

THE **CONSENT** TRAP

AUSTRALIAN **FOCUS GROUPS** ON SMARTPHONES, PRIVACY AND CONSENT

CONSENT is at a crossroads. Regulators globally are trying to use it to bolster privacy protections. In the European Union, the General Data Protection Regulation was introduced in 2018, imposing a rigorous standard of informed consent. Since January, the California Consumer Privacy Act has given people the right to opt out of the sale of personal information. And in Australia, the Attorney-General has just announced the terms of reference for privacy law reform, with a clear emphasis on notice-and-consent provisions.

Among academics, however, there is a growing consensus that consent is broken. Researchers consistently find that people do not read or understand privacy policies.

People just tend to agree so they can access services, including email, search engines and social networks. This problem is particularly acute on smartphones, which present unique design challenges and play an increasingly central role in our lives.

We wanted to know what Australians thought about consent, privacy and smartphones. Did they value notice-and-consent or did they think it was broken? The answer turned out to be both.

We held six two-hour focus groups in July 2020, speaking to 26 people in total. Each focus group had three to five participants ranging in age from 19 to 65. Fifteen participants were in

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

Uma, Coffs, 46

Sydney and 11 were in Coffs Harbour. Due to COVID-19, these focus groups were held online, and involved discussions and creative activities.

Our research was informed by a co-design approach, meaning that we didn't just ask our participants what they thought about consent, privacy and smartphones. We also asked them to imagine what informed consent might look like in an ideal world.

Participants said that privacy was very important to them but felt that companies were often trying to trap or trick them. 'Sometimes, to me, consent is more like a trap,' said Maddie from Sydney. With terms and conditions that were long, complicated and hard to read, participants tended to click accept and hope for the best. However, participants were careful to distinguish between sectors. Many felt that the T&Cs presented by the Australian Government on the COVIDSafe app were easier to understand than corporate privacy policies.



Our participants also raised a number of specific concerns. They noted that current models of notice-and-consent are not sensitive to:

- **vulnerable groups**, including children;
- **how people use technology**, including the fact that multiple users may access one device; and
- **the characteristics of smartphones**, which have small screens and unstructured information.

In spite of all this, our core finding was that our participants were optimistic about consent. As Maddie said, 'It's still useful. It's a tool somehow to protect ourselves. If it can be made more simple, that's better. But it's better than nothing.' Participants wanted it to be fixed and thought it could be fixed. They want informed consent to be:

- **SIMPLE**
- **CLEAR**
- **TARGETED**
- **LOGICAL**
- **RELEVANT**
- **REAL-WORLD**
(with concrete examples)
- **EASILY WITHDRAWN**
- **TIME LIMITED** *and*
- **RE-OBTAINED WHEN APPS CHANGE**
(with new features and data uses).

They said written terms could be supplemented by explainer videos. A standardised privacy rating scheme could work like the energy ratings on our appliances. And all privacy policies could open with a three-point summary: how an app works; what data it collects; and how the app benefits from this. Their suggestions were encouraging, and often went beyond consent. Indeed, analysing the findings of our focus groups, we realised participant insights could be distilled into three 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.

Use simplified language with examples

Xavier, Coffs, 50

2 Improve privacy law.

Participants saw the need to bolster consent through standardisation and active regulatory oversight, and to set a baseline of standards.

3 Focus on design.

User interface and user experience designers and developers need to support consent, and to complement the law so that privacy is appropriately protected.

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

The most important parts highlighted

Jade, Sydney, 25

Ultimately, the focus groups revealed there are no easy answers. This is partly because privacy is networked and collective. If I share photos of myself on social media, there are

often people in the background. Even if I choose not to reveal data about myself, sensitive attributes can be inferred. Participants recognised this point, and further recognised that trust is crucial.

For many, the specifics of consent were dwarfed by the simple question of whether or not they trusted app developers, tech companies or the government. What is needed, clearly, is consent that doesn't set traps, but builds trust.

December 2020

Written and researched by:

Sacha Molitorisz

*Postdoctoral research fellow
Centre for Media Transition*



James Meese
*Senior lecturer
RMIT University*



**Centre
for Media
Transition**

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.

For the complete report see cmt.uts.edu.au