

# SMARTPHONE SHARING WITH INTIMATE PARTNERS:

Implications for  
telecommunications consumer  
cybersecurity



**NOVEMBER  
2025**

Prepared by

MOLLY DRAGIEWICZ,  
JEFFREY ACKERMAN,  
AND MARIANNE  
HAALAND

a((can

Smartphone sharing with intimate partners: Implications for telecommunications consumer cybersecurity

**Authored by Molly Dragiewicz, Jeffrey Ackerman, and Marianne Haaland**

Recommended citation: Dragiewicz, M., Ackerman, J. & Haaland, M. (2025). Smartphone sharing with intimate partners: Implications for telecommunications consumer cybersecurity. Griffith University & Australian Communications Consumer Action Network.

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.

**ISBN: 978-0-9806659-9-4**

### **Griffith University**

Website: <https://www.griffith.edu.au/>

Email: [m.dragiewicz@griffith.edu.au](mailto:m.dragiewicz@griffith.edu.au)

Telephone: +61 7 5552 7040

### **Australian Communications Consumer Action Network**

Website: [www.accan.org.au](http://www.accan.org.au)

Email: [grants@accan.org.au](mailto:grants@accan.org.au)

Telephone: 02 9288 4000

If you are deaf or have a hearing or speech impairment, contact us through the National Relay Service:

[www.relayservice.gov.au](http://www.relayservice.gov.au).

This work is copyright, licensed under the Creative Commons Attribution 4.0 International Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the authors and "Griffith university, supported by a grant from the Australian Communications Consumer Action Network." To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>

This research was made possible by a grant from ACCAN. The authors note our commitment to academic freedom and research integrity. No third party exerted any influence over the research design or analysis.

# TABLE OF CONTENTS

ACKNOWLEDGEMENTS 5

TERMINOLOGY 6

RECOMMENDATIONS 7

INTRODUCTION 8

BACKGROUND 9

FINDINGS 12

Phone Details

How Participants Use Their Phones

Phone Security

Characteristics of Phone Sharing

Reasons for Sharing

Privacy Practices

Communication about Sharing

DISCUSSION 16

Context is Key

Inclusive Cybersecurity Threat Models are Needed

CONCLUSION 19

AUTHORS 20

REFERENCES 21

# TABLE OF FIGURES

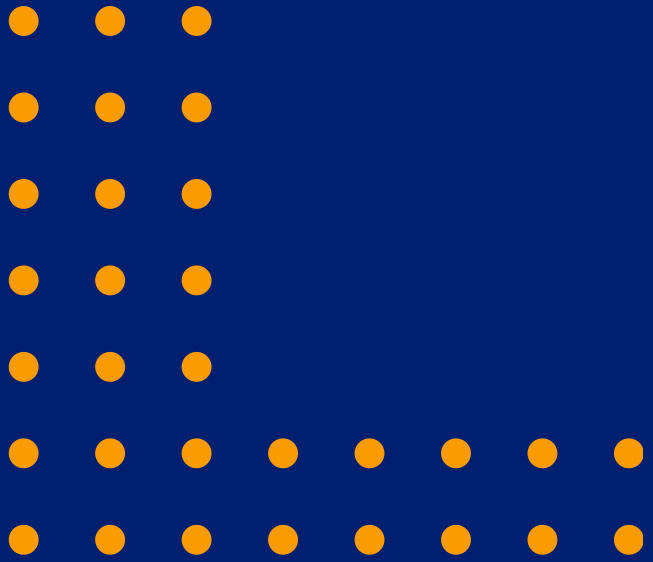
Figure 1. Participants by Sex.	10
Figure 2. Marital Status.	11
Figure 3. Phone Type.	12
Figure 4. Phone Uses.	12
Figure 5. Phone Locking.	12
Figure 6. Unlocking Methods.	13
Figure 7. Access Sharing.	13
Figure 8. Past Year Sharing with Partner	13
Figure 9. Sharing with Others.	13
Figure 10. Sharing by Age.	14
Figure 11. Sharing by Relationship Status.	14
Figure 12. Sharing by Relationship Duration.	14
Figure 13. Reasons for Sharing Access.	15
Figure 14. Privacy Behaviours.	15
Figure 15. Sharing Discussion.	16
Figure 16. Excerpt from ACSC Annual Cyber Threat Report	18

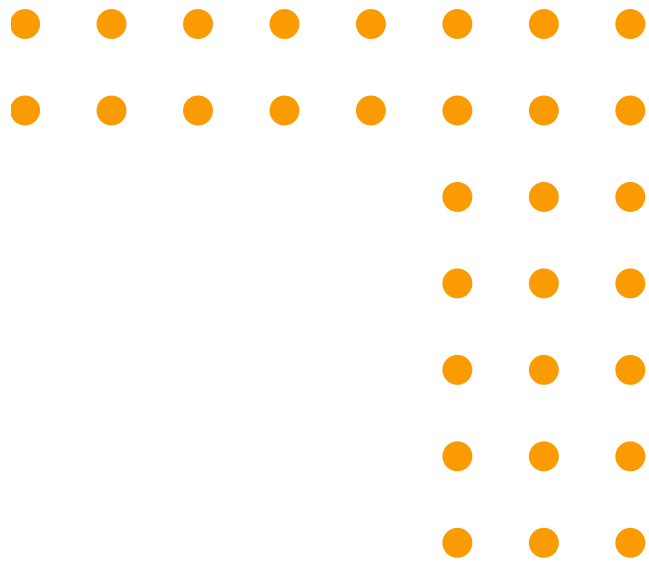


# ACKNOWLEDGEMENTS

The authors would like to express our appreciation to everyone who took the time to complete our survey and follow-up interviews. Sharing your knowledge and experiences has provided an opportunity for telecommunications companies, platforms, services, justice systems, government, and academics to better understand the nature and dynamics of mobile phone sharing. We would also like to thank Rana Al-Mekarry, Manager of the Multicultural Women's Office at Multicultural Families Organisation (MFO), which served as our community partner for this study. Rana's insight, gained from years of community work, greatly improved the survey design. MFO also assisted with recruiting a diverse participant pool and provided an opportunity to share study findings with community members. Support from Griffith University has been invaluable, especially that provided by Angie Signorini, Belinda Watanabe, and Irene Dullaway. This project took place over a transition period at ACCAN, and we had excellent guidance from current ACCAN grants team members Samuel Kininmonth and David Hack, as well as advice from Amelia Radke and Alec Bennetts. We'd also like to thank former ACCAN staff members Tanya Karliychuk and Laetitia Kwan, who initially supported the project. We would like to thank the Australian Communications Consumer Action Network, which made this study possible via their independent research grants scheme.

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.



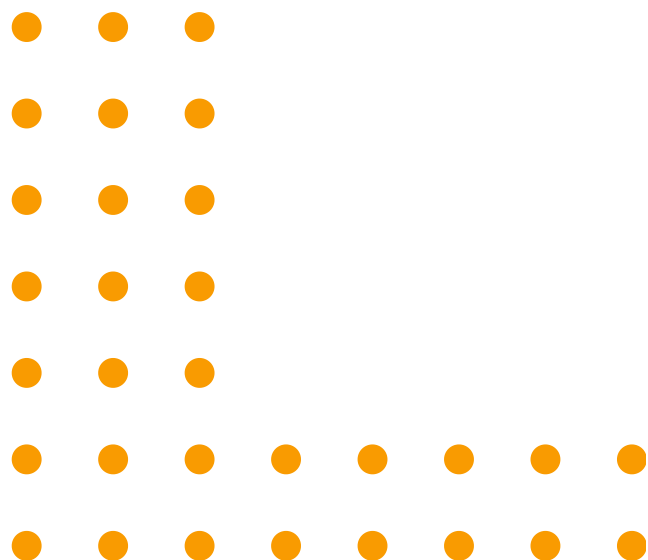


# TERMINOLOGY

## Access Sharing

-

In this report, access sharing refers to a person sharing access to their own phone rather than two people sharing one single phone between them. Access sharing includes a person not locking their phone to allow the partner to use it and sharing access to the phone via credentials such as a PIN, fingerprint, or face recognition.







# RECOMMENDATIONS

1

## **Recommendation One: Expand smartphone cybersecurity options**

- Binary all-or-nothing access models are inadequate for everyday smartphone use.
- Safety by design principles should apply to smartphones and mobile applications.
- Make secure sharing settings the default on smartphones.
- Design devices and applications to facilitate easy adjustments to sharing permissions as needed.

2

## **Recommendation Two: Integrate intimate threats into cybersecurity models**

- While domestic and family violence has been integrated into criminology, law, and policing in Australia, cybercrime frameworks have yet to recognise intimate threats as core concerns for cybersecurity.
- Integrating insights from research on domestic, family, and gender-based violence and how consumers use technology into State and industry cybersecurity frameworks can yield more robust models to address the full spectrum of threats.
- Acknowledge and investigate why consumers share smartphones so that positive social functions can be accommodated alongside harm and risk mitigation.

3

## **Recommendation Three: Promote informed consent for smartphone sharing**

- Any technology or technology behaviour can be used to promote or threaten security and well-being.
- The context of technology behaviours is what gives them their meaning.
- Open communication can help reduce potential conflicts and risks associated with device sharing in couples.
- While communication about expectations for sharing cannot prevent technology-facilitated abuse, it can raise awareness of factors to consider in the future if the nature of the relationship changes.

# INTRODUCTION

This report presents findings from the first study of how Australian couples share smartphone access. The objective of this research was to build a new evidence base to understand Australian couples' everyday smartphone-sharing practices. We conducted a national survey of Australian residents. The survey was conducted online, and participants were recruited via ads on Meta. We conducted follow-up interviews with a diverse group of 10 participants to learn more about their survey responses. In this report, selected quotations from the interviews are used to illustrate typical comments.

This project extends the focus of digital inclusion beyond whether consumers can access the Internet to investigate the relational aspects of smartphone use and their implications. Despite growing recognition that a substantial amount of cybercrime, such as technology-facilitated domestic violence, stalking, identity theft, image-based sexual abuse, and financial fraud, is committed by current and former intimate partners [12,14,20,27,32], little information is available about how couples share smartphones in their everyday lives. This report fills that gap by providing foundational knowledge about smartphone sharing in Australian couples. Our findings can be used to improve privacy protection and security for telecommunications users in Australia and worldwide by providing previously unavailable baseline information about mainstream phone-sharing practices.

Efforts to strengthen cybersecurity have been hindered by a lack of knowledge about threats in interpersonal contexts, such as those arising from everyday smartphone sharing among couples, families, friends, and households [6]. While cybersecurity self-help advice is readily available, most guidance for technology consumers employs a one-user/one-device model, emphasising the importance of not sharing devices, passwords, or personal information. Default mobile phone settings offer all-or-nothing access to users [22]. This can create cybersecurity risks when phones are shared.

This study builds on the growing body of research advocating for increased recognition of interpersonal insider threats to cybersecurity [6,10,14,18]. These threats involve “An authenticated but adversarial user of a victim’s device or account who carries out attacks by interacting with the standard user interface, rather than through the installation of malicious or sophisticated software tools” [18]. They require different tactics for protecting cybersecurity than traditional cybersecurity models centred on remote and technologically sophisticated threats [6,24,27,28]. Based on our earlier research on technology-facilitated domestic violence against women and children, we proposed the Intimate Threat Model for cybersecurity. The Intimate Threat Model includes:

risks created by intentional device and credential sharing;

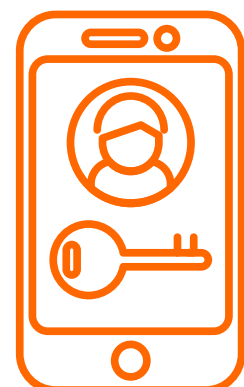
physical access to passwords, networks, and devices; and

intimate knowledge that can facilitate guessing passwords or answering security questions [11,14].

This study created a new knowledge base to understand everyday smartphone use patterns in intimate relationships to better understand Intimate Threats to Cybersecurity. Based on a survey of 967 Australian adults who use smartphones and have been in an intimate relationship, we found that 70% of Australians share access to their phones with their intimate partner. This high rate of shared access suggests that one-user/one-device models are insufficient to promote cybersecurity in realistic smartphone usage conditions.

# 70%

***70% of Australians share access to their phones with their intimate partner.***





# BACKGROUND

Mobile phones are the fastest-spreading communication technology in history [4]. Mobile phones surpassed the number of landlines on Earth in 2002 [8]. By mid-2022, there were more active mobile phone subscriptions than people globally [8]. By 2023, 69% of the global population, approximately 6.7 billion people out of a total of 7.4 billion, owned a smartphone [23].

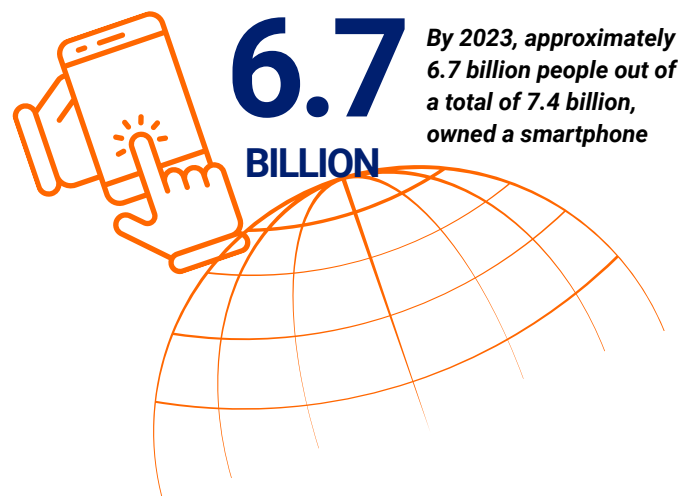
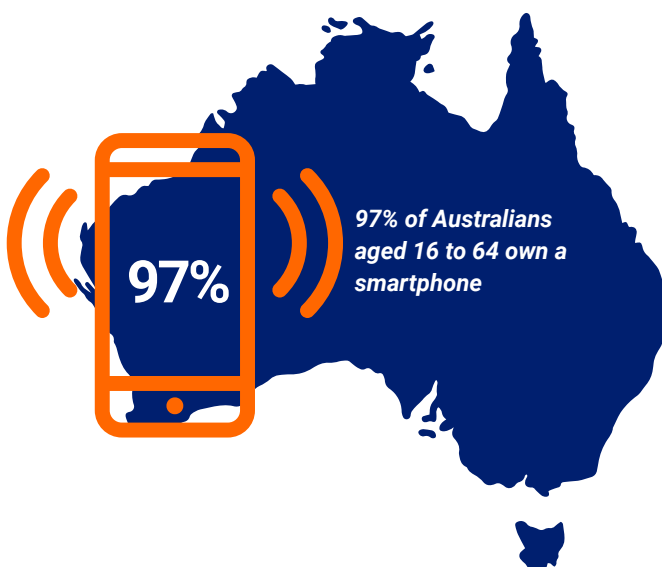
Mobile phone use is near-universal in Australia. Ninety-seven percent of Australians aged 16 to 64 own a smartphone. Comparatively, 75% own a laptop or desktop computer, and 46.1% own a tablet [31]. Over 4 million Australians are mobile-only users, meaning they have a mobile phone with a data allowance but no access to a fixed broadband connection.

Secure access to mobile phones is more critical than ever due to the ubiquity of mobile service interfaces. In Australia, essential private sector and government services are increasingly delivered via mobile interfaces. For example, almost half of Australians aged 16-64 use a banking or other financial mobile app each month, while around one-third use a mobile payment service monthly. Although Australians spend an average of almost three and a half hours using smartphones daily [30], no previous research has investigated whether any of this is on shared devices.

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) leads government efforts to improve cybersecurity in Australia. The ACSC centres a cybersecurity threat model focused on skilled, distant, "malicious cyber actors who continue to target Australia's networks," including government and industry. For example, the ACSC website says,

State-sponsored cyber actors persistently target Australian governments, critical infrastructure and businesses using evolving tradecraft. These actors conduct cyber operations in pursuit of state goals, including for espionage, in exerting malign influence, interference and coercion, and in seeking to pre-position on networks for disruptive cyber attacks. [2]

This focus is consistent with dominant cybersecurity models globally. However, a growing body of research has called for a more holistic approach to cybersecurity that takes the full range of threats into account [6]. This includes greater attention to threats from people we know, including partners, friends, and family.



## METHODOLOGY

To explore mobile phone sharing practices, we conducted a computer-assisted online survey consisting primarily of closed-ended questions, supplemented by open-ended items to capture nuanced insights. Participants were recruited mainly through targeted social media advertising on Facebook and Instagram. These platforms were chosen due to their widespread use, ability to support written advertisements, and capacity to reach diverse audiences through demographic targeting. To enhance diversity, we partnered with the Multicultural Families Organisation, which promoted the survey via their monthly newsletter and in-office signage. This supplemental strategy broadened our participant pool.

Recruitment materials included a brief survey description and a link or QR code embedded with unique query strings. These identifiers allowed us to track recruitment sources and assess whether key survey outcomes varied by recruitment method.

We deliberately chose this recruitment approach over using “representative” samples from commercial survey companies. Such companies typically rely on pre-existing panels of individuals who opt in for financial incentives. This introduces a systematic bias, as these “professional survey takers” may differ from the general population in ways that affect survey responses. While all recruitment methods involve some degree of self-selection bias, social media advertising can reach a broader, more dynamic audience—including individuals less likely to participate in traditional panels—potentially reducing bias and improving representativeness on variables relevant to our study.

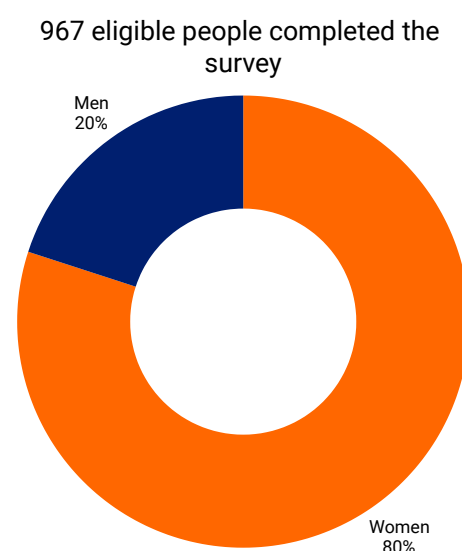
In the context of mobile phone sharing, representativeness should reflect actual behavioural patterns rather than demographic quotas. For example, detecting gender-based differences in sharing practices does not require equal numbers of men and women, but rather a sample whose behaviours align with those observed in the broader population. Our analysis of sharing behaviours across recruitment methods and demographic groups revealed no meaningful differences that would suggest a commercial panel would have offered any advantage over our chosen recruitment strategy.

The survey was open from May through late September 2024. Eligibility was determined through initial screening questions regarding age (18 or older), mobile phone use (e.g., “Do you use a mobile phone in your everyday life?”), current residence in Australia, and current or past involvement in a romantic relationship (same- or opposite-sex). Of those who proceeded beyond the survey information page, 1,049 participants met the eligibility criteria, while 38 were excluded. Among the eligible participants, 988 provided usable responses, defined as having completed the survey at least through the section on mobile phone locking behaviour. Following a quality check, 21 additional responses were removed due to duplication (likely unintentional, based on time gaps between entries), inattentiveness (e.g., identical frequency responses across items), or implausible answer patterns. This resulted in a final analytic sample of 967 participants.

## PARTICIPANT PROFILE

### Demographics

As is common in social science survey research, most participants were women (80%). Less than one percent of participants identified as another sex category.



**Figure 1. Participants by Sex**

Participants ranged from 18 to 82 years old. The average age was 40.

Among respondents who provided information about their ethnicity, 97.5% identified as neither Aboriginal nor Torres Strait Islander.<sup>[1]</sup> Two percent identified as Aboriginal, and less than one percent identified as Aboriginal and Torres Strait Islander. Three-quarters of the participants were born in Australia, and one-quarter were born overseas. Most participants were Australian citizens (90%). In addition, five percent were permanent residents, four percent were on temporary visas, and less than one percent reported some other immigration status.

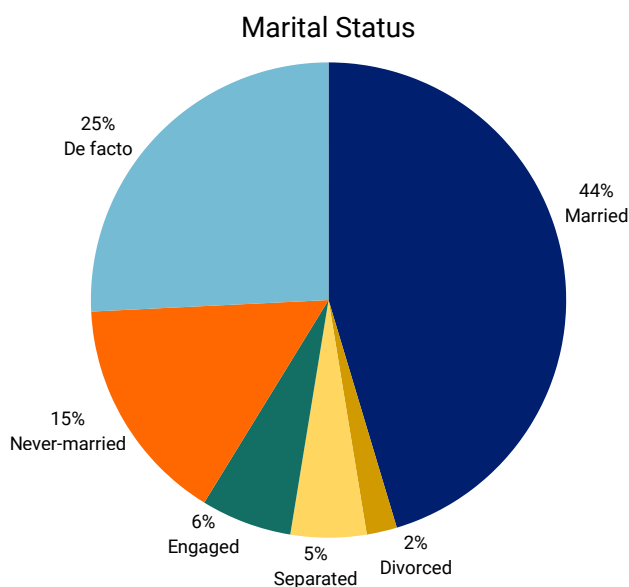
Thirty-four percent of participants reported completing an undergraduate university degree, and 35% had graduate degrees. In addition, 30% reported completing secondary school, and less than one-half of one percent reported completing primary school.

Participant income ranged from \$0 to more than \$200,000. The average annual income for participants was \$72,164.

Three-fourths of our sample identified as straight. Fifteen percent identified as bisexual. Four percent identified as gay or lesbian. The remaining six percent preferred not to answer, didn't know, or selected some other sexuality status.

## Relationship Characteristics

The largest group of participants in our survey were married (44%), followed by those in a de facto relationship (25%). Never-married people were in the next largest category (15%), followed by those who were engaged (6%), were separated (5%), or were divorced (2%).



**Figure 2. Marital Status**

The current or recent relationships participants reported on in the survey ranged from one month to 64 years in duration. The average relationship length for participants was 12 years. Most participants lived with the partner they were reporting on (76%). Almost a quarter of participants (24%) did not live together.

[1] Percentages may not add to 100 due to rounding. In this report, we round most fractions .5 and over to the next highest number. Fractions .4 or less are usually rounded down to the whole number.

# FINDINGS

## Phone Details

Just over half of the participants in our survey used iPhones (51%) as their primary phone. The remaining participants mostly used Android phones (48%), with a few unsure or using other types of phones (less than 1%).

### Phone Type

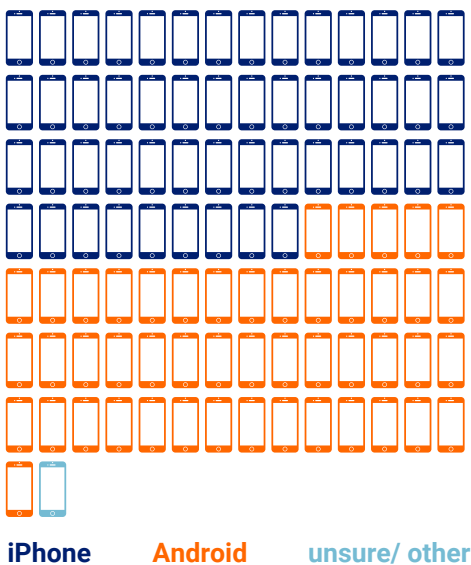


Figure 3. Phone Type

Almost all participants (98%) owned their phone, with one and a half percent saying their partner owned it. Less than one percent reported that someone else owned their phone. Most people (82%) also had their own phone plan, with 17 percent sharing a plan with their partner. Less than one percent said they were unsure who owned the phone.

## How Participants Use Their Phones

Survey participants reported using their phones for essential functions on a daily basis.

### Phone Uses

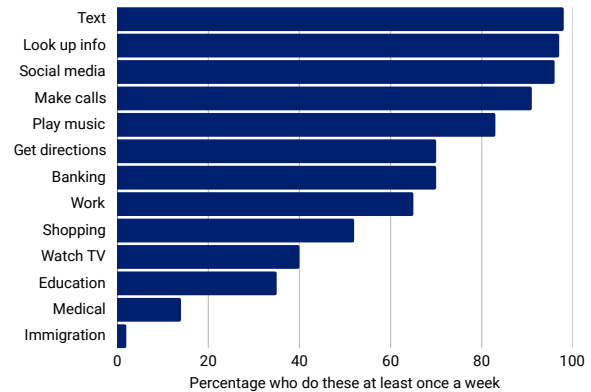


Figure 4. Phone Uses

Most participants text (98%), look up information (97%), use social media (96%), make calls (91%), and play music (83%) at least once a week. More than half of participants use their phones for work (65%), shopping (51%), banking (70%), and getting directions (70%) at least once a week. In addition, 35% use their phones for education, 14% use them for doctors or medical appointments, and 2% use them for visa or citizenship issues at least once a week. Many of these functions are vulnerable to cybersecurity risks, as they involve handling money and sensitive personal information. These findings show that consumers rely on secure access to web-based functions and services via their smartphones.

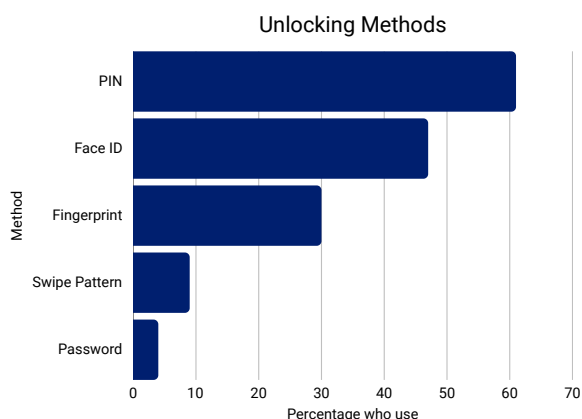
## Phone Security

Ninety-five percent of Australians lock their phone. Only five percent do not use a lock screen on their phone.



Figure 5. Phone Locking

Most people use multiple methods to unlock their phones. A PIN was the most commonly used method to unlock the phone (61%), followed by face recognition (47%), fingerprint (30%), swipe pattern (9%), and password (4%), as seen in Figure 6.

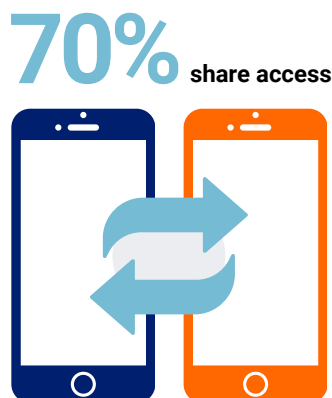


**Figure 6. Unlocking Methods**

Those who didn't lock their phone said they didn't do so because they were the only one who ever had access to it (two percent), so their partner could use it (one percent), or other people could use it (less than one percent). In addition, just under three percent said they didn't lock their phone because they have nothing to hide, and two percent said it wasn't worth the hassle of locking it. One person said they didn't lock their phone because their partner didn't want them to.

## Characteristics of Phone Sharing

Most Australians share authentication permission with their partners so they can access their phone. This report defines access sharing as not locking the phone to permit the partner to use it or allowing a partner access to the phone using credentials. Using this definition, 70% of participants engage in access sharing.



**Figure 7. Access Sharing**

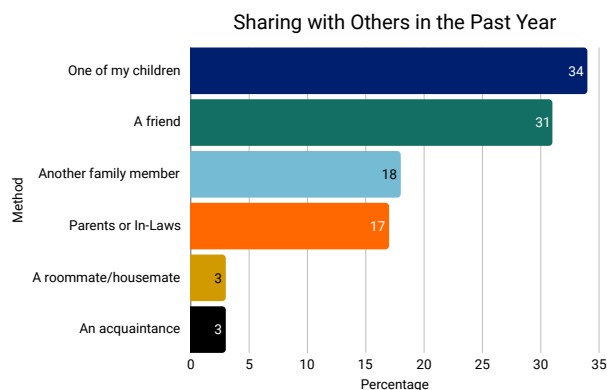
Seventy-four per cent of participants who used a lock screen reported that their partner could unlock their phone. An even higher number of participants (85%) said their partner had used their phone at least once in the last year.



**Figure 8. Past Year Sharing with Partner**

### Sharing Access with Other People

Although this study focused on sharing with partners, many participants reported sharing with others. About 34% reported sharing their phone with one of their children, and about 31% reported sharing with a friend. Around 17% to 18% reported sharing with another family member, parent or in-law. Only about three percent reported sharing with a roommate, housemate, or acquaintance.



**Figure 9. Sharing with Others**

About 34% of participants had never shared their phone with any of these people in the past year.



## Who Shares Their Phones?

### Demographic Characteristics

There were no significant differences in smartphone sharing by sex, income, Indigenous status, education or place of birth.<sup>[1]</sup> Age was the only demographic variable significantly associated with differences in sharing.<sup>[2]</sup> The overall linear trend was for sharing to decrease somewhat as age increased. However, this pattern is complicated by a) the fact that the association between age and sharing cannot be adequately described by a simple linear trend (in actuality, it goes up, down, and back up again), and b) age is associated with matters such as relationship status and duration. These more complex inter-relationships and non-linear patterns require additional exploration beyond the scope of the current report.

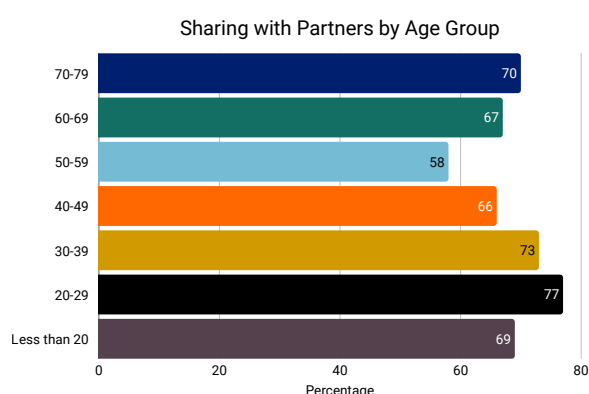


Figure 10. Sharing by Age

### Relationship Characteristics

**Relationship Status** - Unlike the small to non-existent associations between demographic characteristics and sharing, relationship status was more substantially related to phone sharing.

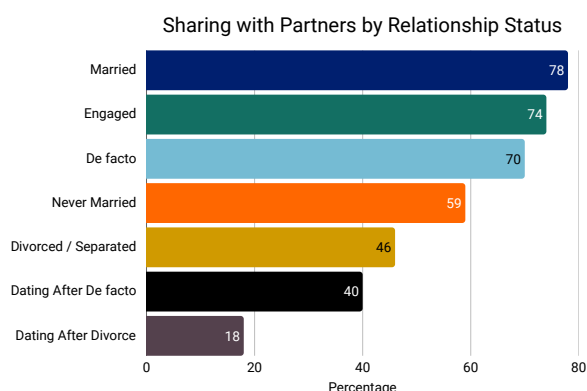


Figure 11. Sharing by Relationship Status

Our chart indicates that relationship categories typically associated with greater levels of commitment involve greater levels of sharing. Married participants were most likely to share (78%), followed closely by engaged participants (74%) and those in current de facto partnerships (70%). Never-married participants were not far behind (59%) these groups. Unsurprisingly, those who were divorced or separated and reported on their former partners reported lower levels of sharing during the prior relationship (46%). In comparison, those who began dating a new partner after the dissolution of their original partnerships reported the lowest level of sharing with the new partner (40% and 18%, respectively). Similarly to what we mentioned for the participant's age, there may be relevant interrelationships between relationship status, age, and relationship duration that require additional exploration beyond the scope of the current report.

**Relationship Duration** - Sharing increased as the duration of the relationship increased to about three years, at which point the sharing levelled off at nearly 75%. As before, there may be relevant interrelationships between relationship status, age, and relationship duration that require additional exploration beyond the scope of the current report.

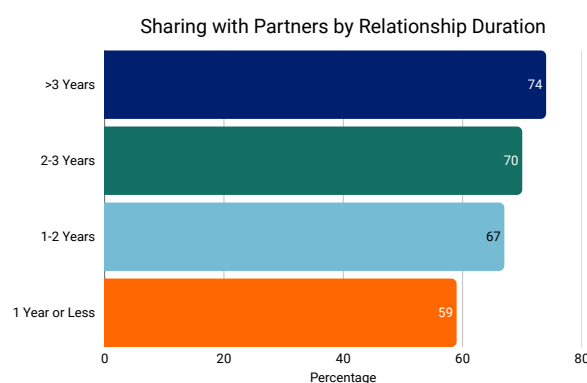


Figure 12. Sharing by Relationship Duration

[1] Australia versus overseas.

[2] At conventional  $p < .05$  levels of statistical significance.

## How did Sharing Start?

Most participants who shared access with their partners said they willingly offered their partner access to their phone (91%). Seven percent said their partner asked for access. Less than one percent said their partner demanded access, and almost one percent said they got access some other way. One percent were not sure how the access started.

## Reasons for Sharing

### Why Do People Share Access to Their Phone with Partners?

The most common reasons reported for sharing access to a phone with a partner were trust and convenience. The quotations from the interviews below are examples of typical comments about trust and access sharing.

"It's almost like an unspoken version of trust."

"I trust him with my life, so there's no reason why I shouldn't. If there is, then that in and of itself is concerning."

Figure 13 shows the percentage of participants endorsing a range of reasons for sharing access.

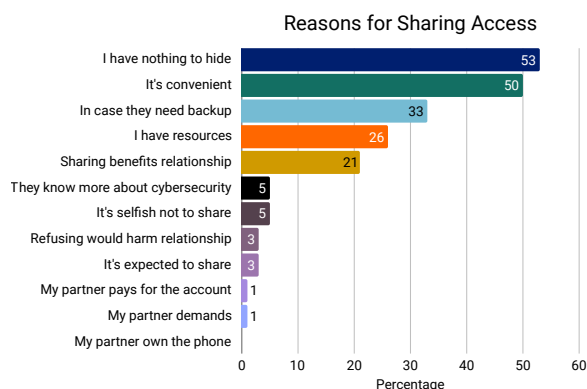


Figure 13. Reasons for Sharing Access

The most common reason participants gave for sharing access was "I have nothing to hide" (53%), closely followed by "It's convenient" (50%). A third of participants (33%) said they shared "In case their partner needed a backup device (because their battery died etc.)." Twenty-six percent said they shared because they "have resources the partner doesn't have (apps, subscriptions, better camera etc.)." Twenty-one percent said they shared because it benefits the relationship. Less common reasons were "My partner knows more about cybersecurity and can check my settings for me" (5%), and "It's selfish not to share" (5%). Three percent of participants said that "Refusing to share would have harmed our relationship" and "It's expected to share mobile access with your partner in my culture." One percent or fewer said they shared because their partner paid for the account, demanded access to their phone, or owned the phone.

## Privacy Practices

Participants who shared access to their phones with their partners reported using a variety of tactics to protect their privacy.

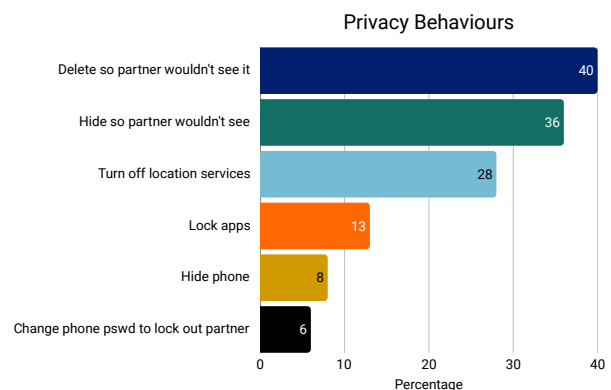
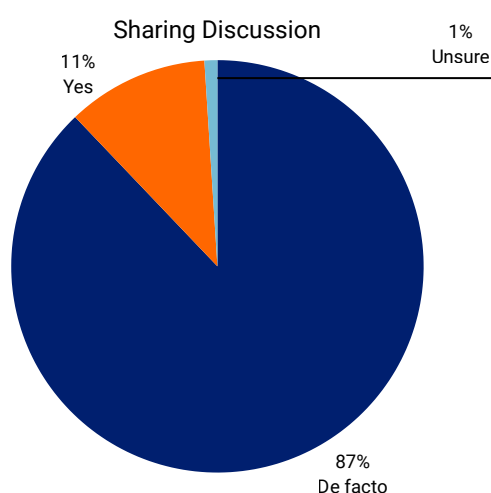


Figure 14. Privacy Behaviours

As shown in Figure 14, the most commonly used privacy practice was deleting something so the partner wouldn't see it (40%). Hiding something so the partner wouldn't see it was the second most common (36%). Turning off location services was used by 28% of participants. Locking apps (13%), hiding the phone (8%), and changing the password to lock out the partner (6%) were less common.

## Communication about Sharing

As noted above, 70% of Australians share credentials so their intimate partners can access their phones. However, fewer of these people reported having discussed their expectations or parameters for sharing. Only 11% of participants said they had discussed their expectations for sharing. Eighty-seven percent of participants had not discussed any rules or expectations for partners when using their phone. One percent were unsure whether they had or not.



**Figure 15. Sharing Discussion**

Those who hadn't had a conversation setting expectations for sharing talked about sharing access as part of trust in a relationship. For those who had an explicit discussion about sharing, the conversation included privacy issues and pragmatic considerations, as illustrated by the following quotes from the interviews.

"We did discuss that you can't just reply to everything without first asking or telling the other person, because you can't really reverse it once you've sent it out."

"I don't think we ever has a sit-down conversation, which I think is okay, it's one of those things where it usually makes more sense to negotiate as you go."

## DISCUSSION

This report presents findings from the first study of mobile phone sharing with intimate partners in Australia. Our research confirms that Australians regularly use smartphones for essential social, economic, educational, and health-related purposes. As described above, most Australians share access to their mobile phones with intimate partners. As might be expected, the more serious the relationship, the more likely participants were to share.

Most participants indicated that they shared voluntarily, for innocuous or prosocial reasons, such as convenience, as part of trust in the relationship. This aligns with prior research highlighting the centrality of convenience and trust in decisions to share or not share credentials and device access with partners [7,25,26]. Contrary to previous research that attributes phone sharing to financial need or cultural demands in discrete communities, our research finds that access sharing is widespread, even among individuals who have their own phones.

While this study focused on exploring mobile phone sharing in couples, the findings are useful to guide future research and policy on a broad range of device, account, and application sharing in family, friend, and carer contexts. The information gathered in this project provides new information to inform education about consumers' real-world mobile phone-sharing behaviours and their implications. This information is needed to educate consumers, telcos, cybersecurity bodies, and technology designers, as well as to promote communication about informed and consensual sharing.

Our findings also contribute to ongoing research on technology-facilitated abuse by filling a key knowledge gap about baseline technology-sharing behaviours in relationships and how people understand them. This information enables greater recognition of the circumstances in which sharing may be beneficial or harmful and how the meaning of the same behaviours can change depending on the context.

In Australia, private sector and government services are increasingly accessed online and via mobile delivery. Secure access to the Internet is more important than ever due to the ubiquity of mobile service interfaces and the reality of widespread sharing.

The Australian Digital Inclusion Index (ADII) uses a composite index of digital inclusion tracking access, affordability, and digital ability, including social digital ability [30]. ACCAN has previously supported research investigating barriers to digital inclusion [16,21], and technology-facilitated abuse [14], including unintended outcomes from family plans [29].

This study contributes to efforts to move beyond first-level digital inclusion, stepping back from deficit and harm-focused frames to understand consumers' everyday sharing behaviours and the thinking behind them. Our findings extend the focus of social digital inclusion beyond whether consumers can access the Internet to investigate the relational aspects and implications of mobile phone sharing. Information about why people share access to their phones and what sharing means to them is necessary to address the social factors shaping meaningful digital inclusion and consumer cybersecurity practices. Key findings are discussed below.

## Context is Key

The meaning and impact of decontextualised technology behaviours are highly ambiguous [3,10,11,13,14].

Accordingly, great care must be taken to capture the nuances of technology use and the context in which it occurs, to avoid distorting technology users' experiences.

For example, without information about the context, meaning, and impact for those involved, altruistic or innocuous technology behaviours and expectations about them (such as expectations that access or locations will be shared) can easily be misconstrued as abusive.

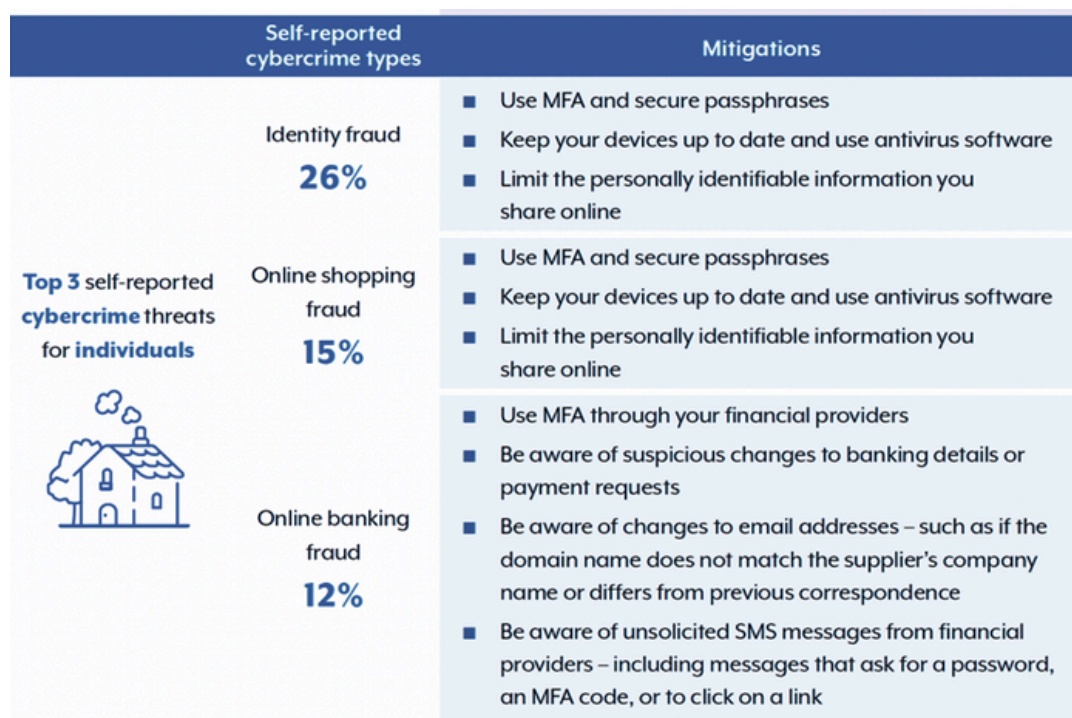
We found that age was associated with sharing behaviours, with people in their twenties being most likely to share and another bump in sharing amongst older people. These findings may indicate that young people are more likely to share access to their phones but only begin entering serious relationships where this behaviour is more common during their twenties. An increased likelihood of sharing was also found amongst our oldest participants. This may reflect older Australians' greater needs for support in maintaining access to essential communication tools in the ever-changing technology context.

## Inclusive Cybersecurity Threat Models are Needed

Our findings show that highly sensitive personal and financial information flows through Australians' personal smartphones. Widespread sharing in couples is a core context for understanding everyday smartphone use.

While this study did not focus on abuse, some participants discussed technology-facilitated abuse and other potentially problematic aspects of phone access. Given that intimate partners are the perpetrators in a sizeable portion of identity crime, financial abuse, and technology-facilitated abuse, and about 40% of marriages end in divorce, separation and abuse are essential considerations for cybersecurity design and policy.

The prevalence of access sharing points to the need for cybersecurity policies and designs that go beyond one-user/one-device models to accommodate how Australians use their phones in real life [26,28]. They also indicate a need for conversation about phone access sharing and its implications. Acknowledging this requires innovative approaches to cybersecurity. Mobile device, platform design, and cybersecurity policy must do more to take this reality into account. Our findings have important implications for interpersonal privacy, cybersecurity, and cybercrime.



**Figure 16.**  
**Excerpt from**  
**ACSC Annual**  
**Cyber Threat**  
**Report**

Despite Australia's focus on threats to national infrastructure, government, and companies, the financial cost of cybercrimes against individuals is increasing faster than that for businesses [2]. In addition, healthcare and social assistance were the most frequently reported non-government sectors reporting cybersecurity incidents during 2022-2023. The most common types of cybercrime affecting individuals were identity fraud (26%), online shopping fraud (15%), and online banking fraud (12%) [2]. While these types of cybercrime are particularly vulnerable to intimate threats and have been identified in research on technology-facilitated domestic violence, the ACSC's threat mitigation advice is focused on stranger danger. For example, this excerpt from ACSC's Annual Cyber Threat Report 2023–2024 lists the top 3 self-reported cybercrime threats for individuals. The mitigations each target threats from strangers [2].

In Australia, 20% of identity theft perpetrators identified by police were current or former intimate partners or individuals related to an ex-partner [19]. These crimes, committed by known persons, are widely understood to be under-reported, particularly when perpetrators use credentials their partners have willingly shared. This suggests that the actual rate of victimisation by someone known to the victim is likely even higher.

This lack of recognition persists despite a high-profile campaign by Australia's largest corporation, Commonwealth Bank, which has acknowledged the strong link between financial cybercrime and domestic violence. In a 2020 report, the bank revealed that over 623,000 women and men were subjected to financial abuse by a current or former intimate partner in that year alone [5]. The report estimated the direct costs of this abuse at \$5.7 billion for victims and an additional \$5.2 billion in broader economic costs. Accordingly, we recommend integrating the Intimate Threat Model into cybersecurity policy and practice.

Findings from this study contribute to the literature on interpersonal insider threats to cybersecurity [6,10,14,18] and the Intimate Threat Model for cybersecurity [11,14]. The implications of the Intimate Threat Model underscore the need for greater transparency and control for smartphone users, allowing them to share what they want on their devices while maintaining their privacy. Because the implications of smartphone sharing change over time according to the status of the relationship, smartphone users need to be able to quickly and easily find and change permissions when necessary. Beyond cybersecurity, legal frameworks need to be adjusted to be able to account for coerced debt and other abuses where credentials or devices have been shared voluntarily due to fraud, coercion, or force [24, 27].



# CONCLUSION

The smartphone sharing practices identified in this study reveal a disconnect between cybersecurity policy, design, and advice and the actual ways Australians use their phones. Due to its prevalence, access sharing is as important, if not more important, to cybersecurity than sharing a single device. Accordingly, our findings point to recommendations for future research and policy priorities.

**Future Research** - This was the first study investigating everyday mobile phone sharing in Australian couples. Evidence about technology sharing is beginning to emerge as part of studies on digital inclusion. However, this study points to additional directions for further research to understand the dynamics and impact of widespread mobile phone sharing. Our findings can inform future research in other countries with larger samples and additional cohorts of diverse consumers.

**Cultural Factors** - First, our findings suggest that social and cultural norms surrounding sharing practices are salient for all Australians, not just those who share devices due to financial necessity. Research on the cultural aspects of phone sharing should be inclusive to build understanding of how our social ecology, including individual preferences, family dynamics, communities, and culture, shapes everyone's technology behaviours.

**Diverse Communities** - While our social environments shape everyone's technology use, specific groups of people will have particular experiences and needs that we won't know about if we don't study them. Some key populations to study include families with children, people with disabilities who rely on technology for different uses than people without disabilities, and older people who often rely on assistance to use technology. More research is also needed on mobile phone sharing in Indigenous communities. Prior research on cybersecurity indicates that unique cultural dynamics shape phone sharing practices, risks, and benefits in remote Aboriginal communities [25]. However, to date, no research has focused on phone sharing in urban Aboriginal communities or among Torres Strait Islander people. Research led by Indigenous communities and researchers should be funded to fill this gap.

**Existing and Future Technologies** - Given the extent of access sharing, more research is needed to identify what features already exist to promote cybersecurity, privacy and informed consent for shared mobile phones, whether/how people are using them, and what new features are needed.

**Limitations** - This study, like all research, has several limitations that should be considered when interpreting the findings. One limitation concerns our recruitment strategy. Although social media advertising enabled us to reach a broad and diverse audience, it also introduced potential self-selection bias. Individuals who respond to online advertisements may differ in important ways from those who do not. This method may reduce reliance on habitual survey-takers commonly found in commercial panels, but it does not eliminate all concerns about representativeness. Our approach prioritised behavioural relevance over demographic quotas, which may still limit the generalizability of our findings. That said, our major findings regarding sharing behaviours were largely consistent across demographic categories – except for age – suggesting that any self-selection biases are unlikely to have meaningfully influenced the results.

Another limitation relates to the nature of survey research itself. Surveys are not always well-suited to capturing complex or abstract constructs such as trust. While we conducted follow-up interviews with a small number of participants to gain deeper insight, a more extensive qualitative component would likely be beneficial in fully exploring these nuanced issues.

Finally, the analyses presented here were limited in their ability to disentangle the effects of interrelated demographic variables. Although we examined mobile phone sharing behaviours across age, relationship status, and relationship duration individually, these factors are clearly interconnected. For instance, older individuals are more likely to be in longer and more serious relationships. Future analyses using multivariate methods could help clarify the unique contributions of each variable and better illuminate their combined influence on sharing behaviours.

# AUTHORS

## MOLLY DRAGIEWICZ

**Molly Dragiewicz** is Professor of Criminology and Criminal Justice at Griffith University. She is a global leader in research on domestic violence survivors' experiences of technology-facilitated coercive control. She led the first Australian study on technology-facilitated domestic violence and the world-first study investigating how children are involved in technology-facilitated abuse in the context of adult domestic violence. Her work is frequently cited in international policy documents to prevent cybercrime, promote safe digital inclusion, end gender-based violence, and promote gender equity. To learn more about her research, visit <https://www.mollydragiewicz.com/>.

## JEFFREY ACKERMAN

**Jeffrey Ackerman** is Senior Lecturer in the School of Criminology and Criminal Justice at Griffith University. Ackerman is an expert in complex survey design and statistical analysis within the context of domestic violence and related forms of offending and victimisation. He led the survey design and analysis for the 2020 world-first study on children's involvement in technology-facilitated abuse in the context of adult domestic violence, funded by eSafety. Ackerman also collaborated on survey design for a pilot study of smartphone credential sharing with Periwinkle Doerfler, who was then a PhD candidate at New York University.

## MARIANNE HAALAND

**Marianne Haaland** is a PhD student in the School of Criminology and Criminal Justice at Griffith University, where she is completing a research project on women's disclosure of unwanted sexual experiences with intimate partners. Her research interests include domestic and family violence, intimate partner violence, and sexual violence against women.

# REFERENCES

1. Akter, M., Alghamdi, L., Kropczynski, J., Lipford, H. R., & Wisniewski, P. J. (2023). It takes a village: A case for including extended family members in the joint oversight of family-based privacy and security for mobile smartphones. *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–7. <https://doi.org/10.1145/3544549.3585904>
2. Australian Cyber Security Centre. (2024). *Annual Cyber Threat Report 2023–2024*. Australian Government, Australian Signals Directorate.
3. Brown, C., & Hegarty, K. (2018). Digital dating abuse measures: A critical review. *Aggression and Violent Behavior*, 40, 44–59. <https://doi.org/10.1016/j.avb.2018.03.003>
4. Castells, M., Fernandez-Ardevol, M., Qiu, J. L., & Sey, A. (2006). *Mobile communication and society: A global perspective*. MIT Press.
5. Deloitte Access Economics. (2022). *The cost of financial abuse in Australia*. Commonwealth Bank Australia. <https://www.commbank.com.au/content/dam/caas/newsroom/docs/Cost%20of%20financial%20abuse%20in%20Australia.pdf>
6. Doerfler, P. (2019, January). Something you have and someone you know: Designing for interpersonal security. *USENIX: The Advanced Computing Systems Association*. Enigma, Burlingame, CA. [https://www.youtube.com/watch?v=VBZ1IPdRjzq&feature=emb\\_title](https://www.youtube.com/watch?v=VBZ1IPdRjzq&feature=emb_title)
7. Doerfler, P., Turk, K. I., Geeng, C., McCoy, D., Ackerman, J., & Dragiewicz, M. (2024). *Privacy or transparency? Negotiated smartphone access as a signifier of trust in romantic relationships*. <https://doi.org/10.48550/arXiv.2407.04906>
8. Donner, J. (2008). Research approaches to mobile use in the developing world: A review of the literature. *The Information Society*, 24(3), 140–159. <https://doi.org/10.1080/01972240802019970>
9. Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, 59(3), 551–570. Scopus. <https://doi.org/10.1093/bjc/azy068>
10. Dragiewicz, M. (2023). Best-practice principles for measurement of technology facilitated coercive control. In B. Harris & D. Woodlock (Eds.), *Technology and domestic and family violence: Victimisation, perpetration and responses* (pp. 49–62). Taylor & Francis Group. <https://www.taylorfrancis.com/books/edit/10.4324/9780429316098/technology-domestic-family-violence-bridget-harris-delanie-woodlock>
11. Dragiewicz, M. A., O'Leary, P., Ackerman, J., Bond, C., Foo, E., Young, A., & Reid, C. (2020). *Children and technology-facilitated abuse in domestic and family violence situations: Full report* (eSafety Research). eSafety Commissioner & Australian Government. <https://www.esafety.gov.au/sites/default/files/2020-12/Children%20and%20technology-facilitated%20abuse%20-%20Summary%20report.pdf>
12. Dragiewicz, M., Doerfler, P., & Woodlock, D. (2022). *Technology-facilitated domestic violence and the intimate threat model for cybersecurity*.
13. Dragiewicz, M., Harris, B., Woodlock, D., & Salter, M. (2021). Digital media and domestic violence in Australia: Essential contexts. *Journal of Gender-Based Violence*, 5(3), 377–393. <https://doi.org/10.1332/239868021X16153782923978>
14. Dragiewicz, M., Harris, B., Woodlock, D., Salter, M., Easton, H., Lynch, A., Campbell, H., Leach, J., & Milne, L. (2019). *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime*. QUT & Australian Communications Consumer Action Network (ACCAN). <https://web.archive.org/web/20250402144237/https://accan.org.au/Domestic%20Violence%20and%20Communication%20Technology%20final%20report%2020190801.pdf>
15. Dragiewicz, M., Woodlock, D., Salter, M., & Harris, B. (2022). "What's mum's password?": Australian mothers' perceptions of children's involvement in technology-facilitated coercive control. *Journal of Family Violence*, 37(137), 137–149. <https://doi.org/10.1007/s10896-021-00283-4>
16. Dulfer, A. N., Smith, C., van Holstein, E., Garner, A., Rueda, L. A., Alexander, L., Hamed, S., Cavanagh, K., & Ruppanner, L. (2022). *Understanding digital inequality: An analysis of unequal connectivity in Carlton Housing Estate, Melbourne, Victoria*. Australian Communications Consumer Action Network.
17. Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM Human-Computer Interaction*, 1(CSCW), 46:1–46:22. <https://doi.org/10.1145/3134681>
18. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). A stalker's paradise: How intimate partner abusers exploit technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI'188*, 1–13. <https://doi.org/10.1145/3173574.3174241>
19. Goode, S. (2017). *Identity theft and Australian telecommunications: Case analysis*. Australian Communications Consumer Action Network.
20. Henry, N., Powell, A., & Flynn, A. (2017). *Not just "revenge pornography": Australians' experiences of image-based abuse*. RMIT University, Gendered Violence and Abuse Research Alliance, Centre for Global Research, Centre for Applied Social Research.
21. Humphry, J. (2014). *Homeless and connected: Mobile phones and the Internet in the lives of homeless Australians*. Australian Communications Consumer Action Network.
22. Karlson, A. K., Brush, A. J. B., & Schechter, S. (2009). Can I borrow your phone? Understanding concerns when sharing mobile phones. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1647–1650. <https://doi.org/10.1145/1518701.1518953>
23. Lariccia, F. (2023). *Global smartphone penetration 2016–2023*. Statista. <https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/>

24. Littwin, A. (2012). Coerced debt: The role of consumer credit in domestic violence. *California Law Review*, 100(4), 951–1026.  
<http://gateway.library.qut.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=78130174&site=ehost-live&scope=site>
25. Rennie, E., Yunkaporta, T., & Holcombe-James, I. (2018). *Cyber safety in remote Aboriginal communities: Final report*. Digital Ethnography Research Centre, RMIT University.  
<http://apo.org.au/node/172076>
26. Singh, S. (2009). Balancing separateness and jointness of money in relationships: The design of bank accounts in australia and india. *Internationalization, Design and Global Development*, 505–514. [https://doi.org/10.1007/978-3-642-02767-3\\_56](https://doi.org/10.1007/978-3-642-02767-3_56)
27. Singh, S. (2022). *Domestic economic abuse: The violence of money*. Routledge.
28. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Security design based on social and cultural practice: Sharing of passwords. In N. Aykin (Ed.), *Usability and Internationalization. Global and Local User Interfaces* (Vol. 4560, pp. 476–485). Springer Berlin Heidelberg.  
[https://doi.org/10.1007/978-3-540-73289-1\\_55](https://doi.org/10.1007/978-3-540-73289-1_55)
29. Sulikowski, D., Brunton, R. and Shin, M. (2022) *An assessment of the risks family plans present for users vulnerable to domestic and family violence*. Charles Sturt University & ACCAN.
30. Thomas, J., McCosker, A., Parkinson, S., Hegarty, K., Featherstone, D., Kennedy, J., Holcombe-James, I., Ormond-Parker, L., Ganley, L., & Valenta, L. (2023). *Measuring Australia's digital divide: The Australian Digital Inclusion Index 2023*. RMIT University. <https://doi.org/10.25916/528S-NY91>
31. WeAreSocial. (2024). *Digital 2024: Australia*.  
<https://datareportal.com/reports/digital-2024-australia>
32. Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women*, 23(5), 584–602.  
<https://doi.org/10.1177/1077801216646277>



# ACCAN



## Contact Us :



Phone Number  
**02 9288 4000**



Email Address  
**info@accan.org.au**



Website Address  
**accan.org.au**