An assessment of the risks Family Plans present for users vulnerable to domestic and family violence

Charles Sturt University

accan

An assessment of the risks Family Plans present for users vulnerable to domestic and family violence

Danielle Sulikowski
Robyn Brunton
Myoungju Shin

May, 2022

Charles Sturt University

accan

An assessment of the risks Family Plans present for users vulnerable to domestic and family violence

Authored by **Danielle Sulikowski, Robyn Brunton, and Myoungju Shin**

Published in **2022**

This project was funded by a grant from the Australian Communications Consumer Action Network (ACCAN).

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.

Charles Sturt University
Website: www.csu.edu.au
Email: dsulikowski@csu.edu.au
Telephone: 02 6338 4778

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: 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: https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service/service-features/national-relay-service-call-numbers

ISBN: **978-1-921974-77-9**
Cover image: **Design by Nathaniel Morrison with images from Shutterstock**

This work can be cited as: Sulikowski, D., Brunton, R., & Shin, M. 2022, *An assessment of the risks Family Plans present for users vulnerable to domestic and family violence*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Table of Contents i

List of Tables iii

1. Acknowledgements 1

2. Executive Summary 2

3. Glossary 4

4. Introduction 5

4.1 Customers, Users and Authorised Users 5

4.2 Domestic and Family Violence 5

4.2.1 Risks beyond surveillance 7

4.2.2 Risk awareness 7

4.3 Aims of the Current Project 8

4.3.1 First aim 8

4.3.2 Second aim 8

5. Methodology 10

5.1 Costs and structure of Family Plan arrangements 10

5.2 Data available to Customers 10

6. Results 11

6.1 Summary of Telcos' Family Plan arrangements 11

6.1.1 Telstra 11

6.1.2 Optus 11

6.1.3 Vodafone 11

6.1.4 Consent to collect personal data 11

6.1.5 Discussion 12

6.2 Data available to Customers 13

6.2.1 Usage data 13

6.2.2 Location data 13

6.2.3 Location tracking features 14

6.2.4 Discussion 15

6.3 Financial incentives to use Family Plans 16

6.3.1 Telstra 17
6.3.2 Optus 18
6.3.3 Vodafone 20
6.3.4 Discussion 21
7. Conclusions 23
7.1 Family Plans and consent to share data 23
7.2 Risks of both overt and covert surveillance 23
7.3 Opaque cost-saving measures 23
8. Recommendations 24
8.1 Recommendation 1 – Provide extensive information 24
8.2 Recommendation 2 – Register primary Users 24
8.3 Recommendation 3 – Encourage User authorisation 24
8.4 Recommendation 4 – Offer dual contracts 24
9. Authors 26
10. References 27

List of Tables

Table 1 Telstra Upfront Mobile Plans for Individual Users 17
Table 2 Potential savings for Telstra Family Plans, compared to individual user plans 18
Table 3 Optus Choice Mobile Plans for Individual Users 19
Table 4 Potential savings for Optus Family Plans, compared to individual user plans 19
Table 5 Vodafone Mobile Plans for Individual Users 20
Table 6 Potential savings for Vodafone Family Plans, compared to individual user plans 21

1. Acknowledgements

Thank you to Lifeline Central West (NSW), in particular, Stephanie Robinson and Jodie Williams, for their expert input into this report. We acknowledge the assistance of Laura Delli-Pizzi for providing us with thorough and reliable research assistance throughout this project. We would also like to thank Tanya Karliychuk and Rebekah Sarkoezy from ACCAN for their support and guidance during the application process and all throughout the project as well. Your enthusiasm was always welcome and uplifting during a very difficult and COVID-19 interrupted year.

2. Executive Summary

This report investigated the surveillance risks associated with so-called Family Plans (i.e., mobile phone/landline in multiple names) offered by most Australian Telecommunications companies (Telcos). Data share arrangements these Family Plans offer can be exploited to harm those involved in family and domestic violence. It is therefore important to understand the surveillance and privacy risks associated with these plans. To this end, we first collated the information regarding Family Plans the three major Australian Telcos (i.e., Telstra, Optus, and Vodafone) provide their consumers. Second, we investigated the strategies used to motivate consumers to sign up for Family Plans.

All three Telcos offer Family Plan arrangements that pose surveillance and privacy invasion risks. For all Telcos, one customer has access to device usage details for all users. The customer also has control over allowing other users on the plan reciprocal access about themselves. Of concern is that none of the Telcos makes any substantial effort to seek informed consent from all users regarding the collection and storage of their data and the availability of that data to the customer.

All three Telcos provide information on usage data (e.g., call, SMS, and data information). This information does not extend to detailed information on the numbers from which calls and messages are received, the content of any SMS messages or the location of any device associated with the plan. However, all three Telcos state that location data of all phones on the plan are collected and stored. Telstra customers may obtain this data through direct request and an associated fee whereas the process for gaining this information for Optus and Vodafone was not explicit.

Telstra and Optus both have features that enable location tracking, whereas Vodafone does not. Telstra's Device Locator is a feature that can be set up on each device and when enabled, provides information on the device's last known location based on its connection to the mobile network. In contrast, Optus offer all customers a free subscription to a third-party app that permits monitoring. However, unlike Telstra's Device Locator, this third-party app must be installed and is not linked to the customer's Optus account.

All three Telcos provide incentives for customers to enter these Family Plan arrangements. These incentives provide discounts for combining multiple plans under a single customer account which is desirable given the affordability of these services is a substantial issue for many Australians.

Based on these findings, we offer four recommendations to reduce or eliminate surveillance and privacy invasion risks associated with Family Plans. Three of our four recommendations are concerned with improving transparency and awareness around data sharing in the context of Family Plan arrangements to ameliorate the risks that these arrangements pose. Our fourth recommendation, however, is to replace Family Plans with dual contract offers so that each individual adult is their own recognised customer. In an age where the importance of maintaining privacy over personal data is becoming increasingly recognised, it is no longer appropriate for Telcos to entice the users of their services to sacrifice this privacy in the name of a better deal. Personal data can be weaponised in domestic and family violence scenarios and Telcos have an obligation to educate their customer base about these risks, and encourage privacy best practice. Family Plans

that necessitate personal data disclosure among multiple device users are not commensurate with these obligations.

3. Glossary

Account holder. Also known as the Customer. The individual with the legal liability for the account and all charges.

Account interface. An online platform provided by Telcos whereby Customers can access account information.

Authorised user. A User who is granted authority (by the Customer) to access account information.

Bot. A software application that runs automated tasks. Used in live chats to provide automated feedback and information.

Customer. See account holder

Cyber dating abuse. Abuse that is perpetuated through technology**.**

Cyberstalking. The use of technology to stalk or harass.

Device. Usually, a mobile phone that enables access to the service provided by the Telco.

Domestic and family violence. A broad term for all acts of abuse occurring between current or former intimate partners, and can extend to other family members, including children.

Family Plan. A plan offered by Telcos that has financial incentives where multiple Users exist on one Customer's account. Also known as multiple user plans.

Live chat. A means of communication on the internet provided to customers to find information or answer queries. The company representative may be an individual or a 'bot'.

Multiple user plans. See Family Plans

SIM. The Subscriber Identity Module contains a microchip that allows a device to connect to a mobile network.

Telco. Any Australian Telecommunications company

User. Any other individual who has a device on the Customer's account.

4. Introduction

This project comprises a preliminary investigation and collation of the surveillance risks presented by so-called Family Plans offered by most Australian Telecommunications companies (Telcos), wherein one **Customer** (the account holder) holds an account with a Telco covering multiple mobile devices. These devices are used by other members of the Customer's family (**Users**) who do not have accounts with the Telco. The **Customer** may (or may not) choose to grant a User authority to access the account information. If such authority is granted the User becomes an **authorised User**. Such arrangements can provide the **Customer** (and any **authorised Users**) with access to information about how other family members are using their devices, which can compromise the safety and security of Users who are vulnerable to domestic and family violence.

4.1 Customers, Users and Authorised Users

Unlike bank accounts and mortgages, accounts with Telcos (whether for mobile phones or landlines) cannot be held in multiple names. Only one customer is recognised for each account as legislated by the Telecommunications Numbering Plan (2015, ch I pt III s 15; see also Communications Alliance Ltd, 2018, pg. 9). Where services for multiple mobile phones that are being used by multiple individual users are provided under a single account, the additional individuals are **Users**. In this situation (where multiple Users exist on a Customer's account) it is referred to as a Family Plan or multiple user plan. For the purposes of this report, we refer to any such plan as a Family Plan. In Family Plans, the Customer has sole liability for all fees and charges accrued on all listed devices and controls access to all User information collected via the account.

Customers may choose to grant Users authority to access information and transact (e.g., purchase more data usage) on the account. When this occurs, the User is called an authorised User and provides them with the same level of access to account information that the Customer has. Authorised Users also can modify and manage the account as though they were the Customer. Providing such authority, however, does not transfer any financial liabilities. This liability remains with the Customer. Customers are also able to revoke this authority at any time. Therefore, when multiple members of one household have their mobile phones on a single account, just one (adult) member of the household is the formal Customer. Other (adult) Users may or may not be granted authority to access the account, and this authority is entirely at the discretion of the Customer.

4.2 Domestic and Family Violence

Domestic violence (also referred to as intimate partner violence), refers broadly to all acts of abuse occurring between current or former intimate partners, and can extend to other family members, including children (Coumarelos, 2019). Such acts include physical violence and sexual assault, stalking and monitoring, as well as verbal, emotional, financial, and psychological abuse (Morgan & Chadwick 2009). Coercive control, a form of psychological abuse, occurs when one person restricts the freedoms of another by inducing a persistent state of fear (frequently through violence or the threat of violence, Hamberger et al., 2017). Family violence is a broader term (often preferred by the Indigenous Australian community, Stanley et al., 2003) that describes similar acts occurring between other family members who may or may not be co-habiting. This includes siblings and can also be

perpetrated by adolescent or adult children on their parents who in some cases are elderly.

'Domestic and family violence' is often considered synonymous with 'violence against women' (for example Australian state and federal governments' strategies for tackling domestic and family violence are contained within The National Plan to Reduce Violence against Women and their Children, 2010 – 2022, Council of Australian Governments, 2010). The gendered nature of domestic and family violence is, however, not one-sided. Since 1989, women have comprised ~75% (and men, ~25%) of the victims of intimate partner homicide (Bricknell & Doherty, 2021). Other sources estimate that more than 35% of the victims of intimate partner violence are men, and the overwhelming majority of these men (~95%) experience intimate partner violence at the hands of a female perpetrator. Moreover, intimate partner violence among same-sex relationships may have a higher incidence than among heterosexual couples (Rollè et al., 2018). Beyond homicide and physical abuse, more even proportions of men and women experience emotional abuse at the hands of a partner (i.e., 16% and 23% respectively, Australian Bureau of Statistics, 2017; Felson & Outlaw, 2007). While these estimates are sobering, concerningly, reports of domestic and family violence are on an upward trend (NSW Bureau of Crime Statistics and Research, 2020).

Pertinent to the current study, very similar proportions of men and women (about 1 in 10 of those experiencing emotional abuse from a partner) report that a current partner kept track of their movements and whom they were socialising with (Australian Bureau of Statistics, 2017). This is consistent with surveillance behaviours (e.g., GPS tracking) an identified risk factor for intimate partner violence perpetration (Toivonen & Backhouse, 2018). From the perspective of perpetrators, men and women tend to report engaging in similar levels of cyber dating abuse and cyberstalking of their long-term partners (Borajo et al., 2015; March et al., 2021;). This 'cyber abuse' includes using mobile phones and call records to monitor whom a partner is communicating with (see also: Deans & Bhogal, 2019; Smoker & March, 2017). Therefore, unlike physical forms of domestic and family violence, the surveillance risks Family Plan arrangements present are much more likely to be distributed symmetrically across both men and women.

When Family Plan contracts are entered into, Users may be entirely comfortable with the Customer (or other authorised User) accessing their usage data. In the context of a healthy relationship, the surveillance risks may seem negligible. The risks these arrangements pose are much more likely to be realised, however, as a relationship becomes coercive or violent. Once a relationship becomes coercive or violent, of course, it becomes much more difficult for any user (whether they be the Customer, an authorised User, or another unlisted User) to revoke this arrangement.

Potential threats to a relationship are known to be triggers of domestic and family violence. Such threats include perceived or actual infidelity (Arnocky et al., 2015; Nemeth et al., 2012) and intentions to leave the relationship. Separation, or imminent separation, often escalates or precipitates domestic and family violence (Brownridge, 2006). Perpetrators of domestic and family violence often seek control over many aspects of their partner's lives (Hamberger et al., 2017). Therefore, even though Customers retain the discretion to revoke other Users' authorisations, in a domestic and family violence situation, such revocation could be a catalyst for escalated abuse (in circumstances where an authorised User is the perpetrator). If the User perceives the revocation of their authorisation as an indicator that the Customer is hiding something, they may use threats of violence and other coercive tactics to ensure that their authorisation continues. Alternatively, when

the Customer is the perpetrator of the abuse, they can easily revoke another User's authorisation, turning a scenario of shared mutual access to private information into a one-sided tool for surveillance. As such, Customers and Users (whether authorised or not) may both be placed at risk of surveillance under Family Plan arrangements.

The above hypothetical scenarios presume some knowledge on the part of the User concerning the device usage information the Customer can access via their Telco's account interface. This presumption is unlikely to apply to all Users. It remains unclear what proportion of either Telco Customers, or Users, are aware of the privacy implications of being party to Family Plan arrangements. Some Customers and Users may agree to Family Plan arrangements when they perceive their relationship to be healthy and do not foresee a time where they would require privacy from their partner. Other individuals, however, may enter Family Plan arrangements naïvely, completely unaware that the arrangement makes their usage data available to the Customer (or another authorised User). They may be unaware that they are not a Customer and do not have ownership of their service. Family Plans entered under these circumstances may present an even greater risk. For example, Users unaware that their data can be accessed by their partner may use their device to contact domestic and family violence services, or a family lawyer, unwittingly signalling their intention to leave their abusive partner. As well as risking an escalation in abuse, such a lack of awareness may facilitate a perpetrator's long-term, covert surveillance of their partner.

4.2.1 Risks beyond surveillance

This report is primarily concerned with the surveillance and privacy risks presented by Family Plan arrangements. Surveillance risks are not the only risks of harm that Family Plans present in the context of domestic and family violence. In cases where the abuser is the User of a device, they may accumulate substantial debt in the Customer's name. Inability to settle this debt could affect the Customer's credit rating, an outcome with substantial and potential long-term flow-on effects such as difficulty securing loans, new phone plans, rental accommodation, or higher loan interest being charged.

In cases where the Customer is the perpetrator of abuse, they own the phone service the User (i.e., the victim) is using. They have the authority to suspend or cancel the service at any time or refuse to give permission for the number to be transferred to the User. If the device was also purchased on the plan, the Customer also owns the phone. This means that they can report the device as stolen and request that it be blocked, preventing it from being used again, even if a new SIM is obtained. The above actions could negatively impact the User in terms of the inconvenience and isolation that a sudden suspension/cancellation of service could cause and the financial impacts of having to acquire a new device.

4.2.2 Risk awareness

The Royal Commission into Family Violence (State of Victoria, 2016) recommended changes to the telecommunications industry to permit Telcos to better support victims of domestic and family violence. In response, changes were made to the Telecommunications Consumer Protections Code (TCP Code, Communications Alliance Ltd, 2019) to acknowledge domestic and family violence as a cause of financial hardship. Industry guidelines for assisting customers experiencing domestic and family violence were also established (Communications Alliance Ltd, 2018).

These guidelines contain extensive guidance to Telcos on the importance of having appropriately trained frontline staff to deal with customers experiencing domestic and family violence. They acknowledge many of the ways in which mobile phones may be used to perpetrate domestic and family violence (including surveillance, account monitoring and financial abuse). The guideline also addresses the need for Telcos to implement processes that would permit Users experiencing domestic and family violence to take ownership of their service from the perpetrator. Recent research, however, suggests that these aspects of the guidelines have not been embraced by all Telcos (Dragiewicz et al., 2019, p. 31).

The guidelines acknowledge the privacy, surveillance, and financial risks presented by allowing the devices of multiple Users to be listed in a single account in the name of one User. The guidelines indicate that the Customer/User distinction can be "exploited by perpetrators in domestic and violence situations" (Communications Alliance Ltd, 2018, p. 9.) These guidelines focus on when a Customer (or User) brings the domestic and family violence they are enduring to the Telco's attention, however, by then it may be too late to prevent many of the harms that Family Plan arrangements can lead to. Few to no guidelines are in place to encourage Telcos to reduce harm by addressing their policies and practices when Family Plans are being contractually secured.

4.3 Aims of the Current Project

The aims of the current project were twofold. We first examined the information Telcos provide consumers and second, we investigated how consumers are incentivised by Telcos to 'sign-up' for Family Plans.

4.3.1 First aim

A key defence for a potential victim of domestic and family violence against surveillance is to know the information that an abusive partner is able to access and how they can access it. With this knowledge, a vulnerable person may regain some control over their information, including how much their partner can access. To this end, we sought to document the usage data and other available information available to Customers (and authorised Users) via the platforms of the three major Australian Telcos (i.e., Telstra Corporation Limited [Telstra], Singtel Optus Pty Limited [Optus], and Vodafone Australia [Vodafone]) for all devices included on the one account. Therefore, our first aim was to:

1. Investigate and document the information that Customers (and authorised Users) of the three major Telcos, can obtain about other Users on their Family Plan.

4.3.2 Second aim

One way to mitigate the surveillance risks of Family Plans is to advise consumers to avoid them and ensure that all adults are individually recognised Customers, with their own separate Telco accounts. However, mobile phone plans in Australia are expensive. Cost of living pressures mean that consumers are price-sensitive, and a substantial proportion of individuals are either unable or barely able to afford their monthly mobile phone bill (Thomas et al., 2021). As such, even modest savings associated with a Family Plan arrangement can be a substantial driver of consumer decision-making. Furthermore, from the perspective of Telcos, the incremental discounts offered for additional devices and services added to Family Plans increase their market share. That is, one Customer's

family members may be more likely to be added to that Customer's plan to maximise discounts rather than to seek the services of another Telco. We therefore sought to quantify the savings offered to consumers who elect to take advantage of Family Plans. Inversely, these savings represent the financial costs consumers would incur to avoid Family Plans and the inherent surveillance risks that these present. Therefore, our second aim was to:

2. Investigate the costs savings available to consumers by taking out Family Plans from the three major Telcos, for multiple devices and services, compared to taking out multiple individual plans to cover those same devices and services.

5. Methodology

Information was gathered on Family Plans offered by Telstra, Optus, and Vodafone between August 2021 and January 2022. The following sources and methods were used to collect data.

5.1 Costs and structure of Family Plan arrangements

We accessed the following websites (including additional pages and documents linked therein) during August 2021 to determine currently available plans and bundle options:

Telstra (https://www.telstra.com.au/mobile-phones/sim-only-plans),

Optus (https://www.optus.com.au/mobile/plans/shop),

Vodafone (https://www.vodafone.com.au/plans/sim-only).

Plans available during this month provided the basis for the analyses presented in Section 6.3 Financial incentives to use Family Plans. Findings reported in Sections 5.1 Costs and structure of Family Plan arrangements) and 6.3 Financial incentives to use Family Plans) were based on the website descriptions of plans and the Terms and Conditions and Critical Information Summary documents available on these websites. Additional URLs are provided where specific documents are referred to throughout the Results section. If these sites were subsequently accessed after August 2021 for any additional verification, the later access times are noted.

5.2 Data available to Customers

To verify the usage data available to Customers, the research team inspected the online account interfaces for Telstra (My Telstra), Optus (My Account) and Vodafone, (My Vodafone). Members of the research team had access to these portals via their personal mobile accounts, and we relied upon this access for these inspections.

To verify how a User's location may be tracked in real-time, we also inspected Telstra's Device Locator information page and Optus' McAfee Safe Family App .

To verify the location data that the Telcos retain, we consulted the Privacy Policies of Telstra, Optus, and Vodafone. Furthermore, to verify the circumstances under which these location data may be released to Customers, we consulted online information about requesting access to data from Telstra, Optus, and Vodafone.

We verified the information provided from the above sources via the online live chat functions and face-to-face consultations instore for each of the three Telcos (with dates as relevant provided in the Results section). This was also done to ensure consistency and veracity of the information between 'bots' and in-store representatives of the Telcos.

6. Results

6.1 Summary of Telcos' Family Plan arrangements

Telstra, Optus, and Vodafone all offer versions of Family Plan arrangements. Key details of these arrangements (current as of August 2021) for the different Telcos are outlined below.

6.1.1 Telstra

Telstra permits Customers to share excess monthly data allowances between as many as ten eligible post-paid plans on one account. The potential for Users to have excess data to share is derived from the structure of Telstra's eligible plans, which have monthly data usage limits of 40GB, 80GB, 120GB, and 180GB. Therefore, if a User typically uses 15GB a month (which corresponds to the average monthly mobile data usage in Australia, Australian Competition and Consumer Commission, 2021), they could be on the smallest plan Telstra offers (i.e., 40GB) and still have 25GB in excess data each month. The large 40-60GB gaps between plan data limits allow plenty of scope for heavier data users to also have excess data remaining each month.

6.1.2 Optus

Optus offers the Optus Mobile Family Plan. This plan allows a single Customer to group up to four SIM services under one account, for a monthly plan price of $149. Up to two additional SIM services (for a total of 6 Users) can be added for an additional $29 per User per month. The Optus Mobile Family Plan offers a pooled data limit across all Users of 200GB per month.

6.1.3 Vodafone

Like Telstra, Vodafone allows eligible plans on the same account to share excess data. Vodafone's eligible plan data usage limits are 40GB, 80GB, 150GB, 300GB, and 500GB. As with Telstra, large gaps between plan limits provide plenty of scope for individual users to routinely have excess data each month. In addition, Vodafone also offers incrementally increasing discounts for all eligible users on the same account, depending on the number of plans listed. This is known as the Bundle and Save discounts. Two plans on the same account each receive a 5% discount on each plan's monthly cost, increasing by 5% per plan up to a maximum of 20% for five plans on the one account.

6.1.4 Consent to collect personal data

The privacy policies of both Telstra and Optus are explicit in indicating that Users should provide informed consent for their data and usage information to be collected and stored by the respective Telco. In both cases, the responsibility to obtain this consent is placed with the Customer. Both Telcos require the Customer to confirm that informed consent has been given by the User, yet no verification is sought by the Telcos that this has indeed been given/received. The Vodafone policy does not mention collecting and storing the information of Users. Moreover, live chats (conducted online with a 'bot') with Vodafone confirm that they do not take any steps to seek consent from or even identify end Users of the multiple devices registered to the one account.

6.1.5 Discussion

All three Telcos offer Family Plan arrangements. These are structured differently across the respective Telcos, but all of these plans pose the same surveillance risks. In all cases, a single Customer has access to the device usage details (i.e., calls made and received and data used) of other Users and can control whether other Users have reciprocal access to the same information about them. Critically, all three Telcos make no substantial effort to seek informed consent from the User(s) to collect and store their data or consent to make those data available to the Customer. It should be noted that while Telstra and Optus explicitly state it is the Customer's responsibility to ensure the Users are fully informed and provide consent for their data to be collected in this way, they rely on the Customer's confirmation and seek no verification from the User. Concerningly, Vodafone, it would seem, seek no such confirmation of informed consent.

We suggest that it is highly unlikely that such policies (found in the respective Telco's privacy policies) ensure that Users provide informed consent regarding the collection of their usage data, and subsequently, the Customer's access to such data. To the best of our knowledge, Telcos engage in no measures whatsoever to verify that Users have provided this consent.

Since it is freely acknowledged that the Customer/User distinction is readily "exploited" by perpetrators of domestic and family violence (Communications Alliance Ltd, 2018, p. 9), it is concerning that Telcos are not seeking to ensure that Users are fully aware of the potential risks and surveillance opportunities that Family Plan arrangements present. We suggest that the point at which a Customer registers multiple services is when Telcos should be proactive in preventing mobile phone assisted surveillance. Preventative strategies include the development of plain language (non-technical) resources that explain the asymmetries that Family Plan arrangements create in the control of information and how this asymmetry can be exploited in coercive and abusive relationships and contexts. Users could also be provided with a link to these resources when their service is activated. If such communications from Telcos were routine, it could greatly increase the awareness among the public about these risks.

Users could also be invited to register as the device's (i.e., the phone) primary user and Customers asked to confirm this registration. In circumstances where relationships are ostensibly healthy and open (even if they are destined to become coercive and abusive), it is likely that Customers and Users would readily provide and confirm this information, especially if the practise of doing so was normalised. This could assist Telcos to more effectively support Users in the future, should they experience domestic and family violence and seek to have their phone and service transferred into their own name. The potential for such transfers to occur could even be flagged in the relevant contract terms. It may be less likely that a Customer would confirm the primary User details in this way if the relationship between them was already controlling and abusive. Even in these circumstances, though, the failure of a Customer to confirm the primary User's identity could itself act as a warning sign for the Telco, that the service in question may be at risk of exploitation in a domestic and family violence scenario.

Telcos could also include an option for Users to request authorised access to the online accounts. The Telcos could pass this request onto the Customer via a text message with a link to update the User's authorisation status. Such communications would increase the number of Users who are granted access to their accounts and increase their knowledge of the information those accounts

provide. Moreover, this option of access would also encourage conversations between Customers and Users about data sharing, privacy, and the risks of covert surveillance. This will increase the extent to which Users are aware of the consent they are giving Telcos to record and share their data using their service.

6.2 Data available to Customers

6.2.1 Usage data

The usage data available to Customers and (and any authorised Users) via Telstra's online account interface (My Telstra), Optus' online account interface (My Account), and Vodafone's online account interface (My Vodafone) was similar across the three Telcos. In all cases, the usage data available for all SIMs registered under the account comprised of:

- all calls made, including:
    - the date and time of the call,
    - the number dialed, and
    - the duration of the call.

- all SMS messages sent, including:
    - the date and time of the message, and
    - the number of the recipient.

- all data used, including:
    - date and time of usage, and
    - the amount of data used.

Vodafone and Optus also provided information about the costs of individual calls and text messages. However, none of the Telcos provided information about the numbers from which calls and messages were received, nor did they provide information about the content of text messages.

6.2.2 Location data

6.2.2.1 Data collected

None of the Telcos provided device location data via their online portals or as part of routine billing information. The privacy policies (all accessed August 2021 and January 2022) of Telstra, Optus, and Vodafone confirm that location data are collected and stored, corresponding to each call made, text messages sent, and mobile data used. This location data is gained from the mobile cell towers connected to the phone during these events.

6.2.2.2 Access to location data

Telstra's site outlines how Customers can request their personal data and indicates that cell tower coordinates will be provided along with this personal data for all calls made and text messages sent. This information (for the last 12-months of device usage) can be obtained for any number registered to the Customer, by paying a $25 fee (verified by Meese et al., 2019). This was confirmed via a live chat in January 2022. The face-to-face consultation in-store suggested that the Customer would not

be able to access location data in this way for devices used by other Users under the same Family Plan. However, we confirmed via live chat that when multiple services are registered to the one Customer, there is no record of which service(s) (i.e., device) is used by the Customer and which device is used by other Users under the same Family Plan. Therefore, no such distinction could be made as suggested by the in-store representative.

The information regarding processes for gaining access to personal data for Optus and Vodafone were not explicit. That is, their policies do not state whether or not the cell tower location data are available upon request. As Meese et al. (2019) point out, these data may not be considered personal data and may not be required by law to be made available to Customers. Face-to-face consultations with an Optus representative in December 2021 indicated that location data would not be available to Customers, even upon request, with such data only provided to the police. Moreover, face-to-face consultations in November 2021 with a Vodafone representative suggested that Vodafone would only provide its cell tower-based location information if subpoenaed to do so.

6.2.3 Location tracking features

6.2.3.1 Telstra

Telstra advertises Device Locator as a feature of the My Telstra App. This locator provides a device's last known physical location based upon the most recent connection to the Telstra Mobile Network. To use this function, this feature must be set-up on each device. Users of each device also can turn this feature off at any time. If the locator is switched on, the users of all devices connected to the one account (the Customer and Users) can see the real-time physical location of all other devices that have the Device Locator feature set up and switched on.

The Terms and Conditions of the Device Locator warn that it must not be used to track the location of a person or an object in that person's possession without their express consent. They also indicate that it is solely the responsibility of the user to ensure they use this feature as permitted by all relevant laws.

Face-to-face consultations with a Telstra representative in store (December 2021) indicated that tracking services available on Telstra plans and phones were considered to be features of the devices themselves that are activated by the users and not by Telstra. The representative indicated that holders of Telstra accounts could not track the physical locations of other users' devices on multi-user plans. This advice did not wholly accord with the advertised Device Locator feature. While this feature must be activated on the phone that is being tracked and switched on, if these conditions are met then the My Telstra App can track the device's physical location in real-time. Therefore, anyone with access to the device potentially can activate this location device without the other person's knowledge.

6.2.3.2 Optus

Optus offer all customers with an Optus Family Plan a free subscription to the McAfee® Safe Family App. This app offers (among other features) device location services and is designed to be installed on children's phones to permit parental monitoring of activity. However, a face-to-face consultation with an Optus representative (January 2022) confirmed that the app could, in principle, be used to track the device of an adult. For its location to be tracked, the app must be installed on the device.

Unlike Telstra's Device Locator, the McAfee® Safe Family App is not linked to the Optus Customer's account. Therefore, customers can use their subscription to track devices upon which they have installed the app, whether or not they are connected to the Optus network. Since the McAfee® Safe Family App is specifically designed to track children's behaviour, if a device user disables the app in any way (including switching off their phone), the main account holder (i.e., the Customer) is notified that monitoring has been paused (verified by Live Chat on the Optus site, January, 2022). The Terms and Conditions for the Optus Family Plan do not warn against using the McAfee® Safe Family App for covert monitoring of an adult's location or online behaviour.

6.2.3.3 Vodafone

Vodafone do not advertise any device location apps, or services. In-store consultation with a Vodafone representative (November 2021) and use of the Live Chat service on the Vodafone site (January 2022) confirmed that Vodafone offers no such service.

6.2.4 Discussion

Ascertaining the usage data available via each Telco's online account interface was reasonably straightforward from within the interface itself. While all the data available from these apps were listed in each Telco's respective privacy policies (as data which are collected and stored), additional data not available via the online accounts was also mentioned in these policies. Ascertaining exactly the data that would be available to access via the online account interface (as opposed to the data that could only be accessed via a special request) was not possible from the privacy policies alone. It was not until the accounts themselves within the Telco's web interface were accessed, that the exact data and information available there became clear. Customers may not elect to provide other Users with authorisation to access the account, and so many Users would likely miss this opportunity to see for themselves the usage data that is presented there.

Information regarding the location data the Telcos collect and store (i.e., how long data is retained and who has access) was more difficult to ascertain. Face-to-face consultations with representatives from all three Telcos suggested that location data pertaining to other Users' devices would not be available to Customers, even upon request. For Telstra, at least, this advice was contradicted by information provided on the Telstra website and the live chat support. Whether Vodafone or Optus would actually provide such data on request remains somewhat uncertain. Meese et al. (2019) investigated the three Telco's willingness to hand over personal data. While they were not explicit about location data, they suggested that Vodafone were willing to provide more than required by law, suggesting that they may have been willing to provide stored location data. Optus, however, were only willing to share personal information as required by law, suggesting that they would not have shared location data unless subpoenaed.

In any case, Telstra's (and possibly Optus') willingness to share location data when requested presents a substantial surveillance risk. This method of obtaining location data would not support real-time monitoring of a target's location. It could, however, reveal key movement information after the fact. In a scenario where a User is preparing to leave an abusive relationship (a time when they are most vulnerable to harm, Toivonen & Backhouse, 2018), they may be making plans in secret (Brownridge, 2006). Should their partner become suspicious, they could request these location data. Depending on the User's normal activity patterns, the location data could reveal movement patterns

they cannot readily account for. For example, it could show journeys to various suburbs (as they inspected alternative accommodation options) at times they would ordinarily be in a single location at work.

The location tracking services provided and promoted by Telstra and Optus also present clear surveillance risks. In the case of Optus, the tracking is provided by a third-party app, which is designed for parents to monitor their children's device use and location. The app is provided free of charge to Optus Family Plan Customers but is otherwise not linked to Optus services. In the case of Telstra, the Device Locator is a feature within the My Telstra App, and its use is restricted to locating (multiple) devices that are registered under one Telstra account. Although, again, we note the contradictory advice offered by the face-to-face consultation with the Telstra representative (who suggested that Customers could not track the physical locations of other devices on their plan, except by using features of the devices themselves that are unrelated to the Telstra service). While it is true that these services must be activated on a device in order for it to be tracked, the placement of the Device Locator feature within the My Telstra App, does not accord convincingly with the claim that this feature is unrelated to the Telstra service.

Similar to the other forms of data a Customer can access, the risks that these tracking apps present are two-fold. Firstly, a lack of awareness can lead to covert surveillance. Even though Users have the option to disable tracking services in both the Optus third-party app and the Telstra Device Locator feature, if these tracking services are set up when a phone is first obtained but rarely used, the User may simply forget that they are activated. Secondly, if both the Customer and User are acutely aware of the tracking service, it can be used for coercion and overt surveillance. The coerced party may feel unable to safely turn the tracking off (for fear of triggering suspicion or violence in their partner) and feel equally unsafe going anywhere without their partner's approval while the tracking is on. Both of these scenarios could readily emerge after the tracking features were activated with all party's full knowledge and consent prior to any (perceived) deterioration in their relationship.

With respect to all the forms of data that Customers and authorised Users may be able to access about other Users' actions, a lack of awareness about the available information is one of the key enablers to using it for surveillance. Secondary to this is a lack of appreciation for how such information can be weaponised in coercive relationships. Here we again argue that Telcos should play a more proactive role in increasing Customers and Users' awareness. For example, in the information sent to Users upon activation of their service, Telcos could include clear explanations of the information about other Users' data activity available to the Customer and the various avenues by which the Customer might acquire this information.

6.3 Financial incentives to use Family Plans

Mobile phones represent a substantial monthly cost. For many Australians, especially those on low incomes, their mobile phone might also be their primary or sole method of accessing the internet (Thomas et al., 2021). The average monthly cost of post-paid mobile phone plans (i.e., plans that are paid retrospectively) range from $33-$38 per device for SIM only plans, and up to $72-$87 per device for plans that include the purchase of a phone (Bradstock, 2021), with recent price increases from all three major Telcos (ACCC, 2021).

Telco Customers are price sensitive (Thomas et al., 2021), and this is reflected in the marketing material of Family Plan arrangements, wherein apparent savings feature prominently. The savings offered by Family Plans across the three major Telcos, however, are not always straightforward for consumers to understand. In some cases, the savings depend on how the devices will be used especially with respect to mobile data usage. Therefore, the extent to which Customers (and other Users) can accurately anticipate their future usage behaviours determines how accurately they can estimate the savings that a Family Plan might represent for them.

The ambiguity around the financial benefits of Family Plan arrangements for consumers is problematic. Even if consumers are fully aware and cognizant of the potential privacy and surveillance risks these plans present, it would still be difficult for them to make an accurate and fully informed choice as to whether the financial benefits outweighed the potential costs of their compromised privacy.

Below are summaries of the Family Plan arrangements offered by the three Telcos, with examples of the available savings across a number of hypothetical scenarios. Plans considered are SIM-only plans. That is, users bring their own phones to these plans or purchase a phone through the relevant Telco, with any monthly repayments for such devices added to the monthly SIM costs quoted below.

6.3.1 Telstra

The cost incentive for Telstra customers to adopt multiple plans under one account comes via the ability to share excess data between plans. These incentives are most significant when users across the family have large discrepancies in their data usage requirements and where individual users' data requirements fall between the data limits of Telstra's various individual plans (see Table 1).

Table 1 Telstra Upfront Mobile Plans for Individual Users

Plan	Data Allowance	Cost per Month
Small	40 GB	$55
Medium	80 GB	$65
Large	120 GB	$85
Extra Large	180 GB	$115

The following three scenarios illustrate the potential savings available to Customers choosing to bundle multiple plans under one account to take advantage of data sharing. Not surprisingly, the potential savings increase as the number of Users increases (see Table 2).

Scenario 1

A family of four users, in which each individual users' monthly data requirements are 20GB, 60GB, 100GB and 140GB, respectively, for a family total of 320GB. Placed on individual plans, with no excess data sharing permitted, these family members would require a Small plan, a Medium plan, a

Large plan, and an Extra Large plan for a combined cost of $320/month. However, by grouping their four plans on one account and thus allowing the data across all plans to be shared among the four users, the family could save $60/month by acquiring their 320GB of data across four Medium plans.

Scenario 2

A family of three, in which one user consumes 140GB/month and the other two users each consume 50GB/month, would individually require an Extra Large plan and two Medium plans, for a total cost of $245/month. However, sharing excess data among plans would permit the family to pay for three Medium plans instead, for a monthly cost of $195, saving $50/month.

Scenario 3

A couple (two users), in which one user consumes 100GB/month and the other user consumers 60GB/month, would individually require a Large plan and a Medium plan for a total cost of $150/month. However, by covering their data requirements across two Medium plans on one account, this couple can save $20/month.

Table 2 Potential savings for Telstra Family Plans, compared to individual user plans

Scenario	No. of Users	Individual Costs	Family Plan Costs	Savings
1	4	$320 / month	$260 / month	$60 / month
2	3	$245 / month	$195 / month	$50 / month
3	2	$150 / month	$130 / month	$20 / month

6.3.2 Optus

Optus offers Customers an Optus Family Mobile Plan, which is designed for four users. It is priced at $149/month and permits a total data download of 200GB/month. Additional Users can be added for an additional cost of $29 per User per month. Additional Users can share the 200GB of data available to the family, but this limit does not increase when more Users are added. Additionally, Optus also offers the same data-sharing provisions as Telstra (described above), wherein the data available for use across all plans listed under the one account is pooled and available to all users on the account. The individual user plans (up to 200Gb/month) that were available in August 2021 are shown in Table 3.

Table 3 Optus Choice Mobile Plans for Individual Users

Plan	Data Allowance	Cost per Month
Small	20 GB	$45
Medium	80 GB	$55
Large	200 GB	$65

The hypothetical scenarios below focus on comparing the costs of the Optus Family Mobile Plan with separate individual user plans. For Optus, the largest savings were observed for larger families where individuals tended to have smaller monthly data usage requirements. Therefore, couples without children would not benefit from swapping their individual plans for an Optus Family Mobile Plan. The outcomes of these scenarios are summarised in Table 4.

Scenario 1

A family of four with each member using 40GB of data per month would be paying $220/month for four Medium plans. Shifting these individual plans to an Optus Family Mobile Plan would save the family $71/month.

Scenario 2

If the family described in Scenario 1 were to add two additional child users who each use only 20GB/month, their total cost for individual plans would be $310/month for four Medium plans and two Small plans. Shifting these six plans to an Optus Family Mobile Plan costing $207/month would save the family $103/month.

Scenario 3

A family of three users, in which one user consumes 100GB/month and the other two users each consume 50GB/month, would individually require a Large plan and two Medium plans, for a total cost of $175/month. However, switching these individual plans onto the Optus Family Mobile Plan, would save this family $26/month.

Table 4 Potential savings for Optus Family Plans, compared to individual user plans

Scenario	No. of Users	Individual Costs	Family Plan Costs	Savings
1	4	$220 / month	$149 / month	$71 / month
2	6	$310 / month	$207 / month	$103 / month
3	3	$175 / month	$149 / month	$26 / month

6.3.3 Vodafone

Like Telstra, the cost incentive for Vodafone customers to adopt multiple plans under the one account comes via the ability to share excess data between plans on one account. In addition, Vodafone offers percentage discounts on the monthly plan fees for all plans held under one account. For example, a 5% discount is applied if two plans are held under one account, increasing to a 10% discount for three plans, 15% discount for four plans, and a 20% discount for five or more plans. These discounts are applied to all plans held under the account (e.g., if three plans are held, the price of each plan is discounted by 10%). The individual plans available from Vodafone in August of 2021 are shown in Table 5.

Table 5 Vodafone Mobile Plans for Individual Users

Plan	Data Allowance	Cost per Month
1	40 GB	$40
2	80 GB	$45
3	150 GB	$55
4	300 GB	$65
5	500 GB	$75

The following three scenarios illustrate the potential savings available to customers choosing to bundle multiple plans under one Vodafone account. These scenarios take advantage of data sharing options under one account, and with Vodafone's plan fee discounts increasing on a sliding scale, the potential savings are higher when more users' plans are bundled together (as detailed above).

Scenario 1

A couple with one user consuming 60GB of data and the other consuming 20GB would require an individual 40GB plan, and an individual 80GB, for a total monthly cost of $85. Two 40GB plans would provide sufficient pooled data when combined under one account, which attracts a 5% discount. The total cost is $76/month, thus saving the couple $9/month.

Scenario 2

A couple with one user consuming 400GB of data and the other consuming 200GB would require an individual 500GB plan and an individual 300GB plan, for a total monthly cost of $140. When combined under the one account, two 300GB plans would provide sufficient pooled data, and with the 5% discount applied, the total cost is $123.50/month. Therefore, this couple would save $16.50 per month.

Scenario 3

A family of four users, who are individually consuming 200GB, 160GB, 120GB, and 80GB would require two 300GB individual plans, a 150GB individual plan and an 80GB individual plan for a total cost of $230/month. When combined under a single account, four 150GB plans would cover this family's data needs and attract a 15% multi-user discount. The total cost is $187/month, saving the family $43/month.

Table 6 Potential savings for Vodafone Family Plans, compared to individual user plans

Scenario	No. of Users	Individual Costs	Family Plan Costs	Savings
1	2	$85 / month	$76 / month	$9 / month
2	2	$140 / month	$123.50 / month	$16.50 / month
3	4	$230 / month	$187 / month	$43 / month

6.3.4 Discussion

All three Telcos offered discounts for combining multiple plans under a single customer account, relative to providing the same services via plans held by multiple individual customer accounts. With the affordability of digital services a pressing issue for a substantial proportion of Australians (Thomas et al., 2021), even some of the more modest savings demonstrated above are likely to persuade users to combine multiple plans under a single account.

However, quantifying the potential savings available for combining plans under a single customer account is not straightforward and requires accurate estimations of a user's data requirements. Telcos could certainly do more to help customers arrive at accurate estimates of the savings they are likely to make by bundling their plans (such as offering online calculators, where customers can enter hypothetical monthly data usage values for different users and observe how different usage patterns alter the savings they are likely to make).

While greater transparency around costs and savings is always a positive for consumers, it is unlikely to ameliorate the surveillance risks of Family Plan arrangements. As long as Telcos provide savings to potential customers in return for what appears, at face value, to be minor compromises to their privacy, many customers will likely be willing to make these compromises. To reduce the risks identified in this report, Telcos must work to provide customers from one household with reduced priced plans without requiring those same adults to forego their status as individual customers. For example, Telcos could offer a 10% discount and an additional 20GB of data per month to all adults residing at the same address who take out an eligible plan with the Telco at the same time.

While some customers may prefer the convenience of having all of their household's mobile phones held under a single account, Telcos could maintain much of this convenience by permitting multiple customers from one household to nominate a single customer to receive amount payable notifications for all members of the household. These notifications could confirm the amount

payable and the due date without including any private usage data or other information that is required to be displayed on bills, pertaining to other customers. The nominated customer would, of course, not have any legal obligation to pay the bills of other customers. Such simple notifications could ensure that if a family wanted just one person to be able to keep track of all billing and payments for the entire household, this could be accommodated without compromising the privacy of other adults in the household (and regardless of which adult's account any children's devices or SIMs were registered to).

Removing the need for members of one household to combine their devices under a single account may increase consumer mobility between the Telcos. If individual users in a household are recognised as independent customers, it may then be difficult for Telcos to insist that any discounted plan prices or increased data limits offered to one of those customers at sign-up, remain contingent on the other customer's continued use of their respective plan. Such contingencies are also undesirable from the perspective of supporting customers experiencing domestic and family violence since they provide opportunities (albeit modest) for one person to influence the financial position of the other, post-separation. In the absence of such contingencies, of course, individual customers having secured a discounted plan for their spouse with one Telco could (in the absence of a lock-in contract) then shift their account to another Telco. Telcos could guard against this by offering discounts and bonus data for 12 months at a time, and renewing these offers every 12 months, provided that all plans in question remain active.

Providing a mechanism to offer multi-user discounts to households without requiring adult users to forego their individual customer status will have tremendous benefits for domestic and family violence victims, beyond protecting their private data from their abuser. When abusive relationships dissolve, Family Plan arrangements can lead to a multitude of problems including an abusive user accumulating substantial debt in the customer's name or refusing to permit a user to take their number and device to a new plan or cancelling their service entirely. Ensuring that all adult users in a household are customers in their own right greatly limits the potential for mobile phone plans to facilitate surveillance and financial abuse, as domestic and family violence emerges in a relationship and during and after a relationship breakdown.

7. Conclusions

7.1 Family Plans and consent to share data

Family plan arrangements are offered by all three of the major Telcos, which are the subject of this report. For all three Telcos, these plans involve collecting the private usage data of the Users and making it visible to the Customer and other Users solely at the Customer's discretion. However, to the best of our knowledge, none of the Telcos took active steps to ensure that Users were aware of the nature of the information collected, stored, and shared about them and their device usage. Two of the three Telcos (i.e., Telstra and Optus) recognised the need for Users to provide informed consent; however, they placed the responsibility for obtaining this on the Customer. Concerningly, neither Telstra nor Optus had any mechanisms in place for verifying that this consent had occurred.

7.2 Risks of both overt and covert surveillance

The Family Plan arrangements offered by all three Telcos compromise the privacy of Users. While industry guidelines acknowledge the surveillance risks that Family Plan arrangements present, they do not encourage Telcos to take active steps to ameliorate the realisation of these risks. These arrangements provide Customers (and authorised Users) with access to other Users' usage data and (in some circumstances) location data, either delayed or in real-time (if tracking features are enabled on the respective devices). Family Plan arrangements are not the only mechanism by which partners can obtain usage and location data about each other, but their widespread use provides an opportunity for Telcos to be proactive in kerbing the extent to which domestic and family violence perpetrators could take advantage of the products and services they offer.

7.3 Opaque cost-saving measures

Telcos use a multitude of techniques to offer savings associated with their Family Plan arrangements. These techniques involve discounted prices for a single bundled plan compared to individual plans, savings by allowing excess data to be shared between bundled plans, and incrementally increasing percentage discounts as additional plans are added. These cost-saving measures can be complex, and the potential savings for the customers are not easy to calculate. Estimating savings often depends on how much data is typically used and how this compares to the data limits offered on individual plans. How accurately a family of customers can project their potential savings also depends on how accurate their estimates of their future data use may be. This makes it very difficult for prospective customers to estimate the actual savings a Family Plan would offer them, and to compare these savings against the potential privacy risks such plans present.

8. Recommendations

We recommend that Telcos use the activation of services acquired under Family Plan arrangements as opportunities to be more proactive in ameliorating the risks of the products and services they offer being exploited by perpetrators of domestic and family violence.

8.1 Recommendation 1 – Provide extensive information

Telcos develop resources in readily accessible language that explain the asymmetries in access to information that Family Plan arrangements create and how these asymmetries can be exploited in the context of domestic and family violence. These resources should also outline the exact nature of the information that Customers can access about other Users' on their plan and how this information can be accessed. Guidance should also be provided on how device-based location information can be blocked in the context of location tracking apps and features. Links to these resources should be sent directly to all devices activated under a Family Plan arrangement so that clear and accurate information is available to Customers and Users alike.

8.2 Recommendation 2 – Register primary Users

We recommend that Telcos invite Users to register themselves as the primary user of their device/service and request Customers to verify these registrations. Notices should request Customers and Users to periodically confirm these details. These registrations would have no impact on the legal ownership of the device or the financial liability under the contract. They would, however, help Telcos to better support victims of domestic and family violence who are seeking to leave a relationship and transfer ownership of a service to their name, by establishing a clear record of primary use of a service over time, endorsed by the Customer.

8.3 Recommendation 3 – Encourage User authorisation

We recommend that Telcos suggest that adult Users request full authorisation to access their service's account online. Telcos can combine this suggestion with a brief explanation of why it is sensible to be familiar with how your data are being used and shared, especially in the context of surveillance risks. Telcos can then pass these requests onto Customers with a link to the online account where such changes can be made. Adopting this practice would increase the number of Users granted access to their service's account thus increasing awareness for all parties about the User data that are shared under Family Plan arrangements (and how under some circumstances, this can present a surveillance risk). It would also increase communication between Customers and their Users about data, privacy, and surveillance. This recommendation will position both Customers and Users to provide fully informed consent for their data to be shared in the context of a Family Plan arrangement.

8.4 Recommendation 4 – Offer dual contracts

We recommend that Telcos offer equivalently priced dual contracts to adults seeking Family Plan arrangements to allow all adults to retain their independent customer status. The above three recommendations would work towards increasing awareness and transparency around data sharing

in the context of Family Plan arrangements and in doing so minimise the risks that these arrangements pose to abuse or coercion in the future. However, avoiding multiple adults' services on a single plan in the first place is a far more desirable solution. This option would eliminate the surveillance risks Family Plans present and reduce the incidence of issues that arise with Family Plans during relationship breakdown. These include (but are not limited to) one partner amassing a large debt in the other partner's name, services being cancelled by the customer (of their ex-partner), or refusal to transfer the ex-partners service into their own name. Offers of fixed, simple discounts and/or increased data caps on dual contracts taken out simultaneously may also allow customers to gauge the savings more easily on offer for choosing the same Telco, compared to current Family Plan arrangements, whose savings can be difficult to estimate and calculate.

9. Authors

Danielle Sulikowski

Dr Sulikowski has 15 years of training and experience in survey design, advanced quantitative data analysis, and report and article writing. She has also considerable experience in managing the logistics of online data collection, including the use of paid recruitment services. She brings to the project her discipline expertise in personality and romantic relationships.

Robyn Brunton

Dr Brunton is a Senior Lecturer with the School of Psychology at Charles Sturt University. Dr Brunton is experienced in the area of childhood abuse and adult victimisation, and mental health problems in vulnerable populations and brings to the project her discipline expertise in domestic violence and coercive control.

Myoungju Shin

Dr Shin has 13 years of training and experience in survey design, quantitative data analysis, and report and article writing. She also has considerable experience in online data collection. She brings to the project her discipline expertise in personality and mobile phone/digital device use, including problematic and maladaptive use of such devices.

10. References

Arnocky, S., Sunderani, S., Gomes, W. & Vaillancourt, T., (2015). Anticipated partner infidelity and men's intimate partner violence: The mediating role of anxiety. *Evolutionary Behavioral Sciences*, *9*, 186-196. https://psycnet.apa.org/fulltext/2014-34825-001.html

Australian Bureau of Statistics (2017). *Personal Safety Survey, Australia, 2016* (Cat. No. 4906.0). Canberra: Australian Bureau of Statistics. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4906.0

Australian Competition and Consumer Commission (2021, June 21). *Australian consumers now paying more for mobile plans.* [Media Release]. ACCC. https://www.accc.gov.au/media-release/australian-consumers-now-paying-more-for-mobile-plans

Borrajo, E., Gámez-Guadix, M., Pereda, N., & Calvete, E. (2015). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, *48*, 358-365. https://www.sciencedirect.com/science/article/pii/S0747563215000916

Bradstock, E. (2021). What is the average mobile phone bill? Canstar Blue. https://www.canstarblue.com.au/phone/average-mobile-phone-bill/

Bricknell, S. & Doherty, L. (2021). *Homicide in Australia 2018-19*. Statistical Report no. 34. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr78153

Brownridge, D. A. (2006). Violence against women post-separation. *Aggression and Violent Behavior*, *11*, 514-530. https://www.sciencedirect.com/science/article/pii/S1359178906000115

Communications Alliance Ltd. (2018). Assisting customers experiencing domestic and family violence. Industry Guideline, G660:2018. https://www.commsalliance.com.au/Documents/all/guidelines/G660

Communications Alliance Ltd. (2019). Telecommunications Consumer Protection (TCP) Code. Code, C628:2019. https://www.commsalliance.com.au/Documents/all/codes/c628

Coumarelos, C. (2019). Quantifying the legal and broader life impacts of domestic and family violence. *Justice Issues, 32*, 1-40. https://search.informit.org/doi/10.3316/informit.963367584342381

Council of Australian Governments. (2010). *National plan to reduce violence against women and their children 2010-2022.* https://www.dss.gov.au/sites/default/files/documents/08_2014/national_plan1.pdf

Deans, H., & Bhogal, M. S. (2019). Perpetrating cyber dating abuse: a brief report on the role of aggression, romantic jealousy and gender. *Current Psychology, 38*, 1077–1082. https://link.springer.com/article/10.1007/s12144-017-9715-4

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.* Australian Communications Consumer Action Network, Sydney. https://accan.org.au/grants/completed-grants/1429-domestic-violence-and-communication-technology-victim-experiences-of-intrusion-surveillance-and-identity-theft

Felson, R. B., & Outlaw, M. C. (2007). The control motive and marital violence. *Violence and Victims*, *22*, 387-407. https://connect.springerpub.com/content/sgrvv/22/4/387.abstract

Hamberger, L. K., Larsen, S. E., & Lehrner, A. (2017). Coercive control in intimate partner violence. *Aggression and Violent Behavior*, *37*, 1-11. https://www.sciencedirect.com/science/article/pii/S1359178917300940

March, E., Grieve, R., Clancy, E., Klettke, B., van Dick, R., & Hernandez Bark, A. S. (2021). The role of individual differences in cyber dating abuse perpetration. *Cyberpsychology, Behavior, and Social Networking*, *24*, 457-463. https://www.liebertpub.com/doi/full/10.1089/cyber.2020.0687

March, E., Litten, V., Sullivan, D. H., & Ward, L. (2020). Somebody that I (used to) know: Gender and dimensions of dark personality traits as predictors of intimate partner cyberstalking. *Personality and Individual Differences*, *163*, 110084. https://www.sciencedirect.com/science/article/pii/S0191886920302737

Meese, J., Jagasia, P. and Arvanitakis, J., 2019, *Consumer rights to personal data: Data access in the communications sector*, Australian Communications Consumer Action Network, Sydney.

Morgan, A. & Chadwick, H. (2009). *Key issues in domestic violence: Summary Paper, no. 7*, Australian Institute of Criminology, Canberra. https://www.aic.gov.au/publications/rip/rip7

Nemeth, J. M., Bonomi, A. E., Lee, M. A., & Ludwin, J. M. (2012). Sexual infidelity as trigger for intimate partner violence. *Journal of Women's Health*, *21*, 942-949. https://www.liebertpub.com/doi/abs/10.1089/jwh.2011.3328

NSW Bureau of Crime Statistics and Research. (2020). *NSW recorded crime statistics quarterly update, December 2019*. https://www.bocsar.nsw.gov.au/Pages/bocsar_media_releases/2020/mr-NSW-Recorded-Crime-Statistics-Quarterly-Update-Dec-2019.aspx

Rollè, L., Giardina, G., Caldarera, A. M., Gerino, E., & Brustia, P. (2018). When intimate partner violence meets same sex couples: A review of same sex intimate partner violence. *Frontiers in Psychology, 9*(1506). https://doi.org/10.3389/fpsyg.2018.01506

Smoker, M., & March, E. (2017). Predicting perpetration of intimate partner cyberstalking: gender and the Dark Tetrad. *Computers in Human Behavior, 72*, 390–396. https://www.sciencedirect.com/science/article/pii/S0747563217301619

Stanley, J., Tomison, A. M., & Pocock, J. (2003). Child abuse and neglect in Indigenous Australian communities. Child abuse prevention issues. Melbourne: Australian Institute of Family Studies no. 19. https://aifs.gov.au/sites/default/files/publication-documents/issues19_0.pdf

State of Victoria (2016). *Royal Commission into Family Violence: Summary and recommendations, Part Paper No 132 (2014–16).* http://rcfv.archive.royalcommission.vic.gov.au/Report-Recommendations.html

Telecommunications Numbering Plan 2015 (Cth) ch I pt III s 15 https://www.legislation.gov.au/Details/F2016C00283

Thomas, J., Barraket, J., Parkinson, S., Wilson, C., Holcombe-James, I., Kennedy, J., Mannell, K., Brydon, A. (2021). *Australian Digital Inclusion Index: 2021*. Melbourne: RMIT, Swinburne University of Technology, and Telstra. https://apo.org.au/sites/default/files/resource-files/2021-10/apo-nid314284.pdf

Toivonen, C., & Backhouse, C. (2018). *National Risk Assessment Principles for domestic and family violence* (ANROWS Insights 07/2018). Sydney, NSW: Australia's National Research Organisation for Women's Safety Ltd (ANROWS). https://www.anrows.org.au/research-program/national-risk-assessment-principles/

An assessment of the risks Family Plans present for users vulnerable to domestic and family violence