International Journal of Communication 12(2018), 1291–13091–18 1932–8036/20180005

Privacy Versus Relatedness: Managing Device Use in Australia's Remote Aboriginal Communities

ELLIE RENNIE[1]
RMIT University, Australia

TYSON YUNKAPORTA
Monash University, Australia

INDIGO HOLCOMBE-JAMES
RMIT University, Australia

Aboriginal Australians living in remote communities are likely to be "mobile only" users. The sharing of devices among kin is common and linked to demand sharing practices that stretch back to presettler times. While sharing can produce benefits (acting as a form of insurance), it can also lead to privacy-related problems among this group, including illicit use of banking and social media accounts via shared devices. In this article, we examine the ways in which the aspect of Aboriginal sociality known as relatedness is interacting with online privacy frameworks designed for individual device use and device management. The findings suggest that the sociotechnical frameworks of platforms and devices do not accord with cultural dynamics, including obligations to others. Moreover, efforts by individuals and Elders to avoid privacy-related problems are leading to digital exclusion in various forms, from the deliberate destruction of devices to whole communities opting out of mobile infrastructure.

Keywords: privacy, digital inclusion, remote Aboriginal communities, social media

Ellie Rennie: ellie.rennie@rmit.edu.au
Tyson Yunkaporta: tyson.yunkaporta@monash.edu.au
Indigo Holcombe-James: indigo.holcombe-james@rmit.edu.au
Date submitted: 2017–02–08

[1] We thank the Elders and research participants for their contribution to this research and for allowing us onto their land. A number of individuals and organizations assisted with the research in central Australia, including Barkly Regional Arts, Piliyintinji-ki Stronger Families, Tennant Creek High School, Elliott School, and the Owairtilla Aboriginal Corporation. Eleanor Hogan was a chief investigator for the first stage of the project and was involved in the data collection and analysis for the central Australian component. Facilitators for workshops for the first stage included Dale Wakefield, Beth Sometimes, Mark Sulikowski, and Micheil Paton. Telstra funded the research discussed in this article as an action within the Connection and Capability priority focus area of their Reconciliation Action Plan 2015–18. RMIT University and Swinburne University of Technology contributed in-kind support.

> *In the Cape York region, in Australia's far northeast, a middle-aged Aboriginal man describes how he tries to manage his mobile phone. His children use his phone, sometimes to start fights: "They fighting here from mobile same way, dirty word like that, all from mobile." A fight between children or teenagers online can easily flare up into a large group fight involving adults. He warns them that the police will know who started the fight because they will confiscate the phone. He is also distressed that when his daughter uses his phone he can 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 explains. In any other situation, the man would avoid a daughter's boyfriend, as some forms of contact with in-law groups may be in breach of kinship rules. Even if it is not the man's fault if he sees the boyfriend's name in his phone, or speaks to him accidentally, he is nonetheless accountable under customary law.*
>
> *During the conversation, the man says in hushed tones, "They bin swear like dead people aa'." He is describing a particularly dramatic incident that had recently taken place on social media. Traditionally, swearing, teasing, and the subsequent fights were always highly ritualized, including songs and dances followed by stylized and theatrical combat designed to release aggression and settle tensions, minimizing harm. Participants were always highly visible and accountable for their words and actions. However, in this incident, with the perpetrator safely anonymous and able to frame others for the transgression (using a fake profile), the double taboo of publicly saying the name of a deceased person and "swearing" them at the same time proved to be an explosive cultural innovation with disastrous consequences for the community. Outraged family members confronted those who had been framed 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 extreme violence involving hundreds of people.*

Stories of social unrest triggered by communication on social media are surfacing from disparate remote Aboriginal communities (Kral, 2014; Vaarzon-Morel, 2014). Some Elders have called for bans on particular platforms, and some communities have rejected mobile phone towers altogether (Rennie, Hogan, & Holcombe-James, 2016). However, many Elders are also aware of the benefits of communication technology, leaving them at a loss as to how to deal with the issue. In this article, we show how technological privacy approaches can fail in the face of social obligations, and that this failure can have serious consequences, including violence. We develop a relational understanding of privacy, drawn from an examination of three types of privacy-related conflict: demands by nonowners for access to devices, impersonation on social media, and retribution when a person or family's reputation is undermined.

When describing how phones are being used and where conflicts start, people from communities will often describe practices related to privacy, such as a young person using another's social media account through a device that has been "borrowed" with or without the owner's knowledge. If reputational damage, shaming, insult, or jealousy occurs, conflict can spread quickly through family groups, as illustrated in the Cape York example. While privacy technologies embedded within devices and platforms

are designed to help people manage and avoid unwanted communication, social dynamics and obligations can prevent Aboriginal people from using devices and settings in the way they were intended.

Technology design mostly presumes autonomy in device ownership and use as well as an individual's ability to dictate social interactions. In cultures where the individual is expected to be open to requests from others in their network, these systems can fail with serious consequences. Not only can the relatedness that characterizes social life in Aboriginal communities render technology privacy systems unworkable, when privacy transgressions occur, relatedness and obligations may be reasserted through violence. These incidents reveal how the sociotechnical frameworks of platforms and devices institute an individualistic notion of privacy at odds with Aboriginal sociality. The article draws on qualitative research conducted in two regions of remote Australia, consisting of consultative workshops and interviews in one region, and ethnographic work in the other, together with analysis of the Indigenous knowledge systems at play.

Privacy as Boundary Work

Research into social media use among teens and adults in Western settings is primarily concerned with what Nippert-Eng (2008) calls "boundary work"—the strategies and practices that individuals develop to create, maintain and modify what they consider to be private. For instance, individuals may organize and delineate realm-specific matters such as family and work.

However, studies have shown that legal and technical conceptions of privacy, based on the rights of the autonomous individual, are inadequate for networked social configurations. Marwick and boyd (2014) argue that the networked nature of social media shows that the "individualistic model of privacy does not accurately map to human behavior" (p. 1063) as there are limits to what individuals can do to control data or their online identity. Privacy is instead negotiated through strategies and codes, and these require "ongoing maintenance and negotiation" (Ito et al., 2008, p. 1).

Boundary work can therefore occur through strategies such as self-monitoring, self-conscious identity construction, and self-disclosure, and each involves the "internalizing of social surveillance" (Marwick, 2012, p. 379; see also Andrejevic, 2005; Trottier, 2011; Vitak & Kim, 2014). While social media disrupts or distorts these acts, none are particularly new: "Technology inflects age-old issues in new ways, and these shifts must be understood" (boyd, Marwick, Aftab, & Koeltl, 2009, p. 410; see also Solove, 2007).

The body of work on social media and privacy poses an important challenge to the notion of the individualistic, autonomous agent requiring protection through privacy. Instead, social media and devices institute privacy frameworks that may conflict with social norms or force the user into difficult choices. Nissenbaum (2009) shows 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" (p. 3). Because of this, technology systems and technology practices "have provoked and continue to provoke anxiety, protest, and resistance in the name of privacy" (Nissenbaum, 2009, p. 3). Her framework of understanding privacy through "contextual

integrity" sidesteps the need to define privacy in legal or normative terms as a value, a right or a preference. Instead, privacy can be examined through the systems that affect flows of information and how this in turn generates positive and negative outcomes for individuals and groups. Understanding boundary work reveals not only social norms through user actions but also the assumptions built into social software (Marwick, 2012).

Following this, our analysis does not attempt to define privacy, but to understand how the sociotechnical systems of mobile devices and social media are interacting with conceptions of privacy in remote Aboriginal communities. A form of boundary work—making oneself open or closed to others—is clearly at work in remote communities, but it does not correspond to the privacy controls embedded in social media platforms and devices. We therefore start from a broader concept of privacy as a "boundary control process" (I. Altman, 1977, p. 67) that can occur in different ways in different contexts and cultures (see Fiske, Kitayama, Markus, & Nisbett, 1998).

The few published studies on social media in remote Aboriginal communities identify particular problems "seeded in the norms of the social interactions particular to remote Indigenous sociality" (Kral, 2014, p. 181). Conflict can arise from the production and sharing of what is considered to be unregulated content, done without oversight from Elders (Radoll, 2014). In relation to identity, Vaarzon-Morel (2014) writes that everyday expectations of conforming to and respecting customary law are bypassed through fake profiles. She provides an example from Yuendumu involving young people creating fake identities to post slanderous messages and spread rumors, denigrating individuals of the opposite faction. Posts concerned allegations of illicit affairs, trumped-up revelations about the paternity of particular individuals, and descriptions of antisocial behaviors and attributes (Vaarzon-Morel, 2014). Daniel Featherstone (2015) observes, in relation to the Ngaanyatjarra and Anangu Pitjantjatjara Yankunytjatjara lands, that Elders 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.

We show that the "problem" of social media in remote communities stems from two competing systems of privacy, whereby the tools available to manage information through technology are ultimately in tension with, and thwarted by, media practices stemming from social norms. The inability to manage devices in ways that accord with social norms, including who has access to information and accounts, can result in individual hardship, while deliberate attacks on a person's identity can flare up into acts of group violence. The technological tools available, including PINs and blocking people through social media privacy settings, are often ignored or abandoned. Before looking at the apparent gap between privacy concerns and behaviors, it is necessary to consider how the notion of relatedness in Aboriginal culture differs from personhood as understood in Western cultures.

Autonomy and Relatedness

The autonomy of the individual is a core concept of the Western rights paradigm 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; the owner of herself (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" (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011, p. 20), it places the autonomous self at the center.

For Aboriginal knowledge systems, the individual is subsumed within the social, defined by membership of clan and kinship. Privacy, as the selective control of access to the self (as per I. 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 a social order characterized by "relatedness."

Fred Myers (1986), writing of the Pintupi in the central desert in the 1980s, described relatedness as "extending one's ties with others outward, on being open to claims by others, on showing sympathy and willingness to negotiate" (p. 22), which makes it difficult for a person to sustain autonomy. Relatedness can be countered by individuals' unwillingness to accept restrictions imposed on them by others. However, these two patterns, Myers observed, are resolved by a third, which he called "looking after." The notion of looking after transcends the individual as a kind of intersubjectivity that connects into nonhuman beings, including country and ancestral persons (see also Glaskin, 2012).

Similarly, David Martin (1993), working with the Wik Mungkan in the Cape York region, observed that individuality was ultimately subsumed by "the essentially social being" (p. 11), where the social was defined by membership of clan and connection to others through kinship as well as gender, language, and totemic affiliations. The concept of the individual self was still present, but one's spiritual essence, as well as one's physical and emotional characteristics, were related to one's totem, making the self socially connected. Because individuals could not be conceived outside the social, neither could their rights: "Rather than people having natural rights, specific others had 'rights' over them. Again, these 'rights' were pragmatic and contextualized, realized through social practices" (Martin, 1993, p. 37).

The concept of relatedness is important in understanding communication practices and choices in remote Aboriginal communities. Our research shows that the sharing of devices among kin 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 denial can have negative consequences.

The distinction between autonomy and relatedness is never a fixed dichotomy, and the differences between Western and non-Western cultures can easily be overdrawn. In the West, while the notion of privacy involves the protection or preservation of the individual, it also enforces the rules of civility and social norms, protecting or violating ritualistic notions of identity (Post, 1989). The concept of privacy as enacted through law tort therefore acknowledges that individuals' privacy needs are inseparable from social life. Spiro (1993) warns against describing the Western self as "autonomous, egocentric, context-independent, and the like," as it 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" (p. 117). Expressions of autonomy are, and have been, expected and accepted within Aboriginal social relations. Cultural change is also loosening the degree to which obligations determine the distribution of material goods and resources. Where relatedness does still influence social norms, one area it can manifest is in the difficulties people experience in attempting to manage devices and online privacy. Relatedness—however nuanced and fluid—is simply not accommodated through the sociotechnical frameworks of mobile devices and platforms.

Research Method and Field Sites

The research occurred in two phases and across two different regions, with permission from the Traditional Owners. In the Northern Territory, people in Tennant Creek, Elliott, and Canteen Creek/Owairtilla took part in the first stage of the research. Tennant Creek is a town of 3,000 people, approximately 50% of whom are Aboriginal. Elliott is a community of 650 people, over half of whom are Aboriginal. Both of these locations have had Internet access and mobile coverage for almost a decade. By contrast, Canteen Creek/Owairtilla is a small remote community, and most of its 180 residents are Aboriginal. It lies 576 km northeast of Alice Springs, 180 km of which is "off the bitumen," and has no mobile coverage and only satellite Internet access. The second stage of the research took place in a large community in far north Queensland's Cape York region. We have chosen not to name the Cape York community for ethical reasons. The community has had mobile coverage for many years.

Historically, the formation of settlements in remote Australia involved colonial injustices and displacement for Aboriginal people. Larger Aboriginal communities were formed from Christian missions and ration stations under policies to encourage centralization, forced sedentariness, and assimilation. From the 1970s, as the land rights movement grew, the Australian government began to replace such fundamentally discriminatory policies with the scaffolds of self-determination, including providing resources to enable people to live on their ancestral lands. Today, some larger townships, including Tennant Creek, also contain Aboriginal communities known as town camps, which house people originating from the area as well as surrounding lands and which are managed by Aboriginal councils. Many communities and town camps are characterized by inadequate infrastructure and low living standards. The socioeconomic profile of remote Aboriginal communities is one of high unemployment, low rates of school completion, and low life expectancy. Attempts by government to improve living conditions in remote communities have largely failed, and experts remain divided on the causes and nature of Indigenous disadvantage (see Hinkson, 2010).

In all of the communities where our research took place, some social systems and norms are a continuation of a culture that stretches back tens of thousands of years. Other aspects of social life relate to, or are in tension with, contemporary Australia. People navigate the market economy and the welfare state with varying degrees of success, interact with government services and the justice system, and consume and participate in international popular culture. They are also likely to participate in customary activities, speak Aboriginal languages, and maintain connections to their ancestral lands.

While there is no space here to detail the differences between central Australia and Cape York, it

is important to note that Australia's first people belong to many different place-based clans and live according to kinship systems that govern social relations. Our decision to conduct the research in central Australia and Cape York was pragmatic, in that working in Aboriginal communities requires extensive ethical consent processes, including gaining permission from Elders and local councils. The project team made enquiries and selected research sites according to which communities were willing to take part.

The first phase of the research, intended to scope the issues, involved workshops and group discussion in three locations in central Australia. Workshops involved dialogue on cyber safety themes, including privacy settings, and costs. Some of these facilitated dialogues occurred over multiple days. In Tennant Creek, workshops took place at the Piliyintinji Stronger Families women's and men's groups (attendance between 30 and 40 women, ages 25 to 65 years; between 12 and 16 men, ages 20 to 60 years), as well as with students at the high school (12 young women and nine young men). In Elliott, one group consisted of 12 to 15 women, ages 20 to 60 years, while four men ages 18 to 35 years took part in a separate group. In Canteen Creek, one workshop was held with 10 women.

In addition, one-on-one interviews took place in each site, including with Elders, teachers, and Aboriginal Corporation managers as well as with 23 workshop participants who agreed to talk privately. Some participants chose not to answer every question. As the first phase was conducted by non-Indigenous researchers (including Rennie and Holcombe-James), an Aboriginal woman from the region assisted by trialing the interview questions and providing feedback. During the interview stage, researchers and participants entered information directly into iPads and laptops using survey software (nonverbal, screen-based interaction can help overcome intercultural problems associated with direct questioning). Participants were offered a small gift in appreciation for their time. Approximately three-quarters of the interviewees were female and a quarter were male. Ages ranged from 14 to 59 years: Just under half were ages 30 to 44 (48%), with the others spread evenly across the 14–17, 18–29, and 45–59 age groups. Sixty percent of participants spoke one or more Aboriginal languages (Warumungu, Warlpiri, Alyawarr, Kaytej, Wambeya, Jingili); all spoke English. The gender balance is partly explained by the makeup of the research team in the first phase. Moreover, women are generally more agreeable to research participation; there is a gendered privacy to men's talk, which is kept separate from women and particularly from outsiders, which can make data collection on perceived community problems difficult.

The second phase, from which this article mostly draws, involved ethnographic research in one community in the Cape York region. The ethnographic component was undertaken by Yunkaporta, who joined the research team for the second phase. Yunkaporta is a Bama man with close ties in the community and experience navigating the complexities of insider–outsider tensions involved with the interface of Indigenous and academic knowledge systems. The ethnographic component involved informal conversations on the broad topic of cyber safety, conducted over a two-week period, supplemented by five in-depth interviews (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.

Internet Access and Social Media Use

Aboriginal people living in remote areas are far more likely to be mobile-only (telephony and Internet) users than other Australians, and this was true of the research participants. Internet adoption in remote Aboriginal communities has increased dramatically since the arrival of mobile broadband and mobile devices primarily due to convenience; prepaid billing suits a culture where resources are shared while also cutting out the more onerous installation processes required for home Internet connections (see Ewing, Rennie, & Thomas, 2015). In central Australia, interviewees said that they used mobile phones to access the Internet (90%, *n* = 19), followed by tablets (33%, *n* = 7), laptops (24%, *n* = 5), and finally desktops (14%, *n* = 3). The majority (85%, *n* = 17) of interviewees said they only used a mobile broadband service, reflecting the high rate of mobile phone and tablet ownership. Only one person said s/he had a satellite connection, one said s/he was not sure, and two said "other" (including using a computer at a government office). Of the 19 people who answered a question about payment methods, all except one person said they used prepaid accounts. The high rates of mobile use are important in the context of our analysis below because mobile devices have evolved—through myriad design decisions and configurations—to favor individual use and portability (Donner, 2015).

In both sites, research participants viewed mobiles and Internet access as beneficial in emergencies, for managing information and interaction with government services (e.g., receiving text message reminders from health providers) and banking. Social media was also highly valued for enabling easy connection to those within their social network, particularly as people are inclined to change phone numbers regularly (discussed below in relation to PINs and privacy). Facebook was used by three-quarters of the interviewees. The second most popular social media platform was the subscription-based Canadian chat application AirG, also known as Divas Chat, which operates under a third-party agreement with Telstra (the only telecommunications provider in many parts of regional and remote Australia). A very small number of older people, and a higher number of young women, were using Instagram, Snapchat, WhatsApp, and Twitter.

Demand Sharing and Devices

In central Australia and Cape York, people's desire to manage devices, including who else has access to their device, can be undermined by obligations. Device sharing is common, despite widespread awareness that giving a device to someone else might lead to problems. In central Australia, 80% of interviewees (*n* = 17) used their own device, but 57% (*n* = 12) said they also used someone else's. Most respondents (72%, *n* = 13) to a question about sharing ICT 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 on request. A senior man in Cape York used the word *borrow* and *to give,* suggesting permitted use of devices by nonowners:

> 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.

In this observation, the Elder's solution is not to stop others from borrowing phones, or to set a PIN, but rather to educate the borrower on appropriate use. In central Australia, the men in one group observed that blocking people on social media could be problematic because they had obligations to people and it would cause offense.

One middle-aged woman living in the township of Tennant Creek said that she had owned five phones in recent years; three were taken from her and two she destroyed deliberately because people were asking for them. Some women said that they had a second "secret" phone that they kept hidden in their clothing. One senior woman said that she and her husband slept with their phones under their pillows, but this did not always prevent young people from taking them. When asked why people were taking their phones, the woman said that they would either use them to access chat sites or transfer credit from their phones to other devices (an automated service provided by the telecommunications provider for prepaid accounts). Taking the time to set or change the security options on a device is, on the surface, more straightforward than tactics such as hiding. Interestingly, digital literacy is not necessarily the barrier; in interviews, the vast majority of interviewees stated that they did know how to set a passcode or password on a device (82%, n = 18). In the workshops, however, women said that kids would find ways to get into phones, including reading fingerprints left on phones as a means of deciphering PINs, while others suggested that they felt obliged to share their PIN with others.

A Torres Strait Islander woman living and working in the Cape York community 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 discarding locked phones and buying new ones regularly. She said that others had given up on using PINs, suggesting they were either unaware of how to get a device unlocked or found dealing with retail service providers too onerous (Rennie, Hogan, Gregory et al., 2016, identify this as a significant factor affecting digital choices in remote communities). When asked "What would you would do if you lost your phone?" the Elliott men's workshop participants said they would buy another phone. Vitak and Kim (2014), observing US students' use of devices, write that an extreme privacy management strategy is possible at the account level by "deactivating/reactivating one's account or creating multiple accounts" (p. 3). However, they write that such strategies are not likely to be a common practice due to the high management costs. While the management costs are likely to be just has high for those living in remote Aboriginal communities (e.g., cannot be contacted at the same number), the pressures and demands associated with relatedness are seemingly higher, as people tend to favor deactivation.

As the story from the introduction illustrates, the sharing of devices can also result in people seeing text messages or chat conversations meant for others, or speaking to someone who they are forbidden to speak to under the kinship classification system. What was commonly described as people "smashing" their own phones can occur in response to such accidental "wrong-way" communication. Changing SIM cards, and hence phone numbers, is another strategy used to reassert order.

In all of these instances, privacy (or lack thereof) is possibly determined by the practice of "demand sharing," which occurs as part of the maintenance of social allegiances. Demand sharing is

defined as a form of asymmetrical reciprocity, in that the demand incurs no debt in return (Macdonald, 2000; Peterson, 2013); if a person within one's network asks for a resource, the owner of the resource is obliged to give, or is put in a position where open refusal is difficult. Demand sharing is a means by which relationships are regularly tested and affirmed. The practice flows through from presettler society, when it may have been a form of risk management or social insurance when resources were scarce. Anthropologist Nicolas Peterson (2013), who coined the term, argues that demand sharing has persisted because it "underwrites a relational ontology in which sharing has profound significance for the nature of personhood" (p. 167). An ethic of generosity underpins sharing, which is embedded in the kin classification system (Peterson, 2013). Among the Wik Mungkan of Cape York, Martin (1993) observes that a refusal to share or a perceived inadequate share 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" (p. 36). Sharing and exchange are thus a means by which the social order is enacted and maintained.

In contemporary Australia, sharing is often blamed for social inequality in Aboriginal communities, particularly as it can be an obstacle to personal or household accumulation, restricting participation in the capitalist economy (J. Altman, 2011). As women are often the holders of welfare payments, they may experience significant pressure from others in the household. The fact that the women in central Australia were more vocal on device management issues than men may be explained by the greater demands placed on them, particularly from young people.

As relatedness is differentiated, there are varying degrees of obligation, which may explain the seeming complexity of mobile practices to outsiders. Moreover, people have tactics to avoid demands; actions such as hiding devices in clothing are a means of denying without committing outright refusal. It is also the case that some contemporary objects can be deemed exempt from demand sharing (Macdonald, 2000). Mobile devices and credit seem to be in a gray zone where denial (and hence autonomy) might eventually be exerted. For instance, two women in Cape York described their interactions over credit. The first, in her 20s, 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."

The other woman, in her 30s, said that in the past she had asked others for credit ("I used to be like that!"), but added that "somebody buy me credit, I'll pay it back," suggesting that reciprocity in relation to credit is, for her, symmetrical and therefore in accord with Western sharing systems.

Privacy, Identity, and Selfhood

The younger of the two women described her experience of "being hacked," a colloquial term that describes illicit use of one's social media account by another:

> Sometimes you get hacked on Facebook. 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 examples of similar incidents happening to other people she knew. She then stated that "Divas is more worse than Facebook." When asked why Divas Chat 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 is describing people creating profiles on Divas Chat and using them to "swear" another person while remaining anonymous (as in the introduction, *to swear* here is different from simply swearing; swearing is almost a curse, an indecent assault that must be answered with vigorous aggression). She also explained that people are likely to have White (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, p. 20; Westin, 1967). In the young woman's account, individuals are losing the ability to control reputation on Divas Chat, while regulating their reputation on Facebook. This, for Marwick (2012), is understood as social surveillance: "the ongoing eavesdropping, investigation, gossip and inquiry that constitutes information gathering by people about their peers" (p. 382). While surveillance can create beneficial outcomes (Albrechtslund, 2008), it can also be harmful (Andrejevic, 2005; Bigge, 2006).

So-called hacking—including creating fake profiles to taunt and tease others—is also viewed as a deliberate undermining of traditional authority. Vaarzon-Morel (2014) discusses such transgressions in relation to the experience of space, and how the "reshaping of space" through online communication mitigates traditional sociospatial schema, "in which physical distance implied social distance and proximity a close kin relationship" (p. 242). Traditionally, space was used to diffuse conflicts, such as by the position of dwellings, through ritual exclusions, or by moving away to prevent fights escalating. For instance, in the Cape York community, the streets are designed to create safe and separate routes for different clans that are in conflict. Such strategies are not necessarily transferable to the online sphere.

As described in the opening story, in the Cape York region, teasing was a part of traditional culture and schisms remain a feature of contemporary sociality (Martin, 1993). Conflict and jealousies have also been described as a means to express differentiation in other regions (e.g., the Pintupi in Myers, 1986). However, online communication has amplified these teasing behaviors, making them widely visible. Therefore, while teasing may have a place within the social norms of the Cape York community, doing so through online platforms or phones can be interpreted as a rejection of relatedness. The senior male 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 man is suggesting an "alone" behavior, akin to walking down a track unaccompanied, which traditionally, and still today, is a behavior that is equated with intent to do black magic or sorcery. Sickness and misfortune that occurs when a person has been exhibiting such solitary behaviors may result in that person being accused of doing *ma' wop* (sorcery) with evil intent. Platforms such as Divas Chat that enable people to "hide" their identities are viewed suspiciously by Elders as they are stepping outside of their social ties, which are in turn connected into ancestral order.

In their study of a class of teenagers in the United Kingdom, Livingstone and Sefton-Green (2016) describe social media platforms as the equivalent of young people closing the bedroom door. The teenage bedroom space does not necessarily exist in remote community homes (see Musharbash, 2009). However, the use of Divas Chat and other social media platforms by young people may be an assertion of autonomy along these lines. The problem as perceived by Elders is that they remain out of reach and hence disconnected from the social (and cosmological) order.

Consequences and the Reassertion of Relatedness

To return to the incident recounted in the introduction, a fight involving multiple participants took place following an online post that involved swearing a dead person. In more traditional communities, images of the dead are not circulated and names are not uttered for a certain period (Elliot, 2008). In their study of home Internet use in three central Australian outstations, Rennie, Hogan, Gregory, and colleagues (2016) found that social media or applications such as Skype caused distress among some residents as photos and names of deceased family members remained visible on the computer, causing members of the household to stop using the computer until profiles were removed. While cultural practices are adapting to cope with such online shadows (Kral, 2014), as the story at the opening of this article illustrates, deliberate acts of cultural transgression are being committed against the dead to incite or inflame interfamily hostilities. In this instance, two serious cultural violations were committed simultaneously: swearing (or cursing) someone and breaching protocols related to naming the dead (see also Carlson, Farrelly, Frazer, & Borthwick, 2015).

While young people committed the acts, other family members became involved in the dispute. A woman described a separate incident that was instigated by a boy impersonating a girl from another family and swearing his own family:

> Participant: 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: They took him to mediation.
>
> Interviewer: But only after they made like big fights and all that.
>
> Participant: Yeah.
>
> Interviewer: So what happened with the big fights, how did they go, spread out to how many people?
>
> Participant: Lots of people. Men folks were fighting; ladies were fighting.
>
> Interviewer: All over or just like lots?
>
> Participant. Two families. [Long pause] Yeah. So that's a bad one there.

As Sutton (2009) has observed, in Aboriginal communities conflicts can be a strategy for "getting subterranean differences out in the open" (p. 98) to resolve them. When trouble occurs, all members of a group are considered to share the problem (Myers, 1986). The term *lateral violence* is often used describe such infighting that can take a range of forms, including "gossip, jealousy, shaming others, verbal and physical attacks, sabotage and bullying" (Clark & Augoustinos, 2015, p. 19). Langton (2009) has defined lateral violence as "the expression of anomie and rage against those who are also victims of vertical violence and entrenched and unequal power relations" (para. 9).

Anthropologists have drawn connections between violence and traditional forms of dispute resolution such as payback (accounts from the 1930s, e.g., by W. E. H. Stanner, are often cited). Although now worsened by alcohol, Sutton (2009) writes that "rates of interpersonal violence were extremely high then also, and marital and sexual relationships and various kinds of jealousies were chief among the prime causes of conflict then as now" (p. 99). Turner-Walker (2012) notes that where once payback (including where another family member is "paid back" in the offender's stead) was supervised and the rules of engagement understood by all, it is now "far more likely that inappropriate payback will be delivered in an impulsive and opportunistic way, by unauthorised and unsupervised members of the

aggrieved family" (p. 81). She further observes that seeing culture as the reason for violence is insufficient, as it is in the places where tradition is most fragile that people are most at risk.

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. The scale and severity of these fights (tears "in the very fabric of social life," to reiterate Nissenbaum's [2009] words) demonstrates that the mismatch, or gap, between one framework of privacy and another can result in harmful social outcomes. In many instances, the fights extended beyond those that committed the original offense and the person to whom it was directed. Although the original communication is often between children (jealousy among adults being the other major type of event), the kin of the receiver 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"), the response is one where relatedness reasserts itself, albeit in an unsanctioned fashion. The sharing of fight videos online might also be seen as part of this continuity, whereby conflict is acted out in public, making allegiances visible and thereby reaffirming connectedness, albeit through unacceptable behavior in the eyes of Elders.

When asked how such conflict should be resolved, some suggested that people needed to be "educated" in appropriate online behavior. Interviewees also tended to see mediation (either conducted by Elders within the community or by external authorities) as a necessary strategy. Such mediation might involve more traditional means of punishment, such as one instance of banishment described by a Cape York participant:

> Yeah, mediation. Say sorry. But like some, 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.

In central Australia, other responses included calls for particular social media platforms to be banned in communities through filters, and some communities have implemented a "kill switch" to turn off community Wi-Fi when things get out of hand.

Conclusion

In remote Aboriginal communities, the consequences of privacy breaches can be serious, 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 for managing boundaries offered through the technology.

We have argued in this article that privacy issues are of a different order and nature in remote Aboriginal communities because the sociotechnical frameworks of platforms and devices institute an individualistic notion of privacy that does not accord with the relatedness that characterizes Aboriginal sociality. Asymmetrical reciprocity, in particular demand sharing, is a feature of remote Aboriginal sociality that continues to influence how people consume and manage resources. 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.

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 unauthorized access to financial accounts. In response, some individuals are choosing to avoid using certain services (e.g., online banking), while others are facing increased costs associated with data credit theft and the regular need to replace 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.

Our findings also suggest that standard digital literacy approaches to cyber safety will not fully resolve community concerns. In central Australia and Cape York, many community members we spoke to had knowledge of how to use basic technology settings (including PINs and blocking people on social media), but had found these strategies to be insufficient or onerous in the face of social obligations. Moreover, the rules governing communication within the kinship classificatory system can be rendered unworkable through phones and social media if devices are shared, leaving users at a loss as to how to honor obligations and avoidances at the same time. Physical conflict can be a reassertion of relatedness, even where it may fail to reinstate social order.

In both regions, Elders and others favored mediation as a strategy when conflict arises as well as the development of protocols around device use that correspond with cultural obligations. Technology companies could consider ways to build these ideas of accountability into platforms—heightening relatedness through visible place-based protocols. The question that follows from this is whether systems that begin from an understanding of relatedness are possible under contemporary market and legal regimes.

Although the particular issues described in this article relate to specific Aboriginal ways of doing and knowing, the limitations of privacy-related technology design are important for other groups. The boundaries of relatedness and autonomy are fluid even in cultures that privilege individual freedoms (including non-Indigenous Australia). As technologies such as artificial intelligence and biometrics evolve, the extent to which these technologies enable us to navigate social networks and obligations in ways that are conducive to social cohesion should be considered.

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday, 13*(3). doi:http://dx.doi.org/10.5210/fm.v13i3.2142

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

Altman, J. (2011). A genealogy of "demand sharing": From pure anthropology to public policy. In Y. Musharbash & M. Barber (Eds.), *Ethnography and the production of anthropological knowledge: Essays in honour of Nicolas Peterson* (pp. 187–200). Canberra, Australia: ANU E Press.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society, 2*(4), 479–497.

Bigge, R. (2006). The cost of (anti-)social networks: Identity, agency and neo-luddites. *First Monday, 11*(12). doi:http://dx.doi.org/10.5210/fm.v11i12.1421

boyd, d., Marwick, A., Aftab, P., & Koeltl, M. (2009). The conundrum of visibility: Youth safety and the Internet. *Journal of Children and Media*, *3*(4), 410–414.

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

Clark, Y., & Augoustinos, M. (2015). What's in a name? Lateral violence within the Aboriginal community in Adelaide. *The Australian Community Psychologist, 27*(2), 19–35.

Donner, J. (2015). *After access: Inclusion, development, and a more mobile Internet*. Cambridge, MA: MIT Press.

Elliot, C. (2008). Social death and disenfranchised grief: An Alyawarr case study. In K. Glaskin (Ed.), *Mortality, mourning and mortuary practices in Indigenous Australia* (pp. 103–120). Farnham, UK: Ashgate Publishing.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (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, Germany: Springer.

Ewing, E., Rennie, E., & Thomas, J. (2015). Broadband policy and rural and cultural divides in Australia. In K. Andreasson (Ed.), *Digital divides: The new challenges and opportunities of e-inclusion* (pp. 107–124). London, UK: Taylor & Francis.

Featherstone, D. (2015). *Connected, creative and cultural communities: Developing an integrated approach to policy and evaluation for remote Australian Indigenous media and communications* (Unpublished doctoral thesis). Murdoch University, Perth, Australia.

Fiske, A. P., Kitayama, S., Markus, H. R., & Nisbett, R. (1998). The cultural matrix of social psychology. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (4th ed., Vol. 2, pp. 915–981). Hoboken, NJ: John Wiley & Sons.

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

Hinkson, M. (2010). Introduction: Anthropology and the culture wars. In J. Altman & M. Hinkson (Eds.), *Culture crisis: Anthropology and politics in Aboriginal Australia* (pp. 1–14). Sydney, Australia: University of New South Wales Press.

Ito, M., Horst, H. A., Bittanti, M., Stephenson, B. H., Lange, P. G., Pascoe, C. J., & Mahendran, D. (2008). *Living and learning with new media: Summary of findings from the Digital Youth Project*. Cambridge, MA: MIT Press.

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*(2), 171–189.

Langton, M. (2009). The end of "big men" politics. *Griffith Review*. Retrieved from https://griffithreview.com/articles/the-end-of-big-men-politics/

Livingstone, S., & Sefton-Green, J. (2016). *The class: Living and learning in the digital age*. New York, NY: New York University Press.

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

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

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

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051–1067.

Musharbash, Y. (2009). *Yuendumu everyday: Contemporary life in remote Aboriginal Australia*. Canberra, Australia: Aboriginal Studies Press.

Myers, F. (1986). *Pintupi country, Pintupi self: Sentiment, place and politics among Western Desert Aborigines*. Berkeley, CA: University of California Press.

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

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

Peterson, N. (2013). On the persistence of sharing: Personhood, asymmetrical reciprocity, and demand sharing in the Indigenous Australian domestic moral economy. *The Australian Journal of Anthropology, 24*(2), 166–176.

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

Radoll, P. (2014). Cyber-safety and Indigenous youth. *Indigenous Law Bulletin, 8*(12), 11–14.

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

Rennie, E., Hogan, E., & Holcombe-James, I. (2016). *Cyber safety in remote Aboriginal communities and towns: Interim report*. Melbourne, Australia: Swinburne Institute for Social Research. doi:10.4225/50/578432D317752

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. New Haven, CT: Yale University Press.

Spiro, M. E. (1993). Is the Western conception of the self "peculiar" within the context of the world cultures? *Ethos, 21*(2), 107–153.

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

Trottier, D. (2011). A research agenda for social media surveillance. *Fast Capitalism, 8*(1). https://www.uta.edu/huma/agger/fastcapitalism/8_1/trottier8_1.html

Turner-Walker, J. (2012). *Clash of the paradigms: Night patrols in remote central Australia* (Unpublished master's thesis). University of Western Australia, Perth, Australia.

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., & Kim, J. (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 - CSCW '14 (pp. 461–474). New York, New York, USA: ACM Press. https://doi.org/10.1145/2531602.2531672

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