THE CONSENT TRAP

AUSTRALIAN FOCUS GROUPS ON SMARTPHONES, PRIVACY AND CONSENT

UTS
Centre
for Media
Transition

'CONSENT IS A TRAP ... BUT IT'S BETTER THAN NOTHING'

SACHA MOLITORISZ is a postdoctoral research fellow at the Centre for Media Transition at UTS. His latest book is *Net Privacy, How we can be free in an age of surveillance* (2020).

JAMES MEESE is a senior lecturer at RMIT University. He holds an early career research fellowship from the Australian Research Council and regularly publishes on media policy and emerging technology.

Written and researched:
Sacha Molitorisz and James Meese
Layout and design: Kevin Kearney
Focus group facilitator: Claire Marshall
Cover illustration: Edie Molitorisz
Additional research:
Jennifer Hagedorn and Charlie Lian
Proofreading: Katie Pollock
Photography: iStock

Suggested citation: Molitorisz, S. and Meese, J. 2020. *The Consent Trap: Australian focus groups on privacy, smartphones and consent.* Centre for Media Transition, University of Technology Sydney, Australia, cmt.uts.edu.au

CONTENTS

Thanks to the International Association of Privacy Professionals for generously funding this research. Thanks also to Claire Marshall, Jennifer Hagedorn, Charlie Lian, Derek Wilding, Chrisanthi Giotis and Caitlin McGrane. Privacy is collective in nature; this research was only possible as a collective effort.

This project was funded by the International Association of Privacy Professionals – Australia/New Zealand Chapter Inc as part of its legacy grants scheme for research projects advancing professionals in the privacy and data industries. The views expressed in this document do not necessarily reflect the views of the International Association of Privacy Professionals – Australia/New Zealand Chapter Inc.

1 EXECUTIVE SUMMARY

When it comes to data and privacy, the growing academic consensus is that we need to look beyond informed consent. By contrast, governments and policymakers are seeking to reinforce and improve consent mechanisms.

Against this backdrop, we wanted to know what Australians thought about the role of informed consent, especially on their smartphones. We also wanted to know if they had any suggestions on how to fix the standard 'notice and consent' process.

- We spoke to 26 participants from Sydney and Coffs Harbour across six two-hour focus groups, held via Zoom in late July 2020.
- Participants felt that companies were often trying to trap or trick them. They were also concerned that current models were: not sensitive to vulnerable groups; did not recognise how people used technology, and specifically smartphones; and failed to offer any real choice.
- When discussing clear failures of consent such as eavesdropping or shadow profiles, participants were outraged. They were also careful to distinguish between sectors. Many felt that government apps offered more digestible information than private apps.
- However, participants still valued informed consent. They wanted informed consent to be: simple; clear; targeted; logical; relevant; and real-world (with concrete examples).

They also gave suggestions on how to improve the process. These focused on three key areas:

CLARITY Here, participants discussed factors including font size, avoiding legalese, and alternative consent mechanisms such as delivering information through images, graphs and videos.

GOVERNANCE Participants said consent alone cannot protect our data. Law and regulation have significant roles to play. This includes imposing standardisation and oversight of app developers and companies.

DESIGN Participants also noted that it was important to design technology with privacy (and consent) in mind.

Ultimately (and perhaps surprisingly), our participants were optimistic about consent. They want it to be fixed and they think it can be fixed. Drawing on the above findings, we have three core recommendations.

CORE RECOMMENDATIONS:

1 **Keep and repair informed consent**. It may only ever play a limited role, but remains a central and important ethical mechanism. What's more, it's still valued by people.

2 **Improve privacy law.** Participants saw the need to bolster consent through standardisation and active regulatory oversight, and to set a baseline of standards. For example, statutory bodies can play a critical role in launching proceedings on behalf of consumers to enforce notice and consent agreements.

3 **Focus on design.** Participants recognised that design also plays a key role. User interface and user experience designers and developers need to work to support consent, and to complement the law to protect privacy appropriately.

PARTICIPANTS FELT THAT COMPANIES WERE OFTEN TRYING TO TRAP OR TRICK THEM

2 | INTRODUCTION

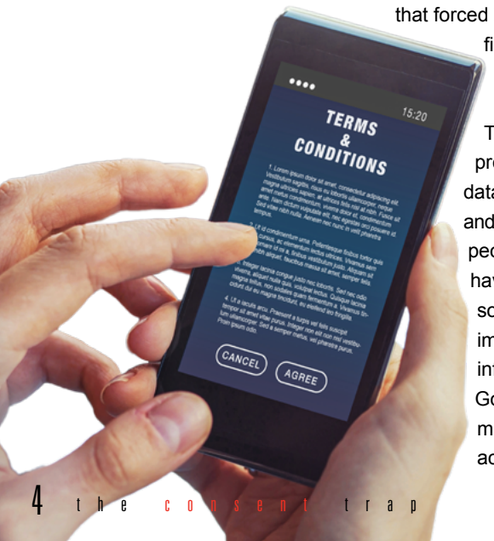
Be suspicious when giving consent to any app

Quentin, Coffs, 65

Consent is a key ethical and legal concept that's easy to understand and common in everyday exchanges. It features prominently in discussions about sexual relations, medical procedures and the use of our data, and can be defined as 'voluntary agreement in the light of relevant information'.[1]

People's online privacy is largely managed through the system of 'notice and consent', which is based on a contractual model of interaction.[2] In an ideal world, the system is straightforward: online services and apps give you clear information about how your data will be used; you then read the information and make a considered decision about whether or not you want to agree to the proposed terms.

Unfortunately, the reality doesn't match the theory. People are often faced with lengthy or unclear contracts they are unable to understand. They end up simply clicking 'agree' or 'accept' so they can access and use the services they want. As a result, companies get access to people's data relatively easily. Previous social experiments have seen people accept terms and conditions that forced them to give up their first-born child[3] or sell their souls to the devil.[4]



There are additional problems. One is that digital data flows are often hidden and unpredictable. For years, people's browsing patterns have been collected and sold to data brokers.[5] While improvements in the privacy infrastructures of Apple and Google mean that people may no longer be tracked across the web, companies will still be able to develop detailed profiles about people who visit their websites.[6] A further problem is that information can be inferred about an individual even without that person sharing any data, a phenomenon that's been dubbed the 'privacy leak factor'.[7]

People do not generally understand how data collection processes work, which raises a critical question: is such consent meaningful? Solon Barocas and Helen Nissenbaum argue that this wider context exposes the 'ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject'.[8] Similarly, Daniel Solove argues:

1. *people do not read privacy policies;*
2. *if people read them, they do not understand them;*
3. *if people read and understand them, they often lack enough background knowledge to make an informed choice; and*
4. *if people read them, understand them, and can make an informed choice, their choice might be skewed by various decision-making difficulties.*[9]

It's an intractable problem: in an ideal world, consent could ensure fairness; in practice, it is deeply flawed.[10] The problem is also particularly acute on smartphones, which have small screens and often command partial, rather than total, attention.[11]

Lengthy, complex sentences are hard to understand

Maddie, Sydney, 35-40

Various reforms have been implemented in response. Europe enacted its General Data Protection Regulation (GDPR) in 2018, introducing sweeping protections that included a fortified definition of consent. Article 7 states that 'the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language'.[12] The article also notes that 'it shall be as easy to withdraw as to give consent'.[13]

In Australia, privacy law reform is under way, following the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry, which found that:

> *Many digital platforms use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limit the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data.*[14]

It is a leap of faith every time

Yves, Coffs, 52

In July 2019, the ACCC recommended the implementation of a privacy code for digital platforms, the introduction of a statutory tort for serious invasions of privacy, and a prohibition of unfair contract terms and certain unfair trading practices. It also recommended a reform of the *Privacy Act 1988 (Cth)*, and a strengthening of the requirements for consent. The latter reform would ensure that 'consents are freely given, specific, unambiguous and informed and that any settings for additional data collection must be preselected to 'off'.[15] In December 2019, the Australian government set out a roadmap for implementing the ACCC's recommendations; in October 2020, the government released the terms of reference for privacy law reform.[16]

Some potential solutions go beyond consent. 'Privacy by design' embeds privacy protection throughout the product design lifecycle and aims to lessen the burden on the individual. The GDPR has formally embraced this approach by mandating 'privacy by design and by default'.[17]

In view of the frequent failure of the notice and consent process and a growing regulatory attention around data issues, we thought it would be worthwhile exploring the issue through qualitative research. We wanted to:

- speak directly to Australians, and see if they valued the informed consent process;
- understand whether smartphones raised further issues around informed consent;
- examine the role of consent in relation to contact tracing apps; and
- explore whether and how they thought informed consent might be improved.

[1] Molitorisz, S. 2020. *Net Privacy: How we can be free in an age of surveillance.* NewSouth Publishing, Sydney, p. 196.

[2] Larsson, S. 2018. 'Algorithmic governance and the need for consumer empowerment in data-driven markets.' *Internet Policy Review*, 7(2), p. 1-13; Solove, D. 2012. 'Introduction: Privacy self-management and the consent dilemma.' *Harvard Law Review*, 126(7), p. 1880-1903.

[3] Kravets, D. 2016. 'TOS agreements require giving up first born—and users gladly consent.' *Ars Technica*, 13 July. Available at: https://arstechnica.com/tech-policy/2016/07/nobody-reads-tos-agreements-even-ones-that-demand-first-born-as-payment/

[4] Friedman, P. 2010. 'Should we allow consumers to sell their souls?' *Techdirt*, April 19. Available at: https://www.techdirt.com/articles/20100416/1201419039.shtml

[5] Federal Trade Commission. 2014. 'Data Brokers are Watching You: A Call for Transparency'. Available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[6] Whittaker, Z. 2020. 'Data brokers track everywhere you go, but their days may be numbered', *TechCrunch*, July 9. Available at: https://techcrunch.com/2020/07/09/data-brokers-tracking/

[7] Molitorisz (n. 1), p. 50-1.

[8] Barocas, S. and Nissenbaum, H. 2014. 'Big data's end run around anonymity and consent.' in Lane, J., Stodden, V., Bender, S. and Nissenbaum, H. (eds.) *Privacy, Big Data, and the Public Good: Frameworks for engagement.* Cambridge University Press, Cambridge, p. 45.

[9] Solove (n. 2), p. 1888.

[10] See: McDonald, A. and Cranor, L., 2008. 'The cost of reading privacy policies'. I/S: *A Journal of Law and Policy for the Information Society*, 4(3), p. 543-568; Obar, J. and Oeldorf-Hirsch, A. 2020. 'The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services'. *Information, Communication & Society* 23(1), p. 128-147.

[11] Wu, Tim. 2017. 'Blind spot: The attention economy and the law.' *Antitrust Law Journal*, 82(3), p. 771-806.

[12] General Data Protection Regulation 2016/679 (EU), Art. 7(2).

[13] Ibid., Art. 7(3).

[14] Australian Competition and Consumer Commission 2019. *Digital Platforms Inquiry: Final report*, p. 23. Available at: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

[15] Ibid., p. 24.

[16] Australian Government Treasury 2020. 'Regulating in the Digital Age: Government response and implementation roadmap for the Digital Platforms Inquiry.' Available at: https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf; Attorney-General's Department 2020. 'Review of the Privacy Act 1988 – Terms of Reference'. Available at: https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-terms-reference

[17] General Data Protection Regulation 2016/679 (EU), Art. 25.

3 METHODS

Our method was participatory and informed by a co-design approach. This 'is a design-led process that uses creative participatory methods'.[18] It involves participants 'in the design process, with the idea that this will ultimately lead to improvements and innovation'.[19] This means that we didn't just ask our participants what they thought about consent but also asked them to imagine what informed consent via smartphones could look like in an ideal world. This approach differs markedly from the more traditional behavioural or survey-based studies found in the literature.[20]

Originally, we had planned to set up rooms with sticky notes, butcher's paper and textas, as well as digital tools to enable users to simulate smartphone screens. The aim was to work with our participants to find new solutions to an old problem. But then COVID-19 hit, presenting the research team with a new challenge. What does online co-design research look like? After some discussion, we turned to the Zoom video-conferencing platform to hold our focus groups. We also used Google Jamboard, a collaborative software tool, to recreate the co-design experience. (The irony, as we discussed in our focus groups, is that both Zoom and Google have been involved in data and privacy scandals.[21])

Our online focus groups were not as interactive and dynamic as face-to-face groups would have been. Nonetheless, we made our sessions as participatory as possible, inviting everyone to contribute at any point, either simply by speaking up or writing in the 'chat' function of Zoom.

Our focus groups were also divided into discrete sections. We had open discussions, asked participants to use Google Jamboard to write down ideas on sticky notes (the sticky notes that appear throughout this report are taken from those Jamboard sessions); and also got them to critique real-world examples of notice and consent, such as initial sign-up processes on various apps. This final approach allowed us to mimic the standard user flows that people engage with when using smartphones and signing up to apps. We also discussed the consent and notification process associated with Australia's contact tracing app, COVIDSafe.

[18] McKercher, K. 2020. *Beyond Sticky Notes*. Beyond Sticky Notes, Sydney, p. 15.

[19] Burkett, I. 2012. *An Introduction to Co-Design*. Knode, Sydney.

[20] Kokolakis, S. 2017. 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.' *Computers & Security*, 64, p. 122-134; Obar and Oeldorf-Hirsch (n. 10).

[21] Warren, T. 2020. 'Zoom faces a privacy and security backlash as it surges in popularity.' *The Verge*, April 1. Available at: https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response; Newman, L. 2018. 'A new Google+ blunder exposed data from 52.5 million users.' *Wired*, 12 October. Available at: https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

4 RECRUITMENT

We recruited participants from Sydney and Coffs Harbour through local Facebook groups, deliberately selecting people to ensure a diverse sample. We had 29 applicants from Sydney and selected 15 participants. We had 17 applicants from Coffs Harbour and selected 11 participants. Eleven of our participants identified as male and 15 of our participants identified as female and we have given all of our participants pseudonyms.

The participants ranged in age from 19 to 65. Each time we mention a participant, we give their location and age, e.g. 'Dave (Sydney, 25)'. Our sample was skewed towards young people, with 12 participants under 35 compared with only two people over 55. Our Sydney sample featured more young people (eight people in Sydney to four people in Coffs) and our Coffs Harbour sample had more people aged 45 and up (five people in Coffs to three people in Sydney).

18-24	25-34	35-44	45-54	55-64	65+
4	8	6	6	1	1

5 WHAT IS PRIVACY AND DOES IT MATTER?

Before we started to talk about notice and consent, we wanted to understand how our participants viewed privacy. First, we wanted to gauge how important privacy was to our participants, by asking them to give privacy a rating out of 10. Participants gave privacy a very high score, as the graph below shows. In all, 10 participants gave it 10/10, six gave it 9/10, five gave it 8/10, two gave it 7/10 and two gave it 5/10. The average score was 8.7/10, the median was 9/10. (One participant gave two scores, which weren't counted.) Clearly, most of the participants in our focus groups valued privacy a great deal.

Privacy is being able to keep things about you and/ or your family to yourselves

Uma, Coffs, 46

Next, we asked participants to define privacy. Even experts disagree about how to categorise the concept. The participants' Jamboard notes and the discussion afterwards saw a few key themes emerge.

Privacy as a right. 'The right to be left alone and in peace,' said Felicity (Sydney, 34); 'My right to be left alone,' wrote Jade (Sydney, 25). 'The right to protect personal information,' wrote Xavier (Coffs, 50).

Safety and security. 'Privacy is having security over your own personal information and not having it shared without your permission,' wrote Ellie (Sydney, 19). Karl (Sydney, 62) simply offered a one word definition, 'Security'.

Control. 'To be able to control the information we share with others,' wrote Sally (Coffs, 36).

Access. 'Our own information and personal affairs not being shared with anyone else or publically,' wrote Olive (Sydney, 25).

Finally, we asked the groups why privacy mattered. The answers were wide-ranging. Ellie (Sydney, 19) said that revealing information could 'put you in danger or affect your future'. Natasha (Sydney, 30) said that if your private details were revealed, that might mean people would treat you differently, and perhaps unfairly. And Xavier (Coffs, 50) said, 'Privacy is important in order to ensure individual freedom and identity.' Another participant, Uma (Coffs, 46) was a survivor of family violence and said that keeping her affairs and movements private was a critical factor to ensure her and her children's ongoing safety.[22]

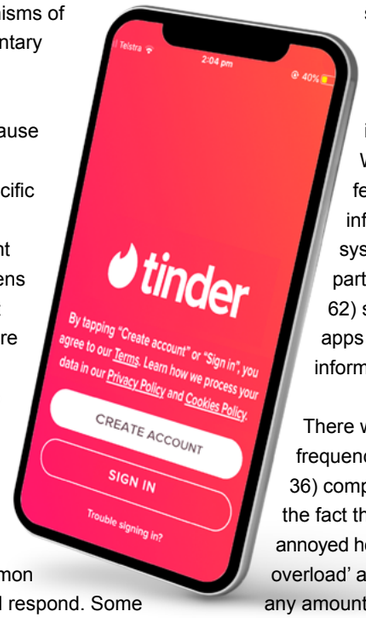
[22] For further research on this area see Dragiewicz, M., Harris, B., Woodlock, D., Salter, M., Easton, H., Lynch, A., Campbell, H., Leach, J. & Milne, L., 2019. 'Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.' Australian Communications Consumer Action Network. Available at: https://accan.org.au/grants/completed-grants/1429-domestic-violence-and-communication-technology-victim-experiences-of-intrusion-surveillance-and-identity-theft

6 | IS NOTICE AND CONSENT WORKING?

There is a simple answer to this question. We already know from the existing research that in many cases notice and consent is broken.[23] However, there is still value in examining people's experiences of the process. Our aim is to shed light on people's experience of consent, to improve the mechanisms of consent, and to further clarify which supplementary mechanisms are needed to protect privacy.

We also wanted to focus on smartphones because while we know that people do not read terms and conditions,[24] there is not much device-specific research available.[25] This is significant, because smartphones have a range of different attributes (or 'affordances'), from smaller screens to more pop-ups, which can make the consent process more complex. We also know that more and more data is collected as smartphone technology advances, with people now able to unlock their phones with their faces and use them as repositories for health data.

We started by asking what people thought about the pop-up notifications common on smartphones. Participants were shown a common request for location and asked how they would respond. Some people were privacy conscious and did not provide many apps with data access; others were relatively open and did not stop to assess these requests. However, a significant proportion of our participants explained that they tried seriously to consider the relevance of requests for data. They generally made a quick calculation about whether the request was in line with the stated purpose of the app. As Felicity (Sydney, 34) said, 'It depends what the app is and why they need it. The thing that just came to mind, [was] apps like Beat the Queue. When I'm at work, for example, I have to allow my location just so it brings up the coffee shops near me.' Felicity saw this as a logical data request and most of our participants were happy to allow this sort of transactional data exchange.



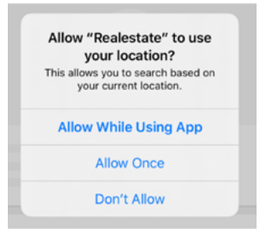
In contrast, people viewed other exchanges as inequitable or illogical. Rosie (Coffs, 42) argued that if she jumped onto the Bunnings warehouse website, the company should not need to know where she lives. She said, 'The price should be the price', clearly believing that this attempt to collect data was an attempt to unfairly extract extra value from the exchange. Participants said unfair value exchanges were common in the retail sector, and also in sporting apps and apps that changed photos of your face (such as FaceApp). As Iris (Sydney, 45) said, 'Unless it's relevant, it's a big fat no from me.' A few participants said that they attempted to review what they allowed apps to do, but others also noted that this was a difficult process to undertake. Ellie (Sydney, 19) said, 'It takes about 10 years, actually to find where it is. Sometimes [they are] hidden under iCloud settings, stuff like that.'

Turning more directly to the issue of *informed* consent, we showed people iOS and Android pop-up notifications. We wanted to see whether people felt these pop-ups provided enough information and whether one operating system was better than the other. Some participants were fatalistic. As Karl (Coffs, 62) said, 'If you have got Google, then these apps are no harm anyway.' Others did not feel informed after viewing either of the pop-ups.

There were also common complaints about the frequency and logic of these requests. Sally (Coffs, 36) complained that the 'permissions are too much'; the fact that 'they need permission for everything' annoyed her. Others pointed out the risk of 'information overload' and that it was going to be difficult to present any amount of information in a pop-up.

Some participants commented on the design of the notifications. Vincent (Coffs, 19) said that the iOS option to click 'Allow Once' '[gave] you more options' than Android. However, Tom (Coffs, 28) countered by pointing out that the iOS request did not give you 'the option for more information'. Olive (Sydney, 25) raised an interesting point about design, noting how many of these notifications mimicked the design of the operating system. As a result, she said that 'if you're kind of a little bit distracted, you might just assume it's from your iPhone itself, like a software update or something like that'. She added, 'There have definitely been times in the past where I've noticed myself like, "Oh crap, I've clicked something I didn't really want to click".'

We turned to whether people were able to manage these forms of consent effectively through their smartphones' permissions architecture. Many participants knew how to do this. Dave (Sydney, 25) was positive about Androids, saying that 'the process of opting in and out of privacy settings [is] not easy, but easier than iPhones'. That being said, several iPhone users also said they knew how to manage permissions. The most prominent reason participants gave for doing so was to manage pop-up notifications and battery life. This suggests they were not accessing their permissions as a way of managing their privacy settings. What's more, some participants did not know how to revoke access to certain data categories, or did not go to the permissions section regularly.



Our final activity in this section focused on terms and conditions. We asked our participants to comment on the contracts from two popular apps, a fitness app (Sweat) and a dating app (Tinder). Several participants said they liked that Sweat presented the terms in a pop-up. In contrast, Tinder was criticised for not forcing people to read the terms. Rosie (Coffs, 42) identified design issues, explaining that, 'our eyes are just immediately drawn to "create account", and you just think, "Oh, that's the next step, click that." And you wouldn't even see that it says by tapping that, you agree.' Aaron (Sydney, 28) went further, saying that he felt like Tinder was 'manipulating me to not get access to the information that should be readily available'.

While Tinder presented a summary of terms, it was only accessible three screens in and then presented the user with additional hyperlinks. Patrick (Coffs, 54) explained this best: 'Once you get on the summary of terms, you've got four hyperlinks on top of that, which obviously must go into more hyperlinks as well.' This maze of additional information would evidently present problems for any enterprising user vaguely concerned about their privacy prior to signing up. However, despite praise for Sweat's pop-up, all of our participants criticised the legalistic nature of the terms. A range of words were used to describe these contracts including 'lengthy', 'lawyer talk' and 'legal jargon'.

We then asked participants to comment on the presentation of terms and conditions during a sign-up process for a Google account on a smartphone. Generally, the feedback on Google's terms was positive, with participants noting the contrast between this process and Sweat and Tinder. Participants said that these terms were 'easier to read', 'all the points [were] summarised' and it used 'simple language'. Vincent (Coffs, 19) suggested that it might be a clever business strategy, because 'it makes them sound much more trustworthy ... the first thing they're doing is they're giving you this concise list of what they're going to do with your data'. This seemed to be a leading example of how to present privacy information. In one focus group, the majority of participants agreed that they would be more likely to read the terms and conditions.

However, other focus groups pointed out that no amount of formatting and summarising would be adequate. Even if Google's approach was exemplary, it didn't translate into actual control. An exchange from one of our Coffs Harbour focus groups bears this out:

James (researcher)**:** Going back to our original definitions of privacy, control was quite important for a lot of people here. Do we feel like we're in control here?
Sally (36): No.
Patrick (54): No.
Quentin (65): No, you're not, you're not.

In another focus group, Gus (Sydney, 38) made a similar point by saying that often people don't really have a choice, other than take it or leave it. 'No matter the way it's presented, it's not really a choice because if you don't agree, you can't use the app,' he said. 'So whether it's one page or a hundred, the final result will be, if you don't agree, you can't use the app.'

Maddie (Sydney, 35-40) summed it up in a neat phrase: 'Sometimes, to me, consent is more like a trap.' For Maddie, consent was often contained in terms and conditions that were long, complicated and in a very small font. 'We just sign it and then when we have any problem later on, then they say, "Well, you already signed." So we're like, "Yeah, okay. Let's hope that it's positive and then they're using in a positive way." Sometimes we don't have any option.'

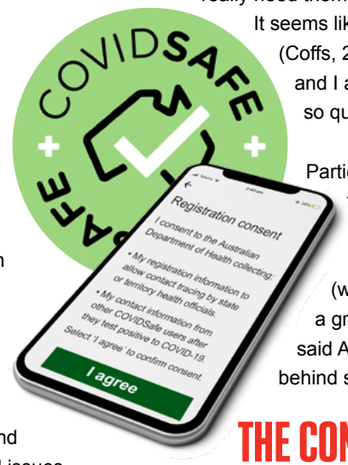
[23] Giannopoulou, I. 2020. 'Algorithmic systems: The consent is in the detail?' *Internet Policy Review* 9(1); Susser, D. 2019. 'Notice After Notice-and-consent: Why privacy disclosures are valuable even if consent frameworks aren't.' *Journal of Information Policy* 9, p. 37-62.

[24] Obar and Oeldorf-Hirsch (n. 10).

[25] We note that there is some emerging work in this area e.g. Tsavli, M., Efraimidis, P.S., Katos, V. and Mitrou, L., 2015. 'Reengineering the user: privacy concerns about personal data on smartphones.' *Information & Computer Security* 23(4), p. 394-405; and Kreuter, F., Haas, G.C., Keusch, F., Bähr, S. and Trappmann, M. 2020. 'Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent.' *Social Science Computer Review* 38(5), p. 533-549.

7 | THE COVIDSAFE APP
GIVING GOVERNMENT CONSENT

In April 2020, the Australian government launched the COVIDSafe contact tracing app. As the government explained: 'The COVIDSafe app is a tool that helps identify people exposed to coronavirus (COVID-19). This helps us support and protect you, your friends and family.'[26] The app, one of various different contact tracing technologies adopted by governments globally, was based on Singapore's TraceTogether app.[27] It relies on Bluetooth technology, Amazon Web Services and a centralised server. In May, the federal government passed legislation to amend the Privacy Act to protect data collected by the app.[28] We thought the app presented a timely and concrete example of new technology that raised issues of consent, privacy and smartphones.



Our focus groups were held in July, three months after the app's launch. The participants expressed a wide range of opinions. In all, the number of those who said they had downloaded the app was roughly equal to the number of those who said they had not downloaded the app. There were also no discernible differences between groups in Sydney and Coffs Harbour: downloaders and non-downloaders were roughly equal in number in both locations, with a correspondingly wide range of views about the app.

TO DOWNLOAD OR NOT TO DOWNLOAD

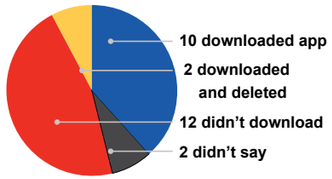
Most people who downloaded the app didn't have privacy concerns. Instead they were focused on getting through the global pandemic. Xavier (Coffs, 50) said that he was 'in a hurry to see international travel return, so I just jumped straight on it'. Beth (Sydney, 47) said that 'the fact that we're facing this global pandemic is the real big concern here, so we just put privacy aside'. Aaron (Sydney, 28) said that people were already giving away lots of information to the government anyway: 'At least with COVIDSafe, there's an actual purpose behind it. There's public good involved in it as opposed to the government just extracting information.'

Of those who didn't download the app, privacy concerns tended to be mixed in with concerns about the app's effectiveness. Harry (Sydney, 41) said that he 'was never really convinced by it. It was built too quickly. Somebody threw money at a problem to fix something and build it up.' But then he also added, 'I don't really need them to know what I'm doing, where I'm going. It seems like a pretty open slather attempt.' As Zara (Coffs, 29) said, 'Privacy was also [a] huge [concern], and I also didn't think how you can push out an app so quickly and expect it to work.'

Participants also expressed concerns about the government's inability to protect the data, and some were concerned about the involvement of Amazon Web Services (which only a few knew about). 'This is a bit of a grey area that some corporation is involved,' said Aaron (Sydney, 28). 'Is there a profit motive behind some of these things?'

THE CONSENT PROCESS

We then led participants through the sign-up process for the app, showing them a series of smartphone screenshots. We wanted to see whether their opinion of the consent process for a government app would be any different to that of a commercial app. Many of our participants were positive about the COVIDSafe consent process. Vincent (Coffs, 19) noted that people were forced to read the terms, saying, 'it's really positive that you have to scroll through the summary to click next'. Beth (Sydney, 47) also liked that the information was 'very clear and not legalistic or jargonistic', which summed up the view of many.



However, a smaller group of participants were unimpressed. 'I feel like it's very contradictory,' said Zara (Coffs, 29), who hadn't downloaded the app and questioned the app's description of how data was being stored. She said the terms were contradictory: 'In the first instance, they're saying that it's only stored on your phone. And then in the second instance, it's saying, "You have to basically ask your information to be deleted from the secure server." So it's not just being stored on your phone.' Jade (Sydney, 25) said that she would have preferred a 'minute and a half or two minute max video explaining it all'.[29]

For our participants, it emerged that many of their decisions about notice and consent revolve around trust. And the participants seemed to divide fairly evenly into two camps: those who trusted governments more than companies, and those who trusted companies more than governments. As Harry (Sydney, 41) said, people would probably be likely to trust these terms and conditions because of the way the app looks. He said, 'It looks like a government form, one that you usually just go, "Next, next, accept".' Beth (Sydney, 47) said that she trusts the government more than companies such as Facebook, even if the government can be hacked too, and has to collaborate with third parties to develop this sort of technology. But Zara (Coffs, 29) disagreed, arguing that while 'companies just want my data to re-market products to me, I just don't trust the government as much'.

[26] Australian Government Department of Health 2020. 'COVIDSafe app.' Available at: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

[27] Taylor, J. 2020. 'Coronavirus apps: how Australia's Covidsafe compares to other countries' contact tracing technology.' *The Guardian*, May 3. Available at: https://www.theguardian.com/australia-news/2020/may/03/coronavirus-apps-how-australias-covidsafe-compares-to-other-countries-contact-tracing-technology

[28] Office of the Australian Information Commissioner 2020. 'The COVIDSafe app and my privacy rights.' Available at: https://www.oaic.gov.au/privacy/covid-19/the-covidsafe-app-and-my-privacy-rights/

[29] The app's consent process does not have video explainers, but video explainers about the app and how it works can be easily found online: e.g, https://www.health.gov.au/resources/videos/covidsafe-app-keeping-us-all-safe-from-coronavirus and https://www.youtube.com/watch?v=JI3uPu9sYRg

8 | FAILURE OF CONSENT:
EAVESDROPPING AND SHADOW PROFILES

On the topic of trust, people felt that they could not fully trust their smartphones. In more than one focus group the conversation switched, unprompted, to concerns about smartphones eavesdropping on users. Iris (Sydney, 45) said, 'I'm equally disturbed about Google hearing everything that we say and listening to our phones.' 'It's disturbing,' agreed Felicity (Sydney, 34). 'I've been in that scenario, copious amounts of times, having conversations, and you'd be scrolling on Facebook or Instagram or something, and it'll just pop up as an ad, what we've been talking about. And it's inappropriate, unethical, and it's also scary.'

This raises an additional complication in the discussions around smartphones and consent. There is a growing perception that companies and app developers are listening to our conversations without asking. In 2019, researchers found that our phones are not listening to us all the time.[30] However, a former employee revealed Apple has paid contractors to listen to people's conversations with Siri.[31] Similarly, both Google and Amazon have admitted that sometimes their employees listen to recordings captured by voice assistants for training purposes.[32] Regardless of the extent of the practice, the prevalence of this belief underlines the lack of trust that people have around their devices and technology companies. At a minimum, it is clear from these discussions that some people no longer always expect to be asked when these companies start collecting data. For several of our participants, this was a grave concern.

We wanted to explore in greater detail the idea of data collection in the clear absence of consent. To do so, we raised a hypothetical. Imagine five friends. Four of these friends are on the same social network, but the fifth is not. That fifth friend, however, appears in the course of various conversations and photos shared by the others. Hence it is possible that our imaginary social network builds a full profile of the fifth friend, even though this person has never used that service, and has never consented to any data collection. Research has shown definitively that such 'shadow profiles' are possible.[33] For its part, Facebook denies collecting shadow profiles, but does admit to collecting data on non-users for the security of its users.[34]

Most of our participants objected strongly to such practices, using words such as 'unethical', 'unacceptable' and even 'illegal'. 'That would be like me spying on my neighbour and keeping a diary and photos of them,' said Rosie (Coffs, 42). 'You'd be so furious if a person was doing that to you, so for a company to be doing that without your knowledge is just appalling.' As Aaron (Sydney, 28) said, 'Why should that organisation get to use your information for their gain? That's where it's a kind of a theft in a way to me. I find that really unethical.'

[30] Tidy, J. 2019. 'Why phones that secretly listen to us are a myth'. *BBC News*, September 5. Available at: https://www.bbc.com/news/technology-49585682

[31] Gartenberg, C. 2019. 'Apple's hired contractors are listening to your recorded Siri conversations, too'. *The Verge*, July 26. Available at: https://www.theverge.com/2019/7/26/8932064/apple-siri-private-conversation-recording-explanation-alexa-google-assistant

[32] Ibid.

[33] Molitorisz (n. 1), p. 49-56.

[34] Ibid.

9 THE ROLE OF THE LAW

Another consistent theme throughout the focus groups was that consent needed to be 'more of a legislative thing rather than an individual thing'. As Rosie (Coffs, 42) said, this is all 'too hard on the individual level ... so it has to be policy-based rather than individual-based'.

Consent alone can't do the job, especially when it comes to vulnerable populations. As Ellie (Sydney, 19) said, 'A lot of people accept [terms and conditions] so willingly because they don't understand it. And they're often maybe the more vulnerable people. I feel like the law has a really big role in that sense.' Participants were particularly focused on transparency and wanted to know more about the companies collecting their data. Olive (Sydney, 25) proposed the idea of a standardised privacy ratings scheme, by using the comparison of a restaurant:

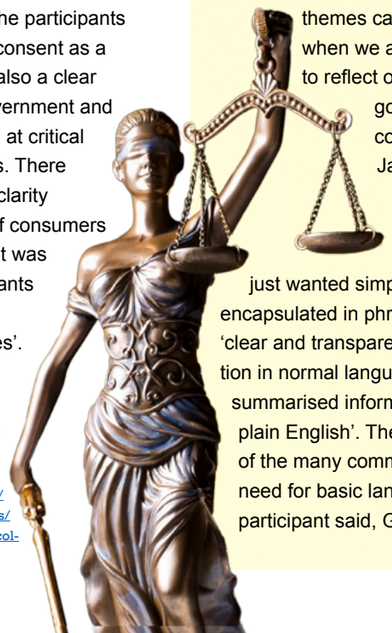
> *The first thing that you see as you walk in through the door is the sanitation rating or the cleanliness rating, and that really holds the restaurant accountable. I think if there was something similar, where we would both be educated as a consumer, but also where companies would be held accountable for the integrity of their data policies, I think that would really help clear certain things up a bit.*

(See also 'Consent: Can we fix it?', below.) Several participants also stressed the importance of education. As Dave (Sydney, 25) said, 'the education of young adults is key, and just bringing this information to a wider audience, so people are more aware. Otherwise it'll just really put people at a disadvantage.'

As part of this discussion about the law, we asked for participants' view on how consent should be defined. Australia's new Consumer Data Right requires consent to be: voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn.[35] We put these criteria to our participants, providing explanation where necessary. Generally, the participants said that these were all important ingredients in a legal definition of consent. However, 'easily withdrawn' was the ingredient most commonly cited as something the law should mandate. As Vincent (Coffs, 19) said, 'It feels like now you give consent really easily, but then it's really, really hard for you to take it back. It should go both ways.'

Our participants recognised the complex nature of consent and how their privacy intersected with that of their friends and family. However, while the participants clearly wanted to keep consent as a mechanism, there was also a clear expectation that the government and regulators would step in at critical points to protect citizens. There was little consensus or clarity about the precise role of consumers vis-a-vis governments. It was just clear to our participants that lots of 'companies [were] out for themselves'.

[35] Office of the Australian Information Commissioner 2020. 'Chapter C: Consent — The basis for collecting and using CDR data'. Available at: https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data/



10 WHAT GOOD & BAD CONSENT LOOK LIKE

Ultimately, we wanted to find new ways to approach the consent problem. But first, we needed to know as clearly as possible what people did and didn't like about consent in its current form. As the above analysis shows, people liked the simplicity of Google's terms. Many also thought the COVIDSafe app design was a good model of informed consent. In contrast, other commercial apps were criticised for legalese and, at times, seemingly tricking people into giving consent. So it was no surprise that these themes came to the fore when we asked participants to reflect on what was good and bad consent through a Jamboard activity.

Above all, participants just wanted simplicity, which they encapsulated in phrases such as 'clear and transparent communication in normal language' and 'simple, summarised information that is in plain English'. These were just two of the many comments about the need for basic language. As one participant said, Google's contract had clear 'spoken-type language', which was an example of what other consent mechanisms should strive towards.

Participants also had additional suggestions that might increase simplicity. Gus (Sydney, 38) suggested that companies offer 'clear, concrete and real-world examples of use'. A number of our participants were pleased that Google's model of informed consent offered 'concrete examples about things you do. You're writing a message, you search for a restaurant, you watch a video'. For many of our participants, this approach helped them get a better sense of how their data might be used. However, Sally (Coffs, 36) noted that the broad scope of Google's terms meant that even a better informed consent process could not solve the unequal relationship between Google and consumers.

Participants also wanted consent to be targeted and clear, with 'the biggest privacy concerns addressed first' (Aaron, Sydney, 28) and 'the most important parts highlighted' (Jade, Sydney, 25). Further, participants wanted relevance. As Dave (Sydney, 25) said, the best consent requests made a 'clear link between the app/service and the allowances you are having to make', while Beth (Sydney, 47) noted that 'it works to ask for consent where it is relevant.'

From these initial suggestions, we started to build a sense of what our participants really valued as part of the informed consent process. For the ordinary person, informed consent needed to be:

- **SIMPLE**
- **CLEAR**
- **TARGETED**
- **LOGICAL**
- **RELEVANT** *and*
- **REAL-WORLD**

(with concrete examples)

We also started to build a sense of what people didn't like about the current consent process. As might be expected, the most prominent issue was the use of legalese and other complicated forms of construction, featuring 'language that benefits the company, not the user'. Some participants noted this is a particular problem for vulnerable groups, including kids. As one participant said, information provided about the processing of children's data was 'too easy for kids to ignore'. Alongside complaints about 'long-winded and complex legal language', people also did not like the 'take it or leave it' model of consent. As one participant noted, 'not consenting shouldn't mean you can't use it at all'.

Specific issues about smartphones were also discussed. Indeed, many participants felt that existing models of consent did not capture the nuances of how people actually used technology. Consent is an individual process that presumes that one person is using the app or phone. However, as Rosie (Coffs, 42) said, 'many people allow their kids screen time on their own phone'. (We return to this point below in a section on collective privacy.) The unique properties of the smartphone were also ignored. A number of our participants noted the issues with 'small print', the fact that the user experience 'wasn't considered in the consent process' and the abundance of 'unstructured information'. >

Some fundamental aspects of the smartphone experience also raised issues. Olive (Sydney, 25) noted that 'smartphone systems themselves don't necessarily provide enough information about built-in features such as touchpads and cameras', suggesting that this raised further issues when apps went on to request the use of these systems. App updates were seen as another potential problem. Rosie (Coffs, 42) said that apps might add new features but that in her experience consent is not always re-obtained. Also, Clarissa (Sydney, 37) noted that withdrawal of consent was particularly hard. As she said, someone might give consent but end up 'not really using the apps'. This led some to suggest that there should be a time limit on consents given.

From our discussion of what participants explicitly did not want, we can supplement our previous list. Informed consent should also be sensitive to:

- **VULNERABLE GROUPS**
- **HOW PEOPLE USE TECHNOLOGY**
  (e.g. multiple users on one device)
- **SMARTPHONE CHARACTERISTICS**
  (e.g. small print, unstructured info)

What's more, informed consent should be:

- **RE-OBTAINED WHEN APPS CHANGE**
  (with new features and data uses)
- **EASILY WITHDRAWN**
- **TIME LIMITED**

11 | CONSENT: CAN WE FIX IT?

Use simplified language with examples
Xavier, Coffs, 50

For researchers, it's easy to become bogged down in largely theoretical discussions about legal provisions and reform agendas, thereby losing focus on the core problem and how to solve it. In this case, it turned out that our participants had a lot of common sense solutions. This was one of the best outcomes from the project: participants went beyond telling us what they liked and didn't like about informed consent. They also offered ideas on how to improve the process. The answers are out there. We just need to ask. And the most interesting answer is that participants didn't think that consent is unfixable. They wanted to keep notice and consent. And, as we have already begun to show, they offered a number of solutions for how to improve it, particularly on smartphones.

Apart from an open-ended discussion, we also asked participants to give us solutions to solve the consent problem by putting ideas on a Jamboard. In this section, we synthesise our findings. After collating and coding notes from all the focus groups, we found a consensus around three key areas, each focused on a different element of the consent puzzle: **clarity**, **governance** and **design**.

CLARITY

Participants still wanted to participate in the consent process but also wanted to be able to understand what they were consenting to. As the earlier sections of this report discussed, our participants generally did not read terms and conditions and many felt that companies were deliberately trying to trick them. The small smartphone screen only made the problems around notification and consent even harder to manage.

In response, participants said that companies needed to be clearer about how their data was being used. Aaron (Sydney, 28) wrote on Jamboard that they should be 'really blunt with how they use your data to make money – i.e. it's used for advertising'. Beth's (Sydney, 47) post was along similar lines, stating that 'T&Cs should be in easy to understand language with clear examples'. Others provided even more detail, noting that on a smaller screen decisions about formatting and font were particularly important. Dave (Sydney, 25) noted the 'importance of formatting (bold, italics, etc.)' and 'clear spacing between text'.

'Incognito mode' for all apps
Aaron, 28, Sydney

The legalistic nature of terms and conditions has long been a problem in the notice and consent space. As noted above, however, many participants were impressed with Google's presentation of terms and conditions. They were under no illusions. They knew that Google collected large amounts of data, but they spoke positively about Google's attempts to provide some clear explanations.

You should be able to consent to some terms of service but not others, you should be able to tell them they can't sell your data
Vincent, Coffs, 19

Participants repeatedly stressed the importance of simplicity. Natasha (Sydney, 30) said that 'being able to explain complex things in simple terms is an art form' but added that 'it's doable, and if you can't do it then find someone who can'. Olive (Sydney, 25) works in the health sector and has previous experience with informed consent from her work. In her mind, technology companies should and could be able to do this. She explained that her industry experience convinced her that 'there was definitely a way to present complicated information in a way that is simple and understandable'. As she said, informed consent was 'not something that you can just skim through' and it should be the same for the tech sector. This was a powerful point made by several participants: that tech companies could make consent work if they wanted to.

Other participants said that more was needed than a standard contract. We've already mentioned Jade's (Sydney, 25) preference for videos. Maddie (Sydney, 35-40) also said that videos, graphs and pictures were 'more catchy, and you [the consumer] want to focus on that'. Iris (Sydney, 45) echoed this, saying 'having the T&Cs in a video would be awesome. I'd be much more likely to watch a [one] minute video then scroll through pages and pages of consent and privacy.' Iris's focus group also had a discussion about the needs of people from a non-English-speaking background. Gus (Sydney, 38) noted that his parents were from Eastern Europe, and while they tried to read through these terms, they ended up just scrolling through and accepting. As Iris said, informative videos could be a great help to many people.The benefits of delivering terms more clearly were also outlined by Quentin (Coffs, 65), an older participant who struggled to read standard contracts. He explained that:

Small print is very, very important, I've been caught before and I didn't look at the small print properly and I did consent. I had a lot of trouble getting that app back off my phone. It was very, very misleading and there were all the ads under the sun for stuff that I did not want. >

Quentin said that he sometimes transfers terms and conditions back to his computer so he can read them clearly. He admitted this was ‘a bit of a pain’. ‘The smartphone with a small print is very hard at times to read.’

Our focus groups suggest that many people have become resigned to the complexity of the current data economy. However, they also suggest that many people have hope that consent can be fixed. Our participants wanted companies (and legal drafters) to engage in a clearer conversation about the process by which data is collected and shared. The solution involves clearer drafting of terms and conditions, but also alternatives such as images, videos and graphics. Regardless of wider legal reform, consumers still want to be part of the conversation. This presents a challenge for drafters who have been speaking to other lawyers, rather than people more widely, including those without a law degree.

GOVERNANCE

Our participants knew that in many cases, companies and in-house counsel were not on their side. Companies and counsel may not want to change their current practices. Moreover, even if some companies did decide to work towards being simple and clear, our participants did not look forward to negotiating a new thicket of contracts, each taking a different approach to the idea of simplicity and clarity. This led some of our participants to suggest various top-down reforms to improve notice and consent, which could be introduced by government or industry.

The Sydney participants focused on standardisation. Dave (Sydney, 25) suggested introducing ‘a streamlined framework/process that all companies/organisations have to adhere to’. In another focus group, Natasha (Sydney, 30) raised a similar idea, but took it further, suggesting that for their terms and conditions ‘all apps have a three-sentence summary at the beginning’. Her three critical elements were:

1. HOW THE APP WORKS/WHAT IT DOES
2. THE SPECIFIC DATA IT COLLECTS
3. HOW THE APP IS BENEFITING FROM THIS

Wendy (Coffs, 19) recognised how hard this idea would be to implement in practice, given how many apps there were on the app store.

Several Coffs Harbour participants were particularly interested in transparency and enforcement as a governance mechanism. Sally (Coffs, 36) suggested introducing ‘a controlling body with standard criteria’ to assist with effective monitoring. Further, she said privacy information could be placed in a searchable ‘over arching archive’. In this archive, a person could see ‘what the app does, what it records, where the information is used and you can literally see it in easy-to-use form.’

A similar idea was suggested in our second Coffs focus group, where Tom (Coffs, 28) called for ‘a system that compares all of the different privacy [terms making] it clearer and easier to choose’. Patrick (Coffs, 54) had a similar idea, explaining how a sort of privacy one-stop-shop might work:

> *So there should be an app that ... all the stuff that’s on your phone, it would go through the whole lot and tell you what permissions are being given, all the access it gives you and all that. And you can go through the app really quickly and just work out what you want to keep and what you don’t want to keep.*

With regulators increasingly collaborating internationally as they work out how to regulate technology companies,[36] some sort of global coordination around these issues is not out of the question. It is also worth noting that community projects that compare terms of service are already available.[37] It may be that educating people about available options and formalising some existing processes is a viable option for privacy regulators. (See also ‘The Role of the Law’, above).

DESIGN

Many participants in Sydney and Coffs recognised that consent was also a design problem – and a potential solution. Widespread agreement on this point suggested to us that privacy-by-design was an approach valued by participants and presented a potential way to get ourselves out of the consent trap.

One group of solutions focused on ensuring that people actually read the terms and conditions. Many of our participants noted that lots of sign-up screens don’t even force you to look at the terms and conditions before signing up. Our Tinder example (see p. 8) used this method, which sparked a discussion in one of our Coffs focus groups.

Patrick (54): There’s no obvious link about checking the terms. It’s just part of the whole paragraph.
Rosie (42): And most people probably would not even read that and just click on the Create Account button.
Quentin (65): Yeah, and you don’t know what you’re clicking on, you haven’t looked at it.

Some participants suggested that people should be forced to read terms and conditions before being allowed to use an app. Suggested options included having to type in an answer or tracking whether or not consumers had opened the terms and conditions (Rosie, Coffs, 42), requiring people to ‘tick a box’ (Uma, Coffs, 46), or making people ‘scroll through a summary’ of terms before accepting (Vincent, Coffs, 19).

Another group of solutions suggested moving towards granular or personalised consent. As noted above, several participants were concerned about the ‘all or nothing’ approach to most terms and conditions, suggesting that people should have more choice. As Beth (Sydney, 47) said, ‘an option to withdraw it or change the conditions would be useful’. More detailed suggestions included ‘boxes you can select or unselect relating to the level of data that you want to share’ (Iris, Sydney, 45), the ability to ‘consent to some terms of service but not others’ (Vincent, Coffs, 19), and even more granular options, allowing data to expire or be de-identified after a certain amount of time (Aaron, Sydney, 28).

Asked to elaborate, Vincent (Coffs, 19) referred back to the COVIDSafe app and explained that he liked the way it forced you to look at the terms, but in a limited way. He noted that ‘you weren’t scrolling through all of it, and you weren’t scrolling through none of it’. Instead, you were ‘scrolling through really important points’. Various companies – including social media platforms – provide customers with some control of their data once they’ve signed up. The Facebook Privacy Checkup is an example, allowing people a degree of control over their sharing and data settings.[38] However, it was telling that participants wanted more control at the outset, at that critical point where they were entering into a legal agreement with a company about the use of their personal data.

Other participants said that it was hard to agree to terms about the use of a service when they hadn’t even used it before. They suggested a preliminary period where people could have ‘the option to use once’ (Ellie, Sydney, 19) or maybe just letting you use some of the elements of the app if you >

agree to certain aspects of the terms and conditions (Felicity, Sydney, 34). This 'try before you buy' consent model is an interesting approach, which would give people a better sense of the value they might get out of an app before committing to signing up.

Our participants shared some excellent ideas. Some were more feasible than others, but all made an important point: that consent is also a design problem. Consent, and the idea of fairness that underpins it, is not just a matter of writing clearer contracts (although that would help), but is also about empowering people to make decisions about their data and ensuring that technology is built according to principles of equity and fairness. Importantly, these design elements increasingly came to the fore as people spoke about their smartphones. We suspect it was because, as Olive (Sydney, 25) pointed out, it's quite easy to accidentally give consent on smartphones.

Future reforms may well involve privacy practitioners working in conversation with developers and user experience (UX) and user interface (UI) professionals to design privacy-enhancing features for consumers. (User experience designers work to improve how people feel when they use products – this might be the touch or feel of a device or the overall emotions you feel when you use it. User interface designers focus on how software looks. These roles can often be combined.) We return to this design issue below.

[36] Australian Competition and Consumer Commission 2020. 'Competition agencies to coordinate on cross-border investigations.' Available at: https://www.accc.gov.au/media-release/competition-agencies-to-coordinate-on-cross-border-investigations-0

[37] E.g. see https://tosdr.org/

[38] Facebook explains how to find and use their Privacy Checkup feature here: https://www.facebook.com/help/443357099140264

12 | COLLECTIVE PRIVACY

Participants tended to talk about individual privacy. However, online privacy is better thought of as a collective or networked phenomenon.[39] Our lives and our privacy are always bound up with other people, and our decisions about privacy are often also decisions about the privacy of our friends, families and sometimes strangers. When I post a picture at a social event, I am revealing my friends and family at the same time.

For several participants, this concept came to the fore when talking about children and social media. Clarissa (Sydney, 37) said that she did not 'put [her] kids on social media, just to protect them'. Natasha (Sydney, 30) said that parents setting up profiles for their babies was her 'pet peeve', being 'unethical because that person has not consented to you documenting their whole life from age one week'.

Another of our participants noted that the networked and collective nature of online privacy could also have ramifications for survivors of family violence. Uma (Coffs, 46) is herself a survivor of family violence. After relocating with her children, she was hyper-vigilant about her privacy, including her visibility on social media. Despite her best efforts, her ex-partner was able to track her down through the social media of her friends and family, forcing her to move again. This shows how people's data is interconnected, and how the accidental sharing of personal information about others can, at times, endanger their lives.[40]

OUR PRIVACY IS ALWAYS BOUND UP WITH OTHER PEOPLE AND OUR DECISIONS OFTEN INVOLVE FRIENDS, FAMILIES AND SOMETIMES STRANGERS

Several participants also said that they had friends or family who didn't want to be on social media, and this meant that caution was required when uploading photos or posting updates. As Zara (Coffs, 29) said, 'One of my best friends who I've known for a decade does not want to be on social media.' Hence, she 'doesn't share any photos of him on social media'.

These examples of the collective nature of privacy present challenges for thinking about the role of consent, as the standard approach still adopts an individualistic model.

[39] Molitorisz (n. 1), p. 166-7.

[40] See also Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. 2018. 'Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms.' *Feminist Media Studies*, 18(4), p. 609-625.

13 | A FUTURE FOR INFORMED CONSENT?

It was clear from our focus groups that the current approach to notice and consent is broken. This finding is unsurprising. As detailed in the introduction, it aligns with previous research. Our participants said that they felt disempowered by the consent process and that in many cases they had no choice but to accept the terms offered. A number of additional issues were raised specifically about smartphones, with participants noting the difficulty of reading contracts on smaller screens, the fear that smartphones were listening in on conversations and the risks that come with the convenience of a high-powered computer roughly the size of a pack of cards that went with them everywhere, and was always on.

However, what was surprising, and also exciting, was that people still valued notice and consent. At the end of the focus group in which she'd said consent is like a trap, Maddie (Sydney, 35-40) said, 'It's still useful. It's a tool somehow to protect ourselves as well. If it can be made more simple, that's better. But now it's useful. It's better than nothing.' Our participants clearly recognised that notice and consent often isn't working, but that doesn't mean they think it's broken beyond repair. Rather, they think it can be fixed. Indeed, they want it to be fixed. Our takeaway here is that people want consent to work.

Overwhelmingly, participants recognised that this fix would require the law to play a major role. First, we suggest this involves better enforcement of existing law. Recently, the ACCC has launched two consent-based court actions against Google. In 2019, the ACCC alleged Google misled consumers on the collection and use of location data;[41] and in 2020, the ACCC alleged that Google misled consumers by not adequately explaining changes to their data collection processes.[42] Even if they fail, these actions will clarify the law concerning data and consent, so that the reach of current regulation is better understood.

Second, we suggest the key role of the law also involves passing new law and implementing new governance structures. This can involve self-regulation and co-regulation, but also requires the reform of top-down law. Fortunately, privacy law reform is under way in Australia.[43] The proposed reforms – including strengthening the requirements for consent, prohibiting unfair contract terms and certain unfair trading practices and implementing a privacy code for digital platforms (see Introduction) – seemingly address the core of our participants' concerns. Our takeaway here is that privacy professionals and others need to recognise the key role of law, and encourage appropriate law reform.

At the same time, participants recognised that design must play a major role. Participants' comments consistently revealed that UX and UI design was critical to ensuring a fair consent process on smartphones. Further, participants engaged with the co-design process and worked to offer solutions. These proposed solutions recognised the increasing complexity of the data environment. Recent research has shown the manipulative potential of options that are not presented clearly and dispassionately. These strategic design choices are called 'dark patterns',[44] and our participants were well aware of the phenomenon. The potential mismatch between law and design can be seen in the recent appearance of consent pop-ups since the introduction of the GDPR. Research has found that many consent mechanisms did not meet the standard for European law[45] and actively 'nudge' users towards consenting.[46] Our takeaway from this is that privacy professionals and others need to continue their engagements with UX/UI designers to ensure that standard user experiences and interfaces work to support, and not undermine, legal frameworks.

As this takeaway suggests, law and design can be complementary. As an illustration, Apple has recently changed how it will handle mobile ad tracking.[47] From next year, Apple devices running iOS14 will specifically ask users whether they want to be tracked by apps. The pop-up is clear, with example text stating:

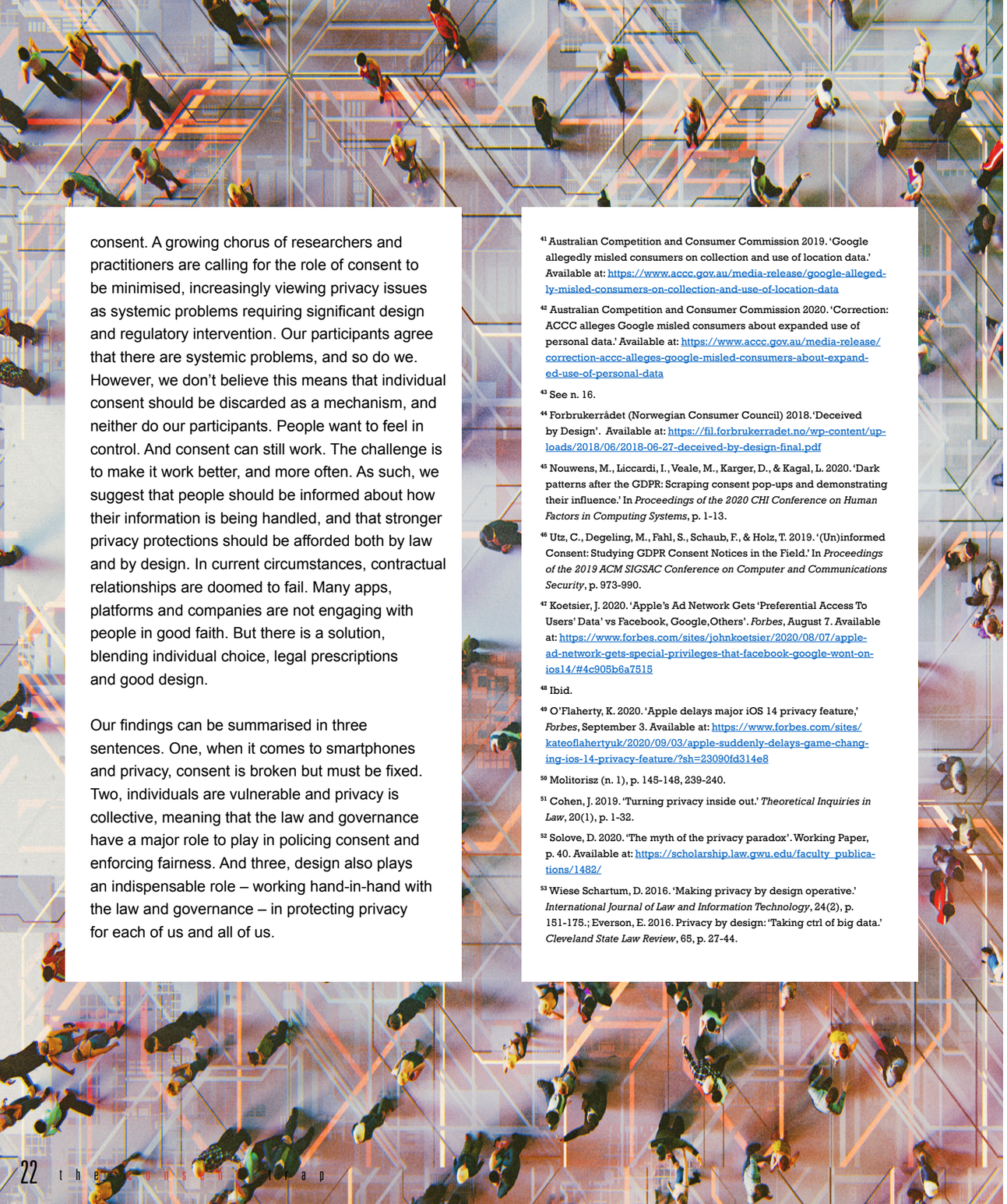
> *'Pal About' would like permission to track you across apps and websites owned by other companies.*[48]

The user has the option to 'Allow Tracking' or 'Ask App Not To Track'. This change has caused outcry among the mobile ad industry as many advertisers and companies expect that people will refuse tracking because of the clear description provided. This predicted outcome suggests that our participants were right. Design is key. But of course, Apple made this decision independently. There is no reason for other companies to follow suit. Indeed, there is no reason why Apple won't perform an abrupt about-face. As it happens, following pushback from Facebook and advertisers, Apple announced in September 2020 that it would delay the launch of its iOS14 privacy feature.[49] However, our point is that the law can work hand-in-hand with design. Here, for instance, the law could make such consent mandatory. This would align with what our participants said they want from their devices.

Our analysis of the role of consent highlights the importance of clarity, law and design working together. Our participants emphasised that more needs to be done to ensure that companies provide clear information to users, and offer real choices. They wanted interfaces to standardise terms, offer clear and simple drafting and work towards minimising people's confusion. This also involves the law (what sort of terms and conditions must be provided?) and design (how can design further ethical and legal requirements?). Best practice demands that options be presented in a way that encourages people to think about their privacy, and that promotes fair choices.

After all, not everything is about what happens on the user's screen. As several participants acknowledged, consent is no longer just an individual decision but part of a systemic process. People do not want to be cut out of the process, but recognise that individually they can only do so much. It's a point supported by recent arguments in the academic literature, which call on solutions that move beyond individual rights. One of the authors of this report has written of the need to protect not just individual privacy, but 'relational privacy', which is increasingly the way that privacy manifests in a digital world.[50] For some academics, this means that solutions must be design-based. Julie Cohen argues that, 'consent is a liberty-based construct, but effective data protection is first and foremost a matter of design'.[51] And Daniel Solove notes that 'effective privacy regulation focuses on the architecture of the personal data economy – data collection, use, storage, and transfer'.[52] However, our participants explicitly wanted good design, but also good law. And indeed, scholars have addressed the question of how regulators can implement privacy by design,[53] just as the GDPR made 'privacy by design and by default' the law in Article 25, as we have noted.

The balance that our participants call for represents a nuanced approach to the problem of notice and >



consent. A growing chorus of researchers and practitioners are calling for the role of consent to be minimised, increasingly viewing privacy issues as systemic problems requiring significant design and regulatory intervention. Our participants agree that there are systemic problems, and so do we. However, we don't believe this means that individual consent should be discarded as a mechanism, and neither do our participants. People want to feel in control. And consent can still work. The challenge is to make it work better, and more often. As such, we suggest that people should be informed about how their information is being handled, and that stronger privacy protections should be afforded both by law and by design. In current circumstances, contractual relationships are doomed to fail. Many apps, platforms and companies are not engaging with people in good faith. But there is a solution, blending individual choice, legal prescriptions and good design.

Our findings can be summarised in three sentences. One, when it comes to smartphones and privacy, consent is broken but must be fixed. Two, individuals are vulnerable and privacy is collective, meaning that the law and governance have a major role to play in policing consent and enforcing fairness. And three, design also plays an indispensable role – working hand-in-hand with the law and governance – in protecting privacy for each of us and all of us.

[41] Australian Competition and Consumer Commission 2019. 'Google allegedly misled consumers on collection and use of location data.' Available at: https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data

[42] Australian Competition and Consumer Commission 2020. 'Correction: ACCC alleges Google misled consumers about expanded use of personal data.' Available at: https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data

[43] See n. 16.

[44] Forbrukerrådet (Norwegian Consumer Council) 2018.'Deceived by Design'. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

[45] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. 2020. 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence.' In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 1-13.

[46] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. 2019. '(Un)informed Consent: Studying GDPR Consent Notices in the Field.' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, p. 973-990.

[47] Koetsier, J. 2020. 'Apple's Ad Network Gets 'Preferential Access To Users' Data' vs Facebook, Google,Others'. *Forbes*, August 7. Available at: https://www.forbes.com/sites/johnkoetsier/2020/08/07/apple-ad-network-gets-special-privileges-that-facebook-google-wont-on-ios14/#4c905b6a7515

[48] Ibid.

[49] O'Flaherty, K. 2020. 'Apple delays major iOS 14 privacy feature,' *Forbes*, September 3. Available at: https://www.forbes.com/sites/kateoflahertyuk/2020/09/03/apple-suddenly-delays-game-changing-ios-14-privacy-feature/?sh=23090fd314e8

[50] Molitorisz (n. 1), p. 145-148, 239-240.

[51] Cohen, J. 2019. 'Turning privacy inside out.' *Theoretical Inquiries in Law*, 20(1), p. 1-32.

[52] Solove, D. 2020. 'The myth of the privacy paradox'. Working Paper, p. 40. Available at: https://scholarship.law.gwu.edu/faculty_publications/1482/

[53] Wiese Schartum, D. 2016. 'Making privacy by design operative.' *International Journal of Law and Information Technology*, 24(2), p. 151-175.; Everson, E. 2016. Privacy by design: 'Taking ctrl of big data.' *Cleveland State Law Review*, 65, p. 27-44.

ABOUT THE CENTRE FOR MEDIA TRANSITION

The Centre for Media Transition (CMT) is an applied research unit based at the University of Technology Sydney (UTS).

Launched in 2017, the CMT is an interdisciplinary initiative of the Faculty of Arts and Social Sciences and the Faculty of Law. It sits at the intersection of media, journalism, technology, ethics, regulation and business. Working with industry, academia, government and others, the CMT aims to:

- Understand media transition and digital disruption, with a view to recommending legal reform and other measures that promote the public interest;
- Assist news media to adapt for a digital environment, including by identifying potentially sustainable business models;
- Develop suitable ethical and regulatory frameworks for a fast-changing digital ecosystem;
- Foster quality journalism, thereby enhancing democracy in Australia and the region;
- Develop a diverse media environment that embraces local/regional, international and transnational issues and debate;
- Combat misinformation and protect digital privacy; and
- Articulate contemporary formulations of the public interest informed by established and enduring principles such as accountability and the public's right to know.

The CMT's published works include reports on digital defamation, trust in news media, the state of regional news and news media innovation. Current projects include work on industry self-regulation, privacy, news verification, foreign reporting and press freedom. The CMT has consulted for the Australian Competition and Consumer Commission and the Australian Communications and Media Authority. We are also the home of the Asia-Pacific bureau of First Draft News, which combats misinformation.

The Centre regularly hosts public events, conferences and forums. You can sign up to our regular newsletter at bit.ly/2lXvs6D. Details of events and the CMT's work can be found on our website at cmt.uts.edu.au