B said they would block people on social media. One man stated, "I block stupid people that friend you and then write stupid things on your profile." When asked what they would advise other people to do if they were being bullied, one man responded that he would advise them to "report them [the bully] to the police." A young woman replied that she would intervene herself, as "I don't think the police will do anything if you are being bullied on Facebook and AirG." Again, people did not speak about reporting incidents to the Office of the eSafety Commissioner unless prompted.

In March 2018, Telstra commissioned a survey of residents of Ali Curung, in the Barkly region of the Northern Territory (NT), as part of the Australian Digital Inclusion Index. Of those who stated that they identified as Aboriginal or Torres Strait Islander, and who had used the internet in the past three months (93 participants), over half had used Facebook in the past four weeks (55 per cent), and a third had used AirG (35 per cent). A smaller number of participants had used Snapchat (12 per cent, mostly young people) and "other" social media (5 per cent). We requested to add an additional question to the survey for the purposes of this project: "Have you ever reported inappropriate content that you've seen on social media (for instance, using the "report" function on Facebook, or the "flag" function on YouTube, or contacting the eSafety Commissioner)?" Only 17 per cent of those who had used the internet in the past three months said they had reported inappropriate content. It is difficult to know whether this data represents particularly low or high reporting rates. A number of submissions to the 2018 Senate Inquiry requested that platforms such as Facebook and Instagram provide data on reporting trends. However, those platforms responded by saying that while they "understand the rationale behind requests...to provide more detail around the data showing reporting trends...unfortunately, at this stage, we are not able to do so".[19]

4.2 Digital literacy and financial literacy programs

A number of older people told us they lacked the skills to use online platforms, and that they needed these skills in order to guide young people towards appropriate use. A young woman in Community B made the point that in most cases conflict management only occurred after physical fights broke out, because Elders are not aware of what's happening on social media:

> *Some Elders they don't go on AirG [...] they don't know how to use a mobile phone or Facebook – some do, some don't.*

Older people are also vulnerable to others misusing their mobile phones. While it was not the intention of our research to evaluate digital literacy programs, we do see value in programs such as those being run through the Indigenous Knowledge Centres in Queensland (State Library of Queensland, with support from Telstra). The importance of these programs is not just in the basic skills they teach; they can also help Elders and parents feel confident in recognising and dealing with cyber safety problems if and when they arise.

Financial literacy training in remote communities and towns is also important. Being alert to scams, keeping online banking passwords safe, being aware of apps and services that incur additional costs (such as 1800MumDad, discussed below) and phone credit transfers all involve financial literacy, alongside digital literacy. While such training programs are key, the social concerns raised in this report cannot always be addressed through digital skills alone. For example, a group of young people in their 20s told us some parents were buying devices for young kids, and that kids were using these devices to set up social media profiles at a young age (Facebook, AirG and Snapchat). Participants viewed this as a symptom of poor parenting behaviours in families that were experiencing multiple challenges, which suggests that digital literacy programs would not necessarily address the issue. Such concerns are clearly not unique to Aboriginal communities.

4.3 Awareness raising

There is an ongoing need to raise awareness of privacy and other common cyber safety issues, such as image-based abuse and cyber-bullying. One older man suggested that written materials would not work due to poor English literacy in his community. He suggested that a loudspeaker was the best approach:

> *What I really believe in we should be getting a hailer going around, somebody should be speaking from hailer that everyone can hear... If we have a loudspeaker, yes, driving around the community and someone, Elders or leaders, giving the information, like strong information and pass the message on to the younger ones.*

While the practicality and desirability of a loudspeaker is debateable, the idea of getting the message out is important. Indigenous media organisations exist to enable communities to share information in ways appropriate to them. A survey by McNair Ingenuity Research and IRCA found that while Indigenous

19 Facebook and Instagram, answers to questions on notice, 9 February 2018: 2 & 3; as cited in Senate Report, 2018: 53.

Australians living in urban and regional areas prefer to use the internet to find government information, those in remote areas prefer to receive such information from their local community radio station (35 per cent preferred radio, while 17 per cent preferred internet), and that nationwide, the main reason for listening to Indigenous radio (61 per cent) was "to hear about my own people and my own community" (McNair & IRCA, 2016).

As a final stage in this project, we commissioned four Indigenous media organisations to produce content on cyber safety themes for broadcast via Indigenous radio networks, and for downloading via podcast apps. We encouraged them to produce stories, rather than community announcements, in order to provoke discussion in communities on what can be complex issues. As we identify in Section 1.4, phones are a grey area in terms of what is shared and with whom. The subtleties of media practices around privacy, including how people respond to demands from others, are in flux. Moreover, the content people share online can go against cultural protocols. Communities need to find a way through these issues on their own terms.

During the latter stages of the project, a cyber safety awareness campaign was produced by the Pitjantjatjara Yankunytjatjara (PY) Media team, "through the Department of the Prime Minister and Cabinet, APY Schools, Telstra, NBN Co., [and] AFP" (PY Media, 2016). With Telstra's mobile network and the NBN being rolled out across the Anangu Pitjantjatara Yankunytjatjara (APY) Lands, the campaign was designed to "ensure information is available and accessible for all people from APY about how to be safe online" (PY Media, 2016). The multimedia resources have been developed in Pitjantjatjara and Yankunytjatjara and cover topics such as cyberbullying, sexting, and the concept of a digital footprint (PY Media, 2016).

4.4 Telecommunications products and services

Our research has focused on how people's practices in using devices and social media platforms relate to their social obligations, and how this can sometimes lead to negative outcomes for individuals and communities. Another aspect is the choices people make, both in their online conduct, and in the platforms and products they use. There is some scope for communications companies to intervene in the problems we have identified through the products and choices they offer.

4.4.1 Third-party apps and reverse charge calls

In December 2017 Telstra terminated Premium Direct Billing, for third party services that are not provided by Telstra, as a consumer protection measure. However, some services were not removed, including AirG VIP.[20]

As discussed in our Interim Report (Rennie et al, 2016a), we found that AirG VIP dominated social media usage in Indigenous communities, and was described as a primary vehicle for cyberbullying, harassment, and conflict. In response to concerns that people thought the service was free, AirG made a number of enhancements, including reducing the no-credit grace period, and becoming a social media partner with the eSafety Commission. These responses were designed to discourage use of the service, rather than remove it.

We were unsuccessful in attempting to measure the impact and awareness of reducing the AirG VIP no-credit grace period (see Part 5 of this report). Our qualitative evidence suggests that Air G/Divas Chat may cause harms beyond financial distress, in particular because children considered it to be an unregulated platform that enables anonymous and problematic behaviour.

Another service that is creating difficulties for people is called 1800MumDad. The "collect call" style service charges a minimum of $6.60 for a 60 second phone call to the person who receives the call, charged as a Premium SMS product. One woman told us that people use the service when they run out of credit, which puts the financial burden on the person they are calling. She estimated that "ten per cent say yes" and choose to receive the incoming call, and believed that people were increasingly refusing to accept the calls.

The woman's concern reflects the fact that reverse call services are a greater burden among social networks where community obligations are strong. She also stated that some people are savvy about knowing when to ask for credit:

> *If someone sees you on Facebook, like online, like "Oh she's online, he's online", they inbox the person – "Can I get credit off you? Just three dollar." Yeah people ask around, even text.*

The 1800MumDad service also offers a product called I'll Pay, which it describes itself as being for when "you are out of credit and the person you want to call either can't or won't pay for the reverse charge call". The I'll Pay product allows the caller to pay $6.60 for up to 300 seconds, charged via Premium SMS, to be paid at a later date. The I'll Pay service is not available to Telstra or Optus customers.

4.4.2 Other products

During an interview in Cape York, one woman mentioned that she switched providers after reading an advertisement. She discovered that an unexpected benefit of switching to this provider was that it did not have a feature to transfer credit from one account to another. When people asked her for credit, she was able to tell them that she could not transfer credit:

> **Interviewer:** *You get much people hassle you for like "Ah, sissi, give me credit. You got phone"?*
>
> **Participant 4:** *Nah, I just tell them I got boosim. I got boosim. Cos you can't transfer credit with boosim.*
>
> **Interviewer:** *What's [boosim]?*
>
> **Participant 4:** *Boost. Yeah. Boost them phones here, and then these sorta SIM cards you can't transfer credit. Telstra you can, but not these.*

A contact in Central Australia mentioned that this same provider does not have a third party agreement with AirG (whereby subscription is deducted from the user's pre-paid credit), making it more difficult for young people to sign up for the service. Other providers may wish to consider products that achieve these outcomes.

20 Only third party (non-Telstra) services and subscriptions were impacted by Telstra's termination of Premium Direct Billing.

4.4.3 Wi-Fi "kill switch"

As we discussed in our Interim Report (Rennie et al, 2016a), cyber safety in remote Aboriginal communities is inseparable from digital inclusion. 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.

Our research found that some communities have chosen to go without mobile infrastructure in order to avoid cyber safety problems that have arisen elsewhere (see, for example, the experience of Canteen Creek outlined in our 2016 Interim Report, as well as Papunya's deliberations on this issue in Hogan et al, 2013). Other communities, which do have access to digital infrastructure, are choosing instead to use Wi-Fi filters. Others are resorting to temporary Wi-Fi blackouts when inappropriate use occurs (McFarland & Iten, 2016). Such Wi-Fi management strategies – referred to colloquially as a "kill switch" – are sometimes implemented by communities themselves, and in other instances managed by external agencies with the community's permission (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 a growing number of services are moving online. The benefits of mobile phones and internet that participants identified in our Interim Report (Rennie et al, 2016) – 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 live remotely, for whom the face-to-face alternatives are costly and time-consuming.

Further, such mechanisms 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). Not only is banning and prohibiting underage mobile phone and social media use not a particularly manageable solution in towns and cities, but it also has the additional drawback of restricting opportunities for young people to develop digital literacy, especially those living in disadvantaged areas.

4.5 Mediation and conflict management

There was agreement among interviewees that conflict management is important. People discussed organised processes to diffuse disputes, or in some cases to reprimand people who have instigated problematic communication online. The word "mediation" was used, but this seemed to encompass a variety of approaches. Conflict resolution (or conflict management) in remote communities can be provided through traditional structures, by Indigenous organisations, or through mainstream legal services (NADRAC, 2006; Kelly, 2002). A young woman in Community B commented that an effective strategy is to bring Elders in to talk directly to perpetrators:

> *They need an Elder to stand up and speak to them so it doesn't have to go all over on AirG and Facebook and all that.*

In Community A we heard similar suggestions. A man who is himself a senior community member (Participant 3) talked about how they had dealt with conflict caused on social media:

> *We come together, the Elders, and say that's enough. Now it can really cause big problem, you know, misusing the phone, you know if you talk to someone, ah, you need to talk, ah, in a polite manner. And respect [...] But in the past it might, you know, we came together and said family group meeting, you know, warn them not to do that again.*

He explained that while there had been problems in the past, "now we have mediations. Though the mediation really works. And you know it stops that happening." However, he also stressed that parents need to take responsibility and remind young people to behave responsibly. Another man said he mediates within his own family, and suggests that they leave town to cool down:

> *If we all, like, my family, fight fight fight, I tell them now, fwshhht! [...] Me, I tell them, I, come on, we gotta have mediation us-mob only. Talk about that what, sshhwt, which-way this town here? We leave this town for a while? Like that see, bang! Take them out [of the community].*

One woman also spoke of taking young people to their outstation if they had been misbehaving online. These strategies, akin to an enforced digital detox, draw on traditional methods of creating community stability:

> **Participant 1:** *Last month this one fella he was in that big fight last year and they told him he's not allowed to stay in town for a month, so the families took him to beach and he was staying there.*
>
> **Interviewer:** *So they take someone, just leave him there like just on his own, or other people stop with him?*
>
> **Participant 1:** *Nah the families go with him. And he can just come to the landing, not come into town. Til it's finish.*

She said this was not as severe a punishment as some traditional strategies for dealing with misbehaviour (including the perpetrator being made to stand in a tree containing an ant nest), but she still considered it to be effective. The responses suggest that "mediation" is occurring within families. However, traditional practices have weakened over time, and external services are often called in to help manage conflict. As one report points out, reliance on these services may further weaken such authority, unless Elders are involved in the design and development of those services (NADRAC, 2006: 6).

Some of the youth focus group participants we spoke to suggested that the best way to de-escalate fights is for Elders from relevant family groups to undertake mediation. This approach recognises that community authority remains an important ongoing tactic in dispute resolution; the role may include handing out punishments, such as insisting that a perpetrator be removed from town for a time. However, this approach requires sufficient resourcing. Workers in Indigenous services told us that the decline (or in some cases complete removal) of funding for organisations that coordinate Elder meetings was preventing timely dispute mediation, and could be reducing Elders' own sense of efficacy in such matters.

Some of the conflicts people mentioned in relation to social media involved couples. In situations of family violence, mediation is not appropriate; people who have less power should not be made to negotiate with those inflicting violence on them (Kelly, 2002: 9). Mediation "does not identify a 'wrong-doer' per se, and mediators do not make a judgment on who is right or wrong: we assist the parties in finding 'common ground'" (Kelly, 2002: 9).

For bigger disputes that might otherwise end up in the court system, youth justice and other legal organisations are being called upon to assist. While we heard that social media communication is often raised during mediation processes, gaining access to mediation records (and interpreting these) was beyond the scope of our project. Further investigation from Aboriginal justice experts, including case studies into how mediation is helping to manage conflict, would be beneficial.

4.6 Trusted flaggers

Recent developments in "flagging" practices have seen some platforms engaging "trusted" or "super" flaggers: users who might be affiliated with "law enforcement organisations, activist organisations concerned with a specific kind of violation or protecting a specific population of users, or long time users who are recognized as reliable" (Gillespie, 2017: 19). Content that is flagged by super flaggers is given priority by online platforms. A report by the Women, Action and the Media (WAM! See Matias et al, 2015) describes the experience of being an "authorized reporter" on the Twitter platform. Over a three-week period, WAM! reviewers "assessed 811 incoming reports of harassment and escalated 161 reports to Twitter, ultimately seeing Twitter carry out 70 account suspensions, 18 warnings, and one deleted account" (Matias et al, 2015: ii).

As WAM! points out, super flaggers have a better understanding of the context and challenges of posts, and are therefore likely to make better decisions than other moderators. Given that there are cultural sensitivities involved, such a method would be an appropriate means of approaching fight video moderation. However, while this practice might increase efficacy and help ensure that marginalised communities are protected on these platforms, implementation puts the burden on those who sign up for the role (Matias et al, 2015).

Part 5: Cyber safety research in remote communities: considerations for methods

During the project's latter stages, Telstra requested that we conduct a survey of service providers about the use of digital media, cyber safety concerns, and the intersection of these practices with particular platforms (if any). For a variety of reasons, this was not successful. In this section, we discuss why this was the case, and refer to existing literature that details similar barriers in similar contexts.

Much has been written about conducting research in Indigenous communities, particularly remote Indigenous contexts. These discussions often centre around questions of ethical engagement. As Holmes and colleagues (2002) note, research with Indigenous communities requires standard research methods to be applied with cultural sensitivity (Holmes et al, 2002: 1268; as cited in de Crespigny et al, 2004: 8). For Aileen Moreton-Robinson (2013), drawing on Rigney (1999) and Smith (1999), this means any research undertaken has to be of benefit to the community, conducted *with* them (rather than "on" them), and the community's needs and interests must be prioritised (2013: 336).

Flowing from such discussions, a common research practice is to hire and train local researchers, a measure designed to ensure local voices are privileged in both data collection and research outcomes (Osborne, 2016: 46; see also Putt, 2013: 5).[21] While this is undoubtedly best practice, this method is difficult to scale up to multi-community studies. In other contexts, surveys (whether conducted by phone or in person) might be usefully deployed to gather such broad-based data. But in remote Indigenous communities, survey delivery confronts many of the same barriers to engagement described above (Lee et al, 2014: 466-7). While such measures as using plain English, or translating surveys into the relevant Indigenous language (Lee et al, 2009; Lee et al, 2008), or hiring local researchers (Gray et al, 1997) might provide solutions, these approaches can be unviable for a variety of reasons (such as time, cost, and geographical distance). Accordingly, for research in remote communities, both survey design and modes of delivery are affected by *interpersonal* and *infrastructural* dimensions.

5.1 Designing surveys, acknowledging interpersonal dimensions

One approach to overcoming the difficulties associated with survey delivery in remote Indigenous contexts is to adapt existing surveys (Osborne 2016: 50). For example, ABS surveys such as NATSISS have questions that "are asked slightly differently in remote and non-remote contexts" (Australian Bureau of Statistics, 2010; as cited in Putt, 2013: 4). But while this might result in more successful engagement, Osborne (2016) suggests that survey questions, by "presenting a statement and seeking to elicit a response" (2016: 54), can result in "gratuitous concurrence" (Liberman, 1980). This is a behavioural pattern "where Indigenous peoples tend to honour and manage relationships by seeking to mirror the assumptions and values of others in dialogue" (Osborne, 2016: 53; Foster et al, 2005, 9–10; see also Campbell et al, 2017: 19 for a discussion of similar dynamics in small group workshops).

Accordingly, Osborne (2016) suggests that in remote Indigenous contexts, surveys are more effective when open questions are used, rather than closed questions, and when the survey itself is conducted in informal settings (2016: 54). This is reiterated by the Centre for Appropriate Technology, which argues that:

> *Semi-structured interview questions that focused on residents' perceptions and experience[s]... [were better able to] accommodate the various cultural protocols and language differences that were involved in varying and unpredictable degrees* (2013: 24).

The Tangentyere Council Research Hub offers useful case studies for putting this approach into practice. The research team use existing surveys to develop their own, so that results are comparable, but questions are tailored to their audience. For example, questions are kept short, and the survey form itself is designed to require minimal writing by both interviewer and interviewee (Foster et al, 2006: 215).

The Tangentyere Council Research Hub also suggests that beyond issues of adapting or reinterpreting existing surveys, the mode of survey delivery also need to be considered. The Hub argues that conducting research (including survey delivery), specifically with Town Camp communities, takes time, and requires that people are "on the ground" and "in community":

> *To ensure good participation, we had to let everyone know that the survey was being conducted. We explained to the Tangentyere Executive and staff what we were planning to do, and asked them to pass on the information to people in the Camps. One week before the survey was due to start, we also asked Tangentyere Council housing property management officers to distribute flyers in the Camps advertising the survey, and we went to each camp and explained to people when we were coming and why. This is very important for Town Campers, because they have had negative experiences with research before and we needed to explain that we were going to do the work* (Foster et al, 2006: 215).

However, as noted above, when large-scale, multi-community data is required, being "on the ground" is often not possible. As such, survey delivery methods conducted "from a distance" – such as over the phone – need to be considered.

5.2 Delivering surveys, addressing infrastructural dimensions

In remote Australia, infrastructural dimensions such as the digital divide further complicate survey delivery. This has long been acknowledged: in 2006, the Tangentyere Council Research Hub argued that phone-based survey delivery was inadequate for gathering data from Town Camp residents, because over 90 per cent of them did not own a telephone, so would not be able to receive the phone call, let alone complete the survey (Foster et al, 2006: 214).

21 Although a step towards ethical engagement, hiring local researchers remains difficult. Barriers include developing and maintaining relationships, initiating and providing ongoing training, as well as supporting and remaining flexible around existing responsibilities (de Crespigny, et al, 2004: 11). Further, while they often gain greater access than external researchers might, local researchers can confront issues of "inter-family and inter-community confidentiality", whereby potential research participants might be reluctant to engage due to familial or community connections or conflict (de Crespigny, et al, 2004: 11).

Instead, the Hub advocates for a face-to-face survey delivery method that deploys broad, open-ended questions (as noted above). Given that the aim of our survey was to detail experiences across the entire Northern Territory, it was not possible to be on the ground in every community. Instead, we devised the following method, which sought to acknowledge and overcome the interpersonal and infrastructural dimensions discussed above.

5.3 Method

Initially, we aimed to collect data from as many remote Northern Territory communities as possible. We therefore tested the feasibility of a phone survey.

Acknowledging both the Tangentyere Council Research Hub's reminder that phone-based survey delivery can exclude many remote Indigenous households, and keeping in mind the interpersonal barriers discussed above, we decided to direct surveys to remote community service delivery points, such as health services, rather than to individuals. The logic underpinning this decision was that the people working in these organisations (whether Indigenous or not) were "on the ground" in the community, and likely in a position to make observations on cyber safety issues. These organisations were also more likely to have access to a phone that we could call. We also drew on our experience from the 2016 iteration of the research (see Rennie et al, 2016a), where we found that some people were unwilling to admit to using certain platforms or practices when asked directly. However, when asked to observe others, people were more willing to speak candidly.

We developed an exhaustive list of remote community services whereby (a) residents were likely to access or use the internet or digital devices, and (b) the services were likely to interface with the results of internet or digital device use. This resulted in >300 organisations across the following sectors:

- Aboriginal art centres;
- Aboriginal drug and alcohol rehabilitation services;
- Aboriginal health organisations;
- Aboriginal legal organisations;
- Aboriginal media organisations;
- Northern Territory legal organisations;
- regional councils;
- local authorities;
- Northern Territory libraries;
- Northern Territory Council of Social Services (NTCOSS) community networks; and
- remote health services.

These organisations were then mapped, and mobile phone access data overlaid, to ensure we would only contact service providers in communities with residents who were readily able to use the internet.

5.4 Survey delivery in practice

Having designed the survey and developed a list of contacts, we began making calls. We had little initial success. Health services were displeased to receive research-oriented calls, telling us they were too busy providing medical services. Council services and art centres were often unavailable to talk – although staff regularly suggested we "call back another time". Libraries were open for only brief periods, so staff were reluctant to spend their opening hours on the phone. This pattern matches our previous experiences of working in remote communities: people are incredibly busy, and often require multiple points of contact before a conversation can be established. According to the Centre for Appropriate Technology, residents of remote communities often experience "research fatigue" (2013: 30), due to the number of projects conducted in such locations. It seems likely that this was a factor.

Given the low success rate, we changed our approach. Eschewing the list of service providers, we reached out directly to members of our reference committee. Members were invited to complete the survey based on their own experiences (either over the phone, or online via Qualtrics). We also encouraged them to pass the survey on to people they might know who had the necessary expertise and experience to comment on the topic. While we received a small number of responses and people were generally willing to assist, the numbers were too low to fulfil the research objective, and we abandoned the exercise.

5.5 Summary

Although our survey method failed to gather the required data, the process resulted in a number of learnings that we hope will assist in future phone-based survey delivery in remote indigenous contexts.

Surveys are difficult to deploy in remote communities. This is due to both interpersonal dimensions (such as language and cultural barriers), and infrastructural dimensions (such as the digital divide). By reviewing the existing literature, we sought to identify these issues, and work around them. One strategy we tried was to target local service providers, rather than individuals. While this arguably resolved some of the infrastructural barriers (in that most service providers had phones we could call, even if they weren't always answered), interpersonal barriers remained (such as work commitments, and hierarchical responsibilities). We found that leveraging existing relationships through our reference committee members was most useful, but still did not produce a large number of responses.

Conclusion

In many respects, the networked nature of Aboriginal sociality accords with social media platforms. Activities such as receiving information, organising logistics, and staying in touch with family – particularly when people change phone numbers frequently – are easily done via social media. However, things can go wrong, and in ways not entirely explained by typical definitions of cyber safety.

Discords and difficulties arise when platform settings don't accommodate certain aspects of sociality. In this report we have focused on two crucial debates in technology/internet studies – privacy and governance – in relation to Indigenous knowledge systems. In doing so, we acknowledge that these are challenges for society in general, but they can manifest in unique ways in Aboriginal communities.

In remote Aboriginal communities, privacy breaches can have serious consequences, including post-hoc destruction of devices and closure of accounts, as well as physical violence. The frequency and nature of these events suggests that users have abandoned the preemptory tools the technology offers for boundary management.

In this context, the preference for mobile devices and the conveniences of social media platforms go hand-in-hand with specific privacy-related ordeals, including identity violations and unauthorised access to financial accounts. In response, some individuals are choosing to avoid using certain 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 are choosing to shut down public Wi-Fi when fights occur. The subtle dynamics of boundary work, as well as the less subtle top-down responses, therefore result in material and informational exclusions for some community members.

Physical conflict can be a reassertion of relatedness, even where it may fail to reinstate social order and may in fact have the opposite effect. In both communities where the research took place, participants favored mediation as a strategy when conflict arose, and suggested there was a need to develop protocols around device use that correspond with cultural obligations. Technology companies could consider ways to build these ideas of accountability into platforms – ways to heighten relatedness through visible place-based protocols. However, this raises the question of whether systems based on an understanding of relatedness are possible under contemporary market and legal regimes.

Online platforms institute sociotechnical regimes that guide user behavior; scholars call this "platform governance". These regimes are based on US notions of free speech, which can limit community moderation possibilities. In addition, platforms are not transparent in how they decide which content to delete, and which to leave be. In the case of fight videos, we have shown that audiences could interpret the content in multiple ways, ranging from sport to social dysfunction. Due to such ambiguities, online platforms are unlikely to make a ruling on these videos. Some strategies, including "trusted flaggers", may provide a way forward, but this response requires that organisations devote time and resources to this work.

Not all of the issues we identified are unique to Aboriginal communities. Some can be addressed through consumer awareness and education programs (for example, teaching people how to avoid scams). There is still a need for programs that address online behaviours and digital literacy.

We have also seen positive developments, such as providers changing or removing Premium Direct Billing services. As these instances demonstrate, cyber safety is an issue that extends beyond the consideration of individual capacities. Understanding the ways in which platform governance intersects with Indigenous governance will need to be an ongoing effort.

Acknowledgements

We thank the Elders and study participants for their contribution to the research, and for allowing us on to their land. This project has been conducted in stages, and across vast distances. We would like to acknowledge the following people and organisations. Without their assistance, the project would not have been possible.

The first stage of the research, which is covered in our 2016 report, was conducted in Central Australia. Eleanor Hogan was a chief investigator for the project's first stage, and we are indebted to her work in establishing the project. Identifying the communities that might participate in the project, and securing their consent, was a complex process. We relied on Reference Group members to suggest potential sites, and on 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.

During the first stage of the research (see Rennie et al, 2016a), 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.

The second phase of the research, which is covered in this 2018 report, was conducted over two trips: one to a location in far north Queensland, the other to a location in central Australia. Tyson Yunkaporta was brought onto the project at this stage as a chief investigator. For the research conducted in Queensland, we would like to thank the local Council and community (who chose not to be named) for their willingness to be involved. For the research conducted in Central Australia, we would like to thank the local community and support services for their willingness to be involved.

Thanks to Lesley Acres from the State Library of Queensland and Nicholas Suzor for participating in the podcast output. We would especially like to thank David Stanley from RMIT's media department for his help with sourcing the equipment (and teaching us how to use it). Thank you also to Camilla Hannan and James Milsom from Audiocraft for their production work on the RMIT podcast.

This project was supported by a number of individual researchers, each coming into and out of the research at various points. A special thanks to Chris Wilson for his efforts on designing the survey despite the many difficulties we faced, and to Yee Man Louie for her work in delivering it. Thank you also to Sam Kininmonth for his work documenting the fight videos found in YouTube playlists.

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 eSafety Commissioner; Indigenous Remote Communications Association (IRCA); Northern Territory Community Justice Centre; Northern Territory Legal Aid Commission; Red Cross Youth Leadership Group; Papulu Apparr-Kari Language Centre; and Piliyintinji-ki Stronger Families.

The Reference Group provides 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 to share 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 ethical and culturally appropriate ways, particularly concerning cultural protocols relating to remote Aboriginal families and communities, and any potentially sensitive local issues. The project included consultations with a range of individual stakeholders, including some people from the Reference Group. In addition to the reference committee, Nancie-Lee Robinson and Mark Sulikowski from Telstra participated in project management meetings.

References

A Dingo named Gerald (2018). *Banned. Again.* Retrieved 17 February 2018, from https://adingonamedgerald.wordpress.com/2018/02/01/banned-again

Altman, I. (1977). Privacy Regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3), 66–84.

Australian Human Rights and Equal Opportunity Commission (2003). *Social Justice Report 2003*, Commonwealth of Australia. Retrieved 21 June 2016, from https://www.humanrights.gov.au/our-work/aboriginal-and-torres-strait-islander-social-justice/publications/social-justice-report-10

Australian Women Against Violence Alliance (AWAVA) (2017). Submission 14 in response to the Senate Inquiry into the Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying, 20 October 2017.

Ben-David, A. & A. Matamoros-Fernandez (2016). Hate Speech and Covert Discrimination on Social Media: Monitoring the Facebook pages of extreme-right political parties in Spain. *International Journal of Communication*, 10, 1167–1193.

Boyd, D. (2014). *It's Complicated: The social lives of networked teens*. Yale University Press.

Brady, F., L.E. Dyson & T. Asela (2008). Indigenous Adoption of Mobile Phones and Oral Culture. In F. Sudweeks, H. Hrachovec & C. Ess (eds). *Cultural Attitudes Towards Technology and Communication*, pp. 384–398. Perth, Australia: Murdoch University.

Brophy, F. & S. Williams (2014). *The Last Showman: The life and times of an Outback tent-boxing legend*. Melbourne: Penguin.

Burbank, V.K. (1994). *Fighting Women: Anger and aggression in Aboriginal Australia*. Berkley: University of California Press.

Campbell, M., L. Crabtree, V. Davis, E. Keltie, S. Madden, A. Flouris, A. Third & R. Hendery (2017). *Keeping Strong: Digital technology, participatory research, and young people's wellbeing amongst Alice Springs Town Camp communities*. Melbourne.

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*, pp. 147–168. Sydney: University of Technology E Press.

Carlson, B., T. Farrelly, R. Frazer & F. Borthwick (2015). Mediating Tragedy: Facebook, Aboriginal peoples and suicide. *Australasian Journal of Information Systems*, 19, 1–15.

Central Land Council. (2012). *Divas Chat Causing Social Chaos: Land Rights News Central Australia*. Retrieved 21 June 2016, from https://www.clc.org.au/index.php?/land-rights-news/publication/land-rights-news-central-australia/315/

Centre for Appropriate Technology (2013). *Housing Experience: Post occupancy evaluation of Alice Springs town camp housing 2008–2011,* Alice Springs.

Citron, D.K. & H. Norton (2011). *Intermediaries and Hate Speech: Fostering digital citizenship for our information age.* Boston University Law Review, 91, 1435–1484.

Clark, Y., & M. Augoustinos (2015). What's in a Name? Lateral violence within the Aboriginal community in Adelaide, South Australia. *Office Bearers of the APS College of Community Psychologists*, 27(2), 19–34.

Cowlishaw, G. (2004). *Blackfellas, Whitefellas, and the Hidden Injuries of Race*. Malden, MA: Blackwell.

Crawford, K., & T. Gillespie (2016). What is a Flag For? Social media reporting tools and the vocabulary of complaint. *New Media & Society*, 18(3), 410–428.

De Crespigny, C., C. Emden, I. Kowanko, & H. Murray (2004). A "Partnership Model" for Ethical Indigenous Research. *Collegian*, 11(4), 7–13.

Dooley, J., L. Thomas, S. Falconer, D. Cross & S. Waters (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. Retrieved 30 June 2016, from http://www.acma.gov.au/theACMA/cybersmart-detectives-report

Dragiewicz, M., J. Burgess, A. Matamoros-Fernandez, M. Salter, N. Suzor, D. Woodlock & B. Harris (2018). Technology Facilitated Coercive Control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*. (In Press).

Ellison, N B., J. Vitak, C. Steinfield, R. Gray & C. Lampe (2011). Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. In S. Trepte & L. Reinecke (eds). *Privacy Online: Perspectives on privacy and self-disclosure in the social web*, pp. 19–32. Berlin: Springer.

Freeman, B., & S. Chapman (2007). Is "YouTube" Telling or Selling You Something? Tobacco content on the YouTube video-sharing website. *Tobacco Control*, 16(3), 207–210.

Foster, D., R. Williams, D. Campbell, V. Davis & L. Pepperill (2006). "Researching Ourselves Back to Life": New ways of conducting Aboriginal alcohol research. *Drug and Alcohol Review*, 25(3), 213–217.

Foster, D., J. Mitchell, J. Ulrik & R. Williams (2005). Population and Mobility in the Town Camps of Alice Springs. *A report prepared by Tangentyere Council Research Unit. Desert Knowledge Cooperative Research Centre Report.*

Fürsich, E. (2009). In Defense of Textual Analysis: Restoring a challenged method for journalism and media studies. *Journalism Studies*, 10(2), 238–252.

Gao, X., S.H. Hamzah, C.K.Y. Yiu, C. McGrath & N.M. King (2013). Dental Fear and Anxiety in Children and Adolescents: Qualitative study using YouTube. *Journal of Medical Internet Research*, 15 (2), e29.

Garlick, M. & A. David (2017). Facebook: Submission 4 in response to the Senate Inquiry, Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying, 18 October 2017.

Gillespie, T. (2012). *The Dirty Job of Keeping Facebook Clean*, Social Media Collective Research Blog. Retrieved 30 June 2016, from https://socialmediacollective.org/2012/02/22/the-dirty-job-of-keeping-Facebook-clean/

Gillespie, T. (2017). Governance Of and By Platforms. In J. Burgess, A. Marwick & T. Poell (eds). *Sage Handbook of Social Media*. Sage. Preprint: http://culturedigitally. org/wp-content/uploads/2016/06/Gillespie-Governance-ofby-Platforms-PREPRINT.pdf

Glaskin, K. (2012). Anatomies of Relatedness: Considering personhood in Aboriginal Australia. *American Anthropologist*, 114(2), 297–308.

Gray, D., B. Morfitt, K. Ryan & S. Williams (1997). The Use of Tobacco, Alcohol and Other Drugs by Young Aboriginal People in Albany, Western Australia. *Australian and New Zealand Journal of Public Health*, 21(1), 71–76.

Hartley, J. (2002). *Communication, Cultural and Media Studies: The key concepts*. London: Routledge.

Heins, M. (2014). The Brave New World of Social Media Censorship, *Harvard Law Review Forum*, 325.

Hogan, E. (2014). *Behind the Mulga Curtain*. Inside Story. Retrieved 30 June 2016, from http://insidestory.org.au/behind-the-mulga-curtain.

Hogan, E., R. Gregory & J. Thomas (2012). *Papunya Internet and Computer Centre Report*. Melbourne: Swinburne Institute for Social Research.

Holmes, W., P. Stewart, A. Garrow, I. Anderson & L. Thorpe (2002). Researching Aboriginal Health: Experience from a study of urban young people's health and well-being. *Social Science and Medicine*, 54(8), 1267–1279.

Hooper, C. (2009). Boxing for Palm Island. *The Monthly*, February. Retrieved 27 March 2018, from https://www.themonthly.com.au/issue/2009/february/1294082214/chloe-hooper/boxing-palm-island

Hopkins, N. (2017). Revealed: Facebook's internal rulebook on sex, terrorism and violence. *The Guardian (Australia Edition),* 22 May. Retrieved 20 November 2017, from https://www.theguardian.com/news/2017/may/21/revealed-Facebook-internal-rulebook-sex-terrorism-violence

Iten, L. (2014). *Southern RIPIA Sites Cyber Safety Program Report*. Alice Springs: Northern Territory Library & Central Australian Youth Link Up Service.

Ito, M., H.A. Horst, M. Bittanti, B.H. Stephenson, P.G. Lange, C.J. Pascoe & D. Mahendran (2009). *Living and Learning with New Media: Summary of findings from the digital youth project*. Cambridge MA: MIT Press.

Johnson, B.G. (2017). Speech, Harm, and the Duties of Digital Intermediaries: Conceptualizing platform ethics. *Journal of Media Ethics*, 32(1), 16–27.

Katz, I., M. Keeley, B. Spears, C. Taddeo, T. Swirski & S. Bates (2014). *Research on Youth Exposure to, and Management of, Cyberbullying Incidents in Australia: Synthesis report*. Sydney: Social Policy Research Centre, UNSW.

Keelan, J., V. Pavri-Garcia, G. Tomlinson & K. Wilson (2007). YouTube as a Source of Information on Immunization: A content analysis. *Journal of the American Medical Association*, 298(21), 2482–84.

Kelly, L. (2002). Mediation in Aboriginal Communities: Familiar dilemmas, fresh developments. *Indigenous Law Bulletin*, 5(14), 7–10.

Kieu, B.T., R. Ichise & S.B. Pham (2015). Predicting the Popularity of Social Curation. In V. Nguyen, A. Le & V. Huynh (eds). *Knowledge and Systems Engineering: Proceedings of the Sixth International Conference* KSE 2014, 413–24. Cham: Springer International Publishing. DOI:10.1007/978-3-319-11680-8_33

Kral, I. (2011). Youth Media as Cultural Practice: Remote Indigenous youth speaking out loud. *Australian Aboriginal Studies*, 1, 4–16.

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*, 25, 171–189.

Langton, M. (1988). Medicine Square. In I. Keen (ed.). *Being Black: Aboriginal Cultures in "Settled" Australia*, pp. 201–226. Canberra: Aboriginal Studies Press.

Lee, K.K., K.M. Congrave, A.R. Clough, T.A. Dobbins, M.J. Jaragba & G.C. Patton, (2009). Five–year Longitudinal Study of Cannabis Users in Three Remote Aboriginal Communities in Arnhem Land, Northern Territory, Australia. *Drug and Alcohol Review*, 28(6), 623–630.

Lee, K.S., M.J. Jaragba, A.R. Clough & K.M. Congrave (2008). Wa! Ningeningma arakba akina da! (Oh! Now I know, that's it!): Providing feedback to communities about studies of cannabis use in Arnhem Land, Northern Territory. *Medical Journal of Australia*, 188(2), 113–116.

Lee, K.S., T. Chikritzhs, S. Wilson, A.O. Wilkes, D. Gray, R. Room & K.M. Conigrave (2014). Better Methods to Collect Self–reported Alcohol and Other Drug Use Data from Aboriginal and Torres Strait Islander Australians. *Drug and Alcohol Review*, 33(5), 466–472.

Lumby, B. (2010). Cyber-Indigeneity: Urban Indigenous identity on Facebook. *The Australian Journal of Indigenous Education*, 39(S1), 68–75.

Liberman, K. (1980). Ambiguity and Gratuitous Concurrence in Inter-cultural Communication. *Human Studies*, 3(1), 65–85.

McFarland, J. & L. Iten (2016). Community Management of Public Internet Wifi Hotspots, paper presented to Broadband for the Bush Forum V, 8–9 July, Brisbane.

McLennan, W. (2007). *Tent Boxing: An Australian Journey*. Granta Books: London.

McNair Ingenuity Research and the Indigenous Remote Communications Association (2016). *Remote Indigenous Communications and Media Survey*. Retrieved 30 July 2017, from http://www.irca.net.au/projects/remote-indigenous-communications-and-media-survey-2016

Macdonald, G. (2000). Economies and Personhood: Demand sharing among the Wiradjuri of New South Wales. *Senri Ethnological Studies*, 53, 87–111.

Macdonald, G. (1988). A Wiradjuri Fight Story. In I. Keen (ed.). *Being Black: Aboriginal Cultures in "Settled" Australia*, pp. 179–199. Canberra: Aboriginal Studies Press.

MacKinnon, R., E. Hickok, A. Bar & H. Lim (2015). Fostering Freedom Online: The roles, challenges and obstacles of internet intermediaries. *Other Publications from the Centre for Global Communication Studies*. Retrieved July 30 2017, from http://repository.upenn.edu/cgcs_publications/21

Martin, D.F. (1993). *Autonomy and Relatedness: An ethnography of Wik people of Aurukun, western Cape York Peninsula*. (Unpublished doctoral thesis). Canberra: Australian National University.

Marwick, A.E. (2012). The Public Domain: Social surveillance in everyday life. *Surveillance & Society*, 9(4), 378–393.

Marwick, A.E. & d. boyd (2018). Understanding Privacy at the Margins. *International Journal of Communication*, 12, 1157–1165.

Matias, J.N., A. Johnson, W.E. Boesel, B. Keegan, J. Friedman & C. DeTar (2015). Reporting, Reviewing, and Responding to Harassment on Twitter. Women, Action, and the Media. 13 May 2015. Retrieved July 30 2017, from http://womenactionmedia.org/twitter-report

McFarland (née Turner-Walker), J. (2012). *Clash of the Paradigms: Night patrols in remote central Australia* (Unpublished M. Crim. Justice thesis). Perth: University of Western Australia.

Milosevic, T. (2016). Social Media Companies' Cyberbullying Policies. *International Journal of Communication*, 10, 5164–5185.

Mueller, M.L. (2015). Hyper-transparency and Social Control: Social media as magnets for regulation. *Telecommunications Policy*, 39(9), 804–810.

Moreton-Robinson, A. (2013). Towards an Australian Indigenous Women's Standpoint Theory. *Australian Feminist Studies*, 28(78), 331–347.

National Alternative Dispute Resolution Advisory Council (NADRAC) (2006). *Indigenous Dispute Resolution and Conflict Management*. Retrieved July 30 2017, from https://www.ag.gov.au/LegalSystem/AlternateDisputeResolution/Documents/NADRAC%20Publications/Indigenous%20Dispute%20Resolution%20and%20Conflict%20Management.PDF

Nippert-Eng, C.E. (2008). *Home and Work: Negotiating boundaries through everyday life*. Chicago: University of Chicago Press.

Nissenbaum, H. (2009). *Privacy in Context: Technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

Office of the eSafety Commissioner (n.d.-a). *Legislation*. Retrieved 26 March 2018, from https://www.esafety.gov.au/about-the-office/legislation

Office of the eSafety Commissioner (n.d.-b). *About Tier 1 of the Scheme*. Retrieved 26 March 2018, from https://www.esafety.gov.au/social-media-regulation/about-tier-1-of-the-scheme

Office of the eSafety Commissioner (n.d.-c). *About Tier 2 of the Scheme*. Retrieved 26 March 2018, from https://www.esafety.gov.au/social-media-regulation/about-tier-2-of-the-scheme

Office of the eSafety Commissioner (n.d.-d). Submission 13 in response to the Senate Inquiry into the Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying.

Overlander.tv. (2008). *Outback Tent Boxing: End of an era*. Retrieved 17 February 2018, from https://www.youtube.com/watch?v=p4LQysWei3Q

Osborne, S. (2016). Cultural Capacity and Development: The case for flexible, interdisciplinary research in remote Aboriginal and Torres Strait Island communities. *Learning Communities Special Issue: Synthesis & Integration*, 19, 46–63.

Post, R.C. (1989). The Social Foundations of Privacy: Community and self in the common law tort. *California Law Review*, 77(5), 957–1010.

Putt, J. (2013). *Conducting Research with Indigenous People and Communities*. Sydney: Indigenous Justice Clearinghouse.

PY Media. (2016). *Cyber Safety Project*. Retrieved 26 March 2018, from http://www.pymedia.org.au/cyber-safety-project/

Queensland Family and Child Commission (2017). Submission 8 in response to the Senate Inquiry into the Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying.

Radoll, P. (2014). Cyber Safety and Indigenous Youth. *Indigenous Law Bulletin*, 8(12), 11–14.

Rennie, E., E. Hogan & I. Holcombe-James (2016a). *Cyber Safety in Remote Aboriginal Communities and Towns: Interim Report*. Melbourne: Swinburne Institute for Social Research.

Rennie, E., E. Hogan, R. Gregory, A. Crouch, A. Wright, J. Thomas & M.D. Rasch (2016b). Internet on the Outstation: The digital divide and remote Aboriginal communities. *Theory on Demand*, 19.

Rennie, E., T. Yunkaporta & I. Holcombe-James (2018). Privacy Versus Relatedness: Managing device use in Australia's remote Aboriginal communities. *International Journal of Communication*, 12(19), 1291–1309.

Rieder, B., A. Matamoros-Fernández & Ò. Coromina (2018). From Ranking Algorithms to "Ranking Cultures": Investigating the modulation of visibility in YouTube search results. *Convergence*, 24(1), 5–68.

Rigney, L.I. (1999). Internationalization of an Indigenous Anticolonial Cultural Critique of Research Methodologies: A guide to Indigenist research methodology and its principles. *Wicazo Sa Review*, 14(2), 109–121.

Senate Report (2018). *Adequacy of Existing Offences in the Commonwealth Criminal Code and of State and Territory Criminal Laws to Capture Cyberbullying*. Legal and Constitutional Affairs References Committee. Commonwealth of Australia, March 2018.

Shaw, G. & P. d'Abbs (2011). *Community Safety and Wellbeing Research Study: Consolidated report*. Canberra: Department of Families, Housing, Community Services and Indigenous Affairs.

Smith, L.T. (1999). *Decolonizing Methodologies Research and Indigenous Peoples*. London: Zed Books Ltd.

Spiro, M.E. (1993). Is the Western Conception of the Self "Peculiar" Within the Context of the World Cultures? Ethos, 21(2), 107–153.

Stanner, W.E.H. (1905–1981/2009). *The Dreaming and Other Essays*. Melbourne: Black Inc.

Sunder, L. (2016). *Predictive Model for Views in YouTube Beauty Community*. Retrieved 30 July 2017, from https://www.causeweb.org/usproc/sites/default/files/usresp/2016/Predictive Model for Views in YouTube Beauty Community_VF_C.pdf

Swist, T., P. Collin, J. McCormack & A. Third (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*, 25(2), 239–255.

Vitak, J., & J. Kim (2014). You Can't Block People Offline: Examining how Facebook's affordances shape the disclosure process. In *Proceedings of the 17th ACM conference on Computer Supported Cooperative Work & Social Computing*, pp. 461–474.

Westin, A.F. (1967). *Privacy and Freedom*. New York: Atheneum.

Willis, M. (2011). Non-Disclosure of Violence in Australian Indigenous Communities. *Trends and Issues in Crime and Criminal Justice, 405*. Canberra: Australian Institute of Criminology. Retrieved 30 July 2017, from https://aic.gov.au/publications/tandi/tandi405

YouTube (2010). *Terms of Service.* Retrieved 30 October 2017, from https://www.youtube.com/t/terms?hl=en-GB&gl=AU

Appendix

As noted in Section 1.3, as part of Yunkaporta's Indigenous standpoint methodology, data analysis was executed through "yarns" with family and knowledge-keepers, deep reflection, and the carving of symbols on a traditional wooden object before translation into standard English print forms. The result of this can be seen to the right.

Based on this translation – from yarns to standard English – Yunkaporta also developed a matrix for understanding cyber safety actions and responses within the specific context of Indigenous sociality. This coding of the Cape York ethnographic observation has been included for reference below, as it helped frame the analysis presented in this report.

Legitimate Power				Illegitimate Power			
eTransgression		eConsequence		eTransgression		eConsequence	
Insider	Outsider	Insider	Outsider	Insider	Outsider	Insider	Outsider
Family members sending pics to stay in touch are using too much data, spending more than they can afford. Some older people self-exclude from phone use, and thus much family comms (technophobia, unfamiliarity). Difficult culturally to say no to reverse charges, or share credit when family members demand it. Some parents (minority) refuse to allow young children access to phones or social media. Many parents buying phones for children for games, from age 5 or 6. Reluctance to use security pin number. Males and females have different attitudes towards phones and internet.	Slow internet, inferior infrastructure provided. Prepaid only available to most. Data usage prohibitively expensive. Reverse charge calls that Aboriginal people feel obligated to accept are overly expensive. People face disconnection if they can't afford to recharge credit for an extended period. More govt control and surveillance via technology. Higher bureaucratic burden of welfare in regulating daily life (online forms, programs and processes via on-site offices) that demand continuous compliance and locals' presence in town to receive welfare benefits, limiting excursions on country.	Family members have begun refusing to accept reverse charge calls or share credit. People blocking troublemakers on Divas and Facebook. Additional household economic stress due to additional costs of phones, credit, etc. Loss of privacy due to camera surveillance. Some like, some don't. Some willing to sacrifice privacy for safety, both online and in community. Increased literacy and exposure to print through phones. People avoiding phones or Facebook accounts are excluded from a lot of family and community information and comms.	Telstra pressured to upgrade internet services for community. Government installs surveillance cameras on street to curb violence caused by social media misuse. Government-sponsored local Justice Group, made up of Elders with non-Aboriginal manager, facilitates mediation between families, forces perpetrators of online strife to apologise, sometimes sends them out bush for a period of suspension from community. Two posters about cyberbullying displayed briefly at local store.	Young people misusing 1800MumDad reverse charge calls. Concerns about youth accessing inappropriate material on Google, Facebook and Divas. Minors lying about their age on social media, pretending to be over 18. Youth hacking Facebook accounts and starting fights in community with offensive posts. Divas anonymous profiles used to commit taboo cultural offenses unheard of before (e.g. "swearing" at dead people and babies, boy assuming female identity online). "Teasing" has escalated alarmingly with online anonymity. Exclusive problem to new digital native generation.	Rare circumstances of people getting economically scammed or exploited. Understanding of this is limited (e.g. respondent is unaware that her own car loan falls into this category). Monthly Divas cost runs down pre-paid credit. Occasional incidences of racist posts and content. Not seen as a problem. Perception that white people are "always busy" on the phone. Seen as a cultural flaw. Technology introduced though marketplace without adequate information or education about its use. Concern about outsiders luring or grooming children, but no actual cases of this have been reported.	Unnamed consequence of "swearing" or trolling on Facebook, associated with white people being able to see. White gaze seen as a deterrent to wrongful behaviour, which is only done covertly online. Individuals exacting violent revenge for online insult, but targeting innocent people. Two families violently feuding to avenge online insult, without knowing identity of true perpetrators. Family communication breakdown due to overuse of phones ("We're not family anymore.") Community now under street camera surveillance in response, due to violence escalating via misuse of social media. Loss of sleep.	People posting racist comments are occasionally rebuked with comments like, "This is our land". Outsiders threatened with violence online for racist posts, but this seems to be done by Aboriginal people from other communities.

Legitimate Power				Illegitimate Power			
eTransgression		eConsequence		eTransgression		eConsequence	
Insider	Outsider	Insider	Outsider	Insider	Outsider	Insider	Outsider
Peer pressure to keep a Facebook account for family comms, and to stay up to date with community events. Males use and abuse social media less than females, and in different ways. Some male resistance to (and sabotage of) technology in rugged assertions of identity and autonomy. Feuds started on social media spill out into conflicts across community, causing violence: often people pursing legitimate grievances against perceived illegitimate authority (e.g. in workplace), or misplaced anger against peers. Reliance on phones for sense of safety out bush – people don't go anywhere now without phones. Elders lack proficiency and specialist knowledge about phones and how kids use them, feel a need to surrender some authority to outside experts to inform and advise. Elders lack knowledge or even desire to use IT to communicate with the young about device misuse (e.g. would prefer to use a loudspeaker in community to spread messages about appropriate device use). Use of Aboriginal language in conflicts over the phone can escalate conflict more intensely than when English is used. Limited use of parental lock on internet use – most don't know about this. Tendency to smooth over or cover up disputes and conflicts, rather than address root causes of e-violence. Shame and a need to display a picture that everything is okay now, and the violence is in the past.	Inadequate explanation or instruction in technology introduced via programs into the community (e.g. PCYC Wi-Fi). Discontinuity and transience of programs introduced to give access to technology (e.g. Knowledge Centre). Invasive welfare tech infrastructure and surveillance encroach on privacy.	Community Elders and families involved in mediation to handle perpetrators and feuding families after online strife. Mission Day punishment now illegal and discontinued (e.g. tying to tree with ant nest, flogging with switch, etc.) Agreement throughout community not to talk about past feuds caused by social media abuse. Universally adhered to. Widespread downloading and use of games, access to digital entertainment Sometimes young people fighting due to online conflicts are banished from town for a while, to stay out bush with family. Elders approach youth informally in community life to warn them about misusing devices. Limiting phone contacts to close family members only, policing who is contacted by phone (for privacy and security). Some struggle between competing needs for safety/ control and freedom/ privacy. Most err on side of safety, and embrace idea of punitive measures and controls. Strong assertion by males that culture/ spirituality and technology are to be kept separate, and don't affect each other. But some females report the opposite.		Teenagers "walking head down on their phone", limiting interaction with family and place, abandoning previous inventive and physical forms of play. Young people pressuring family to buy more costly phones, often replacing phone. Phone theft widespread. Some conflict with family in other communities is partially carried out via social media. With excessive phone use, a perceived loss of focus on cultural activity, decrease in cultural participation from younger generation. Internet addiction – Facebook. Peer pressure to participate in social media. Male violence provoked by phone theft – fighting, stealing cars, self-harm in vindictive fits of rage. Willful continuation of social media use, despite awareness of own social media addiction and damage it is doing. Rejection of pin security measures because phones become locked when children try to guess the pin. Young people, especially girls, posting fight videos on YouTube. Some relational concerns, with girls inappropriately using uncle's device to call boyfriends, can cause misunderstandings and cultural problems for uncle.		Headaches from overuse of devices. Assimilation – people being "always busy" on the phone, which is seen as a more mainstream cultural trait. Refusal to share credit can alienate a person from informal local economy. Sense that children "boss" parents, and that when measures are put in place, young people increase pressure via violence to get access to technology (tantrums, property damage until demands met). Sense that kids will find ways around controls, by stealing devices, hacking etc. There's a kind of genius in how some children find "hacks" to frustrate social control measures. Has always been simultaneous pride and condemnation of this behaviour from adults. Pride is expressed away from the colonial gaze, while condemnation is expressed beneath it. Same could be said of resistant and sometimes destructive behaviours by adults, both online and offline.	


RMIT
UNIVERSITY