Volume **3** (2) 2021 https://doi.org/10.5204/lthj.1874

From Shadow Profiles to Contact Tracing: Qualitative Research into Consent and Privacy

Sacha Molitorisz
University of Technology Sydney, Australia
James Meese
RMIT University, Australia
Jennifer Hagedorn
University of Technology Sydney, Australia

Abstract

For many privacy scholars, consent is on life support, if not dead. In July 2020, we held six focus groups in Australia to test this claim by gauging attitudes to consent and privacy, with a spotlight on smartphones. These focus groups included discussion of four case studies: 'shadow profiles', eavesdropping by companies on smartphone users, non-consensual government surveillance of its citizens and contact tracing apps developed to combat COVID-19. Our participants expressed concerns about these practices and said they valued individual consent and saw it as a key element of privacy protection. However, they saw the limits of individual consent, saying that the law and the design of digital services also have key roles to play. Building on these findings, we argue for a blend of good law, good design and an appreciation that individual consent is still valued and must be fixed rather than discarded - ideally in ways that are also collective. In other words, consent is dead; long live consent.

***Keywords**:* Contact tracing apps; COVIDSafe; privacy; consent; design; shadow profiles.

1. Introduction

In recent years, privacy has emerged as a critical social and policy issue. In 2013, Edward Snowden revealed the widespread surveillance of US citizens by US government agencies. In 2014, Shoshana Zuboff invoked the phrase 'surveillance capitalism' to denote 'an extractive variant of information capitalism',[1] before later arguing that internet companies have been effectively granted 'a license to steal human experience and render it as proprietary data'.[2] And in 2018, the Cambridge Analytica scandal taught us that the misuse of Facebook data had potentially compromised democratic processes in several countries.[3] These developments made it clear that people's data and privacy need better protection for the sake of those individuals and society and democracy.

Then, in early 2020, came the global COVID-19 pandemic. In a matter of weeks, questions of privacy took on a new complexion as governments released technology to collect data about people's movements and interactions in the attempt to stem the spread of COVID-19. This technology was led by contact tracing apps. Alongside the new technology, laws were passed to safeguard privacy, including spelling out what data could be collected, under which conditions, and what sorts of consent were required.[4] Aspects of the privacy debate that had previously seemed esoteric and remote were suddenly playing out at speed, with life and death at stake. In this way, the pandemic, and the technology developed to thwart it, had the effect of crystallising several privacy and data issues and raising the prospect of potential solutions.

[1] Zuboff, "A Digital Declaration."
[2] Zuboff, "The Coup We Are Not Talking About."
[3] Molitorisz, Net Privacy, 61–63.
[4] Ahmed, "A Survey of COVID-19 Contact Tracing Apps."

Against this backdrop, we wanted to revisit the role of informed consent. Specifically, we wanted to ask three questions. First, what is (and what should be) the role and value of individual consent when it comes to our privacy, particularly in a digital context? Second, what is (and what should be) the role of the law? Finally, how can design work together with consent to protect privacy properly?

To answer these questions, we conducted desktop and qualitative research with a particular spotlight on four case studies: shadow profiles, eavesdropping on smartphones, government surveillance and contact tracing technology. Our qualitative research comprised six focus groups held in mid-2020 with a total of 26 Australians.[5] The process helped us understand how people negotiate privacy, particularly on smartphones. The research seeks to contribute to a field often focused on desktop notice-and-consent processes.[6] Our analysis allows us to identify the limits of informed consent, locate suitable spaces for future legal intervention and spell out more clearly the pivotal role that design can play. Our focus groups were held in Australia, but the issues under consideration are global in nature, and we anticipate that our findings will be relevant internationally. Similarly, although our research focused on smartphones, we suggest that our findings and arguments are more widely applicable.

Following this introduction, Section 2 of the paper examines the scholarly literature on informed consent; here, we also sketch out our hypothesis in more detail. In Section 3, we detail the methods and general findings from our six focus groups. In Section 4, we examine four case studies that present specific challenges for consent and privacy: shadow profiles, eavesdropping, government surveillance and contact tracing technology. In Section 5, we synthesise our findings to articulate a possible future for privacy and informed consent, complete with practical and legal recommendations. We end with a brief conclusion.

2. Is There a Future for Informed Consent?

It has become standard practice for privacy scholars to criticise notice and consent, suggesting that maybe consent is dead. These scholars argue that in a digital context citizens can no longer meaningfully understand what they are giving consent to, nor can they control downstream uses of their data.[7] As Daniel Solove writes:

> (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.[8]

The frantic rate of technological change only makes Solove's concerns more pressing. The increasing centrality of automated decision-making systems means that ordinary citizens often do not turn their minds to potential future uses of their data.[9] Their data may be combined with other citizens' data,[10] unknowingly parsed by human analysts[11] and passed on to data brokers, who buy and sell data in the background.[12] These challenges are likely to become more acute as society moves towards an environment of pervasive computing. With people passively engaging with digital technologies, both in their homes and through smart cities, capturing consent meaningfully will become increasingly difficult.[13]

As such, it is hardly surprising that some scholars are calling for notice and consent to be abandoned, or at least significantly downgraded. In an early contribution to the debate in 2009, Solon Barocas and Helen Nissenbaum argued that when it comes to online behavioural advertising, notice and consent is not practicable and does not adequately protect individuals.[14] Further, Julie Cohen argued that 'consent is a liberty-based construct' and that 'effective data protection is first and foremost a matter of design'.[15] Cohen expressed concerns about inequitable power relationships and viewed consent's focus on the individual as 'unilluminating and impracticable in the face of inscrutable, machine learning-driven algorithmic mediation'.[16] Sharing Cohen's concerns about power, Elettra Bietti then undertook a rigorous deconstruction of the more common arguments about

[5] Our research was approved by the UTS Human Research Ethics Committee, project ETH19-4345.
[6] Obar, "The Biggest Lie on the Internet"; Martin, "Transaction Costs, Privacy, and Trust."
[7] Solove, "Introduction"; Sloan, "Beyond Notice and Choice."
[8] Solove, "Introduction," 1888.
[9] Waldman, "Power, Process and Automated Decision-Making."
[10] Cate, "Notice and Consent in a World of Big Data."
[11] Lynskey, "Alexa, Are You Invading My Privacy?"
[12] Larsson, "Algorithmic Governance."
[13] Maple, "Security and Privacy in the Internet of Things."
[14] Barocas, "On Notice."
[15] Cohen, "Turning Privacy Inside Out"; Sloan, "Beyond Notice and Choice."
[16] Cohen, "Turning Privacy Inside Out", 2.

notice and consent to find that 'democratically determined standards and redlines regarding the generation, collection, storage and use of data need our focus more than notice and consent schemes do'.[17]

However, the anti-consent position is not unanimous, with some scholars contending that consent should be retained in some form. One position is that *consent* frameworks are outdated but that the act of providing *notice* is still a critical aspect of preserving privacy.[18] Despite the reservations noted above, Solove believes that 'privacy self-management should not be abandoned', proposing that the process 'is key to facilitating some autonomy'.[19] Even Barocas and Nissenbaum argue that consent is important but that it should play only a supporting role: when it comes to the collection and analysis of large amounts of data, they suggest that 'rights and obligations' are more important;[20] notice and consent would only come into play when individuals are required to waive these rights and obligations, as is standard practice in scientific and medical research.[21] Ryan Calo goes further still, arguing that we have not experimented enough; he thus calls for experiential and personalised notice processes, including in the form of emerging strategies of 'visceral' notice.[22]

Like these scholars, regulators and policymakers are also keen to retain notice and consent. Since coming into effect in 2018, the European Union's General Data Protection Regulation (GDPR) has been the most significant privacy reform of the past decade, with informed consent being one of its key elements. Article 4 prescribes that consent must be 'freely given, specific, informed and [an] unambiguous indication'.[23] Article 7 then prescribes 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'. Article 7 also requires companies to make it just 'as easy to withdraw as to give consent'. Meanwhile, the *Californian Consumer Privacy Act* mandates that people have a 'meaningful understanding' of how their data is used and have the right to opt out of the sale of their personal information.[24] In Australia, notice and consent are also central to the way the law addresses data issues. In October 2020, the Australian Attorney-General's Department released an Issues Paper signalling the start of a major privacy law reform process, in which 23 of the 68 questions raised for comment concerned notice and consent.[25]

Regulators and courts have also been active in policing breaches of consent provisions. In 2019, France's data privacy body, the Commission Nationale de l'Informatique et des Libertés, fined Google €50 million because of a flawed consent process for new Android users. The Commission found that 'essential information ... was excessively disseminated over several documents', opt-outs were not pre-ticked by default and people were asked to give broad consent, all of which contravene the GDPR.[26] More recently, in 2019 and 2020, the Australian competition regulator, the Australian Competition and Consumer Commission (ACCC) launched three legal actions, two against Google and one against Facebook, for allegedly misleading people about the consent given for data collection and processing. One case concerns Google's DoubleClick. In 2016, Google combined data from people using their products with data from their advertising service DoubleClick to provide better advertising services.[27] The ACCC alleges that Google did not obtain valid consent from consumers because 'consumers could not have properly understood the changes Google was making nor how their data would be used, and so did not - and could not - give informed consent'.[28] In another case, the ACCC scored a partial victory in mid-2020 when the Federal Court held that Google had misled Australians in its collection of personal location data.[29] Individuals are litigating too. In early 2021, a class action brought against Facebook in the United States under Illinois's stringent biometric privacy law was finally settled, with Facebook ordered to pay US$650 million for not obtaining the requisite user consent in its use of facial recognition and tagging technology.[30] These developments reveal that governments, regulators and courts are actively working to improve the consent process rather than do away with it.[31] This is in line with privacy scholars keen to retain certain elements of the notice and consent process. In this vein, one of the authors of this paper has contributed by applying a Kantian framework, which begins with a robust conception of individual consent. First, 'if consent is required because a morally significant privacy issue is at

[17] Bietti, "Consent as a Free Pass," 392.
[18] Susser, "Notice After Notice-and-Consent."
[19] Solove, "Introduction," 1899.
[20] Barocas, "Big Data's End Run around Anonymity and Consent," 54.
[21] Barocas, "Big Data's End Run around Anonymity and Consent," 66.
[22] Calo, "Against Notice Skepticism in Privacy (and Elsewhere)."
[23] *General Data Protection Regulation 2016/679* (EU).
[24] O'Connor, "(Un)clear and (In)conspicuous."
[25] Attorney-General's Department, "Privacy Act Review."
[26] Dillet, "French."
[27] Clark, "Google's Ad-Tracking."
[28] ACCC, "Correction"; Zhou, "ACCC Sues."
[29] ACCC, "Google Misled."
[30] Channick, "Nearly 1.6 Million."
[31] Tene, "The Draft EU General Data Protection Regulation."

stake, if there is competence to consent, and if there are no relevant conditions that are ethically required or forbidden, then actual individual consent must be obtained'.[32] This approach places the onus on the data collector to secure appropriate consent, one that keeps in mind people's 'strengths and weaknesses' and ensures that consent is an 'ongoing process'. The proposed approach is, thus, less *caveat emptor*, and more *caveat venditor*.[33] Such a robust conception of individual consent, it is argued, must then be supported and sometimes limited by the law.[34] This proposed approach is compatible with the findings of our focus groups, as described below.

3. Methods and Findings: The Limits and Potential of Individual Consent

a. Methods

To test our hypothesis, we conducted six focus groups in Australia during July 2020.[35] We deployed a 'co-design' method, which is a 'design-led process that uses creative participatory methods'[36] and that differs markedly from the more traditional behavioural or survey-based studies found in the literature.[37] The method allowed us to involve participants 'in the design process, with the idea that this will ultimately lead to improvements and innovation'.[38] In practical terms, it meant that we did not just ask our participants what they thought about consent but also asked them to imagine what consent could look like in an ideal world.

Using local Facebook groups, we recruited 26 participants: 15 from Sydney (metropolitan) and 11 from Coffs Harbour (regional). We then held six two-hour focus groups, each with three to five participants. As far as possible, we deliberately selected participants to ensure a diverse sample. Of our participants, 11 identified as male and 15 as female. The participants' ages ranged from 19 to 65 years. The majority were under 35 years of age, but there were also several middle-aged participants and a small group of retirees. Throughout this report, we use pseudonyms for our participants. As is common in qualitative research, we do not claim that this sample is representative of Australians generally, or even of views in these two cities. Instead, these focus groups allow us to capture opinions and beliefs at a granular level, complementing the wider representative surveys conducted by the Office of the Australian Information Commissioner.

As our research was conducted during the COVID-19 outbreak, we held focus groups on the Zoom video-conferencing platform. Focus groups were divided into discrete thematic sections and semi-directed, with most focus groups consisting of open discussions. At some points, participants were asked to use Google Jamboard (a collaborative software tool) to share perspectives; at other points, participants were asked to respond to smartphone screenshots featuring various examples of notice and consent. This final method allowed us to mimic the standard user flows that people engage with when using smartphones and signing up to apps. To analyse our findings, we conducted an inductive thematic analysis.[39] We collated the data from the Google Jamboard responses into a Microsoft Excel spreadsheet, then clustered and colour-coded comments thematically. Coding the interview transcripts involved a similar approach in which relevant quotes were grouped together to identify themes. In this way, a range of key themes emerged around governance, design and consent. Although not every view presented in the focus groups could be included, the quotes selected for this paper provide a fair representation of the tone and the views that prevailed.

Participants proved to be largely critical of current efforts to protect their privacy. Given that representative surveys have revealed that most Australians consider social media sites and smartphones to pose major privacy risks, this strong agreement across the sample should not come as a surprise.[40] The coherence in responses across participants also meant that we reached saturation with our original recruitment drive.

[32] Molitorisz, Net Privacy, 216. To give an example of 'ethically required', someone's emails may justifiably be read without their consent to save that person's life, or to save the life of others, such as if that person is reasonably suspected of conspiring to murder. To give an example of 'ethically forbidden', some images, such as sexual images of a minor, may not be shared or accessed even with consent.
[33] Molitorisz, Net Privacy, 220–223.
[34] In fact, this approach prescribes a two-tier model of consent, in which individual consent is overarched by the law, which is characterised as 'collective consent'. Molitorisz, Net Privacy, 224–237.
[35] For more on the methods employed, see Molitorisz, The Consent Trap, 6–7.
[36] McKercher, "Beyond Sticky Notes," 15.
[37] See Obar, "The Biggest Lie on the Internet"; McDonald, "The Cost of Reading Privacy Policies"; Martin, "Privacy Notices as Tabula Rasa."
[38] Burkett, "An Introduction to Co-Design," 3.
[39] Charmaz, Constructing Grounded Theory.
[40] Office of the Australian Information Commissioner, "2020 Australian Community Attitudes to Privacy Survey."

b. General Findings

Considering the anti-consent literature cited in the previous section, it was somewhat surprising that many participants tried seriously to engage with the informed consent process. Many participants said they genuinely considered the relevance of requests for data. This often meant making a quick calculation about whether the request was in line with the stated purpose of the service or app. As Felicity (Sydney, 34) explained:

> It depends what the app is and why they need it [the data]. 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 viewed this as a logical data request, and most of our participants were happy to allow this sort of transactional data exchange. They were also happy to reject requests from inequitable or illogical exchanges. As Iris (Sydney, 45) said, 'unless it's relevant, it's a big fat "no" from me'.

While we know that people mostly do not read terms and conditions, researchers are only just starting to account for smartphones in their analyses.[41] This is significant as these devices have a range of different affordances, from smaller screens to more pop-ups, that affect the consent process. 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. Overwhelmingly and unsurprisingly, people agreed that notice and consent was, in practice, a failing model. Sally (Coffs Harbour, 36) complained that despite some improvements, the 'permissions [were] too much', and the fact that 'they need permission for everything' annoyed her.

Crucially, however, our participants did not think that informed consent was unfixable. They even offered iterative solutions. They wanted companies to be clearer about how their data was being used and said that more was needed than a standard contract. For example, Maddie (Sydney, 35–40) said that videos, graphs and pictures were 'more catchy, and you [the user] want to focus on that'. Our participants recognised the complexity of the current data economy but still wanted to be part of the conversation about solutions.

To this end, participants also explored potential *design* solutions. One group of solutions focused on ensuring that people actually read the terms and conditions. Many participants noted that sign up screens often do not force you to look at the terms and conditions before signing up. Suggested options included having to type in an answer or tracking whether or not people had opened the terms and conditions (Rosie, Coffs Harbour, 42), requiring people to 'tick a box' (Uma, Coffs Harbour, 46) or making people 'scroll through a summary' of terms and conditions before accepting them (Vincent, Coffs Harbour, 19). Another group of solutions suggested moving towards granular or personalised consent. One suggestion was that people should be able to use some of the elements of an app if they agree to certain aspects of the terms and conditions (Felicity, Sydney, 34). Indeed, several participants were concerned about the 'all or nothing' approach to most terms and conditions and suggested that people should have more options. As Beth (Sydney, 47) said, 'an option to withdraw it or change the conditions would be useful'. Other participants said that it was hard to agree to terms about the use of a service when they had not used it before. They suggested a preliminary period where people could have 'the option to use once' (Ellie, Sydney, 19). This 'try before you buy' consent model would potentially give people a better sense of the value they might get out of an app before committing to signing up.

Of course, our participants also recognised that there were genuine limitations to the individual consent process. There was a clear sense that while consent should be retained at certain points, *the law* needed to step in. People wanted more assistance from the government and regulators so they could take more responsibility for their privacy. Participants were particularly focused on transparency and wanted to know more about the companies collecting their data. However, there was also a clear expectation that the government and regulators would step in at critical points to protect citizens. Our participants did not come to a consensus about the precise role of citizens vis-a-vis governments but it was clear to our participants that, in many cases, consent had 'to be policy-based rather than individual-based' (Rosie, Coffs Harbour, 42) and 'more of a legislative thing rather than an individual thing' (Sally, Coffs Harbor, 36).

[41] Obar, "The Biggest Lie on the Internet."

4. Case Studies: Specific Challenges for Individual Consent

a. Shadow Profiles

In our desktop research and focus groups, we concentrated on four case studies that present particular challenges for issues of consent and privacy. One of these is the 'shadow profile', by which we mean digital platforms building profiles of individuals who do not use that platform. Research shows that shadow profiles are possible.[42] In a 2019 paper, James P. Bagrow et al. used 'information-theoretic estimators to study information and information flow' on Twitter to show that '95% of the potential predictive accuracy for an individual is achievable using their social ties only, without requiring that individual's data'.[43] Working with a dataset of nearly 14,000 users, the researchers found that 8–9 of an individual's contacts will be enough to reveal that individual, without that individual needing to share anything at all. This is largely due to the phenomenon of 'homophily', describing how people tend to socialise with like-minded others. The researchers concluded that 'information is so strongly embedded in a social network that in principle one can profile an individual from their available social ties even when the individual forgoes the platform completely'.[44] Other studies have reached the same conclusion.[45]

Do companies such as Facebook actually build profiles of non-users? The answer is not clear. In US Congressional hearings in 2018 following the Cambridge Analytica scandal, Facebook's Mark Zuckerberg was pressed on the issue. He denied knowledge of 'shadow profiles', saying, 'I'm not familiar with that', but admitted that Facebook collects some data on non-users so that it can keep its users safe.[46] While researchers have repeatedly demonstrated that shadow profiles are possible and journalists have shed some light on the practice, the extent of the practice is hard to gauge.[47]

To raise the issue of shadow profiles in our focus groups, we asked the participants to imagine five imaginary friends, four of whom are on a social network. The fifth, by contrast, does not want a social media presence. However, that fifth person can still be revealed thanks to the homophily described above, as well as other means. When presented with this scenario, most participants objected strongly, using words such as 'unacceptable', 'abhorrent', 'unethical' and 'illegal'. 'That would be like me spying on my neighbour and keeping a diary and photos of them', said Rosie (Coffs Harbour, 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'. Wendy (Coffs Harbour, 19) said that people's choice not to use a service should be respected: 'If you haven't got that social media, it's obviously for a reason. You don't trust it or something'. However, one participant felt resigned. Karl (Sydney, 62) said:

> I think we have come into that era now. Digital marketing, digital profiling, these things are happening, and we have to move with the world. We cannot go back 20, 30 years and get the sales journal, purchases journal, ledgers—those things are gone. We have to move with the time. It is reality. You have to suck it up, whether you like it or not. You just have to live in this world.

Karl was alone in saying people needed to accept the practice. However, a number of others did point out that the practice would be very hard to eliminate. As Yves (Coffs Harbour, 52) said:

> Obviously, it's unethical. But in this day and age of everyone having a camera in their pocket, 24/7, and by a majority of people using one social network or another, as unethical and abhorrent as it may seem, to put in place rules and laws to force those companies to not store that information, is a big job.

Implicit in Yves's response is that 'rules and laws' do have a job to perform here, even if it is 'a big job'.

b. Eavesdropping

Another major challenge for informed consent concerns tech companies listening in—or 'eavesdropping'—on people's conversations. Anecdotal evidence of such practices is widespread.[48] As with shadow profiles, the available literature has revealed that eavesdropping is technically possible. One 2020 paper focused on eavesdropping by accelerometers, the sensors in a smartphone that measure how that phone is vibrating or changing in motion. The researchers did not show that

[42] Sarigol, "Online Privacy as a Collective Phenomenon"; Garcia, "Leaking Privacy and Shadow Profiles in Online Social Networks."
[43] Bagrow, "Information Flow Reveals Prediction Limits in Online Social Activity."
[44] Bagrow, "Information Flow Reveals Prediction Limits in Online Social Activity."
[45] Garcia, "Privacy Beyond the Individual"; Garcia, "Collective Aspects of Privacy in the Twitter Social Network."
[46] Molitorisz, Net Privacy, 53–55.
[47] Hill, "How Facebook."
[48] BBC News, "Is Your Phone?"

accelerometers *do* eavesdrop, but that they *can*, by demonstrating that accelerometers can capture the audio of adult speech.[49] Much of the literature concerns security risks, such as the risk of hacking and malware attacks by third parties, rather than the inadequacy of consent/permissions, or to what extent such eavesdropping does, in fact, occur.

Several digital platforms have admitted to some form of eavesdropping. In 2019, Facebook admitted paying contractors to transcribe audio clips from users of its services;[50] also in 2019, Google, Apple and Amazon all admitted to winding back their practice of having people analyse recordings captured by voice assistants following adverse reports.[51] That same year, one academic study concluded that 'we cannot rule out the possibility of sophisticated large-scale eavesdropping attacks being successful and remaining undetected'.[52]

In our focus groups, many participants were deeply concerned that their digital devices were listening in without consent. Iris (Sydney, 45) said she was:

> ... disturbed about Google hearing everything that we say and listening to our phones. I was with a group of friends a couple of weeks ago, and we were talking about placement of ads. And we talked about BMW, and then a couple of days later, one of the women said, "Oh look, BMW popped up on Facebook on my phone." Even if your phone's not in use, if you've got the Hey Google activated, it's basically listening to you, which is a little disturbing to me. That's definitely not consensual.

Felicity (Sydney, 34) agreed:

> It's disturbing. 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. It's inappropriate, unethical, and it's also scary.

c. Government Surveillance

The past decade has also revealed that some governments are engaged in widespread non-consensual surveillance of their citizens. In the United States, extensive practices of domestic surveillance by the National Security Agency (NSA) and other agencies were exposed by Edward Snowden in 2013.[53] Some of these practices were subsequently declared unconstitutional or illegal.[54] In other countries, there have been no analogous whistle-blowers, so less is known about whether such practices occur. Government surveillance can take different forms. On the one hand, a surveillance technique can be surreptitious, widespread and unauthorised by law, as was the case with some of the NSA's practices. On the other hand, a surveillance technique can be known, targeted and authorised by law. In our focus groups, we did not try to pinpoint exactly which practices the participants found unacceptable; rather, we initiated open-ended discussions to gauge our participants' general responses.

Several participants said that sometimes the government would be justified in non-consensually accessing photos, emails or other personal data, as in cases of national security, but that such access would only be justified with a warrant and only in extreme circumstances. As Sally (Coffs Harbour, 36) said, 'If they have a warrant, if they've gone through the legal channels and there's evidence that says I might be about to blow something up …. They need to do it in that way'. This prompted several replies:

> *Rosie* (Coffs Harbour, 42): You'd have to be planning something pretty horrendous.
>
> *Patrick* (Coffs Harbour, 54): If it was national security, I'd be okay with it.
>
> *Sally* (Coffs Harbour, 36): If it was just trying to find out who votes left or right or whatever, then I would have a problem with that.

Uma (Coffs Harbour, 46) said that it's a fine line. If a government accesses a person's email, they might find that the person has been doing paid work but not declaring it for income tax purposes. However, they might also find that the person has been having an affair. As Uma said, 'That's none of the government's business.' Beth (Sydney, 47) noted that if the government can non-consensually access information about you, then it could use that information maliciously without you ever knowing. This would mean that you have no ability to appeal: 'You've lost opportunities or you're suffering some sort of penalty, without any

[49] Ba, "Accelerometer-Based Smartphone Eavesdropping."
[50] Frier, "Facebook Paid."
[51] Metz, "Yes, Tech."
[52] Kröger, "Is My Phone Listening In?"
[53] Schneier, Data and Goliath.
[54] Reuters, "NSA Surveillance."

knowledge about it, or your children are, because of what you've done, or what they perceive you've done. That's a police state. It's really wrong'.

Some participants were fatalistic about non-consensual government surveillance. 'I think we don't really have a choice when we talk about a government agency,' said Karl (Sydney, 62). 'Regardless if we like it or not, they still have our data. So, I cannot really comment if it's fair or not, because I think there's no choice at all.' However, most participants were adamant that governments should not be able to surreptitiously access all our correspondence and data. As Xavier (Coffs Harbour, 50) said, 'There are countries in this world that do operate that way. We don't want to be ... *I* don't want to be there'.

d. Contact Tracing Technology

The issue of government surveillance was suddenly cast in a fresh light following the outbreak of COVID-19, which was declared a global health emergency by the World Health Organization in January 2020.[55] To combat the global pandemic, many governments released contact tracing apps.[56] While contact tracing has traditionally been conducted by interviewing infectious people about their contacts and movements, contact tracing apps automate the process, relying on Bluetooth and other technology to collect personal data. In a sense, the boundaries of individual privacy are being redrawn in the interests of public health, with people being asked to make 'trade-offs' by relinquishing some privacy to save lives.[57] In countries including Australia, these apps are supported by legislation that attempts to minimise the risk of privacy harms.

Internationally, governments have adopted a variety of contact tracing technologies, which 'are generally not mandatory and work on an opt-in basis'.[58] To this end, they tend to rely on notice and consent. However, researchers have also found that the consent mechanisms are imperfect. One study analysed factors such as the word count and word complexity of seven contact tracing apps to find that their privacy policies required a reading ability considerably higher than that of the average adult.[59] In July 2020, a comprehensive review of contract tracing apps and their attributes specifically identified the difficulty of 'consent withdrawal' as a concern for app users; it also found that app adoption rates increase significantly with greater transparency and legislative guarantees against data misuse.[60] One specific concern among researchers involves the role played by private companies in these apps, which can increase the risk of illegal data collection and sharing.[61] An attendant privacy issue concerns whether data is stored on a centralised database, or in a decentralised manner.[62] Several scholars have also expressed concern about the normalisation of this type of surveillance.[63]

In Australia, the Federal Government launched the COVIDSafe contact tracing app in April 2020. It was based on Singapore's TraceTogether app, which relies on Bluetooth technology, Amazon Web Services and a centralised server.[64] In May, Australia's *Privacy Act* was amended specifically to protect data collected by the app (see discussion below).[65] In our focus groups, more than half the participants had not downloaded the app because they had concerns about the app's privacy or efficacy. However, for Beth (Sydney, 47) public health trumped privacy concerns in this case:

> I downloaded it. And I actually bought my son a phone so he could download it because he was catching public transport at the time. But there's no need to excessively give away my data so once, hopefully, the plague is over, I will delete it. And I'll get my son to delete it as well. For me, and for society, it's better that we opt in … this global pandemic is the real big concern here, so we just put privacy aside.

Zara (Coffs Harbour, 29) had not downloaded it:

> I live in a very small town. I'm very much a home body. But ... I don't want the government knowing my every move. I don't want them knowing everyone I'm in contact with. I don't want the government intimately melding into my life that much. No thank you. Not today.

[55] Ahmed, "A Survey of COVID-19 Contact Tracing Apps."
[56] Ahmed, "A Survey of COVID-19 Contact Tracing Apps."
[57] Cho, "Contact Tracing Mobile Apps for COVID-19."
[58] Abbas, "COVID-19 Contact Trace App Deployments."
[59] Zhang, "COVID-19 Contact-Tracing Apps."
[60] Ahmed, "A Survey of COVID-19 Contact Tracing Apps."
[61] Guinchard, "Our Digital Footprint Under Covid-19."
[62] Stevens, "TraceTogether."
[63] Couch, "COVID-19: Extending Surveillance and the Panopticon"; Goggin, "COVID-19 Apps in Singapore and Australia."
[64] Goggin, "COVID-19 Apps in Singapore and Australia."
[65] Goggin, "COVID-19 Apps in Singapore and Australia."

When we walked participants through the consent process by showing them smartphone screenshots, they were generally positive. Overall, despite some reservations along the lines of those detailed above, our participants viewed the Australian app as an improvement on corporate terms and conditions. This was because participants felt they had a choice about whether to participate or not and were being presented with a relatively comprehensive and comprehensible consent process. And they were pleased that associated legislative provisions had been passed to protect their personal data. One issue of concern, however, was that even those who had downloaded the app had limited knowledge of key information, including the existence of the legislation and the fact that Amazon Web Services were providing the infrastructure for the app.

5. Discussion: A Tripartite Response

The participants in our focus groups confirmed what the academic literature reveals: there is an intractable problem when it comes to consent and data. In addition, the case studies discussed in this article show that there are clearly situations where the process of notice and consent is particularly fraught. However, just like our focus group participants, we think there is scope to improve the mechanism of notice and consent. Indeed, we propose that consent remains core to the protection of privacy but needs to be construed in fresh terms. Current approaches focus on the individual. Given the relational and collective nature of our data and, indeed, our lives, a better approach recognises that individual consent often requires the support of good design and good law. This is the model that emerged most clearly from our consideration of contract tracing apps, which sought to balance individual consent with legal protections and clear design. We will first clarify the role of law and design, before returning finally to the role of consent.

a. The Law

As our research shows, there are clear instances where individual consent is inadequate and legal protections are needed. This is most obvious with shadow profiles and eavesdropping. Both practices are ethically suspect: it is hard to imagine a clearer failure of individual consent than shadow profiles; and if people have, in fact, consented to eavesdropping, they have done so unwittingly. Our participants were outraged by the practices. They wanted the law to protect their privacy more effectively, and here are two prime examples. Privacy laws ought to rigorously restrict, if not outlaw, shadow profiles and eavesdropping, as there is no meaningful way for people to consent to these experiences, even if companies attempt to provide notice. This is clearly what most of our focus group participants wanted. Similarly, participants had strong views around the circumstances in which government surveillance of its citizens is acceptable and unacceptable.[66]

One key point here is that good law must be accompanied by effective enforcement. There is certainly scope to enforce existing laws more vigilantly. As noted above, Australia's competition watchdog (the ACCC) has launched three lawsuits (and at the time of writing has scored one victory) in a 'world-first enforcement action' against Google and Facebook for the alleged non-consensual collection of data under longstanding prohibitions on misleading and deceptive conduct,[67] while in early 2021, in the United States, a judgment was finalised in a class action under the biometric privacy law of Illinois, with Facebook ordered to pay US$650 million for its non-consensual use of facial recognition and tagging technology.[68] Meanwhile, in Norway in 2021, Grindr was fined an estimated 10% of its global revenue for not 'gaining a valid consent' from users to sell data to advertisers.[69] For the law to do its job, good legislation must be accompanied by effective enforcement.

We do not view this reliance on law as a move away from consent. We regard law as a space where societies can address issues that extend beyond the individual to establish collectively agreed boundaries through democratic mechanisms. The law is, to quote Immanuel Kant, an expression of the 'united will of the people'.[70] It is the law that draws the line on behalf of individuals, particularly in cases where the individual is powerless to draw the line themselves. Often the united will of the law works to support individual consent, as is evident in the cases we have just described. It is also evident in the GDPR, which stipulates (in Article 4) that individuals must *actively* consent to the sharing of their data, thereby ensuring that a pre-ticked opt out box will be legally insufficient. (This leads to the larger point that the default position for users ought to be *for* privacy, not for sharing.) Further, the right to erasure contained in the GDPR (Article 17) enables people to request that, for instance, specific links be removed from results returned by a search engine in certain circumscribed conditions. Meanwhile, facial recognition software has been banned in various jurisdictions, including San Francisco, given the inaccuracy and inequity of the technology but also the way it can be used for unforeseen and non-consensual purposes.[71] We support each of these provisions (among others) and hope they are more widely adopted.

[66] See Molitorisz, Net Privacy, 229–236.
[67] ACCC, "Google Misled"; ACCC, "Correction."
[68] Channick, "Nearly 1.6 Million."
[69] BBC News, "Grindr."
[70] See Molitorisz, Net Privacy, 226–229.
[71] Conger, "San Francisco."

The key role of law becomes yet more apparent when we recognise the collective nature of privacy. As researchers are increasingly demonstrating, privacy transcends the individual.[72] This is particularly evident with developments such as shadow profiles: as detailed above, a social network can build a profile of a person who never uses that network simply by accessing information from other sources (including offline sources) and by inferring information about someone. This prompted researchers to coin the phrase 'privacy leak factor',[73] and led others to begin to conceptualise the notions of 'collective privacy', 'networked privacy' and 'relational privacy'.[74] The issue of inferred data sits right at the heart of notions of collective/networked/relational privacy and is one of the most vexing issues confronting data regulators. When should inferred data count as personal data? What sort of protections should it attract? When should it be outlawed?[75] It is beyond the scope of this paper to address these questions. However, we propose that the best hope for a just response to the challenges of collective privacy generally and inferred data more specifically is likely to emerge in the shape of good law.

Fundamentally, the law can address problems with informed consent; it can specify when individual consent is required, detail what elements are needed for individual consent to be legally valid and provide top-down regulations when individual consent cannot do the work. The GDPR provides a good template. Admittedly, its implementation has not been perfect, with website operators often following the letter rather than the spirit of the law. As Bornschein et al. note, 'Most cookie notices are hardly visible and/or do not offer consumers a choice regarding information collection practices'.[76] This view supports our point that law and regulation can only be effective with effective enforcement.

b. The Supporting Role of Design

Consent must be understood as more than just the written terms of agreement. It also encompasses people's experience. In other words, we need to ask: How are these terms being presented to individuals? How are consent mechanisms being *designed*?

In our focus groups, participants noted many instances where design fell short, including limited/persuasive buttons or menu options, small typefaces, simplistic text and a lack of consistency in presentation across apps and platforms, all of which led participants to feel a lack of control when consenting.[77] Our participants consistently wanted simplicity and clarity in design. Natasha (Sydney, 30) said that 'being able to explain complex things in simple terms is an art form', adding that 'it's doable, and if you can't do it then find someone who can'. Olive (Sydney, 25) previously worked in the health sector, where her professional experience with informed consent 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 with the tech sector. She reiterated a powerful point made by several participants: tech companies could make consent work if they wanted to.

When options are not presented clearly and dispassionately, the risk of manipulation or deception is high.[78] Manipulative design choices are called 'dark patterns', a term coined by user experience (UX) and user interface (UI) practitioner Harry Brignull, who compiled a list of established design patterns and user behaviours that are employed within an interface design to manipulate or deceive users into agreeing to particular terms and conditions.[79] Subsequently, Colin M. Gray et al. developed a comprehensive framework to articulate the various UX patterns that can be deployed to persuade users to engage in specific behaviours; these patterns include 'nagging', 'obstruction', 'sneaking', 'interface interference' and 'forced action'.[80] Representing a subversion of user-centred design principles, these techniques see designers use knowledge about users (and society more broadly) against them.[81] While these techniques are not necessarily intended to be 'dark', they 'have the potential to produce poor user outcomes, or force users to interact in ways that are out of alignment with their goals'.[82]

[72] Sarigol, "Online Privacy as a Collective Phenomenon"; Bannerman, "Relational Privacy and the Networked Governance of the Self"; Molitorisz, Net Privacy.
[73] Sarigol, "Online Privacy as a Collective Phenomenon."
[74] Sarigol, "Online Privacy as a Collective Phenomenon"; Garcia, "Privacy Beyond the Individual"; Marwick, "Networked Privacy"; Bannerman, "Relational Privacy and the Networked Governance of the Self"; Molitorisz, Net Privacy.
[75] E.g., see Attorney-General's Department, "Privacy Act Review."
[76] Bornschein, "Effect of Consumers' Perceived Power."
[77] See Molitorisz, The Consent Trap, 17–18.
[78] Forbruker Radet, "Deceived by Design."
[79] Brignull, "Dark Patterns."
[80] Gray, "The Dark (Patterns) Side of UX Design."
[81] Gray, "The Dark (Patterns) Side of UX Design."
[82] Gray, "The Dark (Patterns) Side of UX Design."

In the absence of adequate regulatory standards, UX and UI designers lack appropriate guidance on best practice when it comes to informed consent. Recent research by Cherie Lacey et al. exploring the privacy decision-making processes of designers revealed that design choices involving privacy were often 'like the Wild West':[83]

> (1) designers feel motivated to act ethically due to their 'moral compasses'; (2) designers are restricted in their ability to act ethically due to commercial pressures and a limited purview of the project; (3) designers' understanding of the ethics of their practice do not currently match determinations made by international privacy and design scholars and demonstrate a limited understanding of how user behavior can be shaped that, in turn, obfuscates beneficial privacy outcomes for users.[84]

As awareness of these issues grows, the 'privacy by design' movement is gaining momentum.[85] This involves the recognition that the due protection of privacy involves coding it into the very architecture of digital services and platforms. Rather than a mere afterthought or add-on, privacy must be embedded in software and hardware design. One innovation here is Google's Federated Learning of Cohorts, which aims to replace data tracking by cookies with a system that is less privacy invasive.[86]

Design and law can work together, as they do in the GDPR's prescription for 'privacy by design and by default'.[87] Overall, stronger collaboration between the design community and lawmakers is required so that UX and UI design standards implement and mandate privacy by design strategies, including by prioritising consent at the development stage, rather than on an ad-hoc basis or retrospectively. Here, considerable work has already been done. The World Wide Web Consortium (W3C) develops design and accessibility standards for the web and fosters the development of privacy by design for web standards.[88] This shows how design, law and consent can complement one another. To give users more autonomy and agency around consent, designers need to develop experiential and personalised notice processes that build in ongoing opportunities for users to confirm or retract consent. This, in turn, needs to be combined with good law and robust enforcement provisions, to ensure that these standards are maintained and upheld.

c. Fixing Individual Consent

The participants in our focus groups tried hard to make careful judgments about their data. For instance, they were unlikely to accept consent requests that were seen as irrelevant for the service they were seeking to access. Clearly, people still highly value individual consent, even as they recognise that consent mechanisms often fail them. What's more, companies and governments seem to be working on the assumption that individual consent can be fixed. In response to Apple's plans to introduce a notification asking iOS users whether or not they want to be tracked by apps, Facebook objected that this would lose them revenue from personalised advertising.[89] Facebook's fears were seemingly based on a presumption that millions of people would choose privacy; Facebook's concern, in other words, was that Apple was giving people *the genuine opportunity to withhold consent*. In 2020, consent also played a central role in the development of Australia's contact tracing app. In April, the COVIDSafe app was launched; in May, the *Privacy Act* was amended specifically to protect the data it collected, including by creating a series of serious offences for unauthorised access, use or disclosure of data collected.[90] The consent mechanisms, and the law underpinning them, were not perfect.[91] However, privacy experts had reason to be positive about protections contained in the legislation,[92] just as our participants were positive about the app's design. Let's hope this interplay of consent, law and design is a portent of things to come.

Yes, there are serious limits to the efficacy of individual consent. Many of these stem from its focus on the individual. The complexity of online data flows means that no individual can hope to monitor all relevant data, let alone the inferences that might be drawn from that data. Indeed, emerging work in law and philosophy has challenged the normative basis upon which individual approaches to data governance are founded, arguing that this basis is no longer viable in a world where data is increasingly used as an economic resource.[93] The advent of machine learning and algorithmic governance only increases the challenges facing consent, with emerging harms from predictive decision-making likely to be not only significant but inequitably distributed.[94] In response, scholars have proposed novel solutions that include collective data governance

[83] Lacey, "It's Like the Wild West."
[84] Lacey, "It's Like the Wild West."
[85] Molitorisz, Net Privacy, 281–286.
[86] Fischer, "Google Says."
[87] *General Data Protection Regulation 2016/679*, Art. 25.
[88] W3C, Report from W3C Workshop on Permissions and User Consent.
[89] Peters, "Apple Defends."
[90] Goggin, "COVID-19 Apps in Singapore and Australia"; Greenleaf, "Australia's COVIDSafe Experiment, Phase III."
[91] Greenleaf, "Australia's COVIDSafe Experiment, Phase III."
[92] E.g., see Crompton, "COVIDSafe."
[93] Viljoen, "Democratic Data."
[94] Viljoen, "Democratic Data."

mechanisms, such as data trusts and data cooperatives, which allow large groups of persons to have their interests represented by an intermediary body.[95] This line of thinking is encouraging: perhaps in time consent can be re-imagined and implemented in a way that is less individualistic and more collective, and at the same more effective. We hope so. For now, at least, individual consent has a key role to play. And that's unequivocally what our participants want. Despite its limitations, consent needs fixing, not discarding.

6. Conclusion

Our focus groups showed that people value consent but also recognise that major work is needed to improve the process in practice. As focus group participant Maddie (Sydney, 35–40) said, 'Consent is a trap … but 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 better than nothing'. The limitations of consent became particularly apparent from our discussion of shadow profiles, eavesdropping and government surveillance, which confirmed systemic problems around data collection and processing. In response, the academic literature has proposed innovative solutions such as the articulation of forms of consent that are less individualistic and more collective (e.g., data trusts). We encourage these developments. More immediately, however, there is a pressing need to fix individual consent, where considerable scope for improvement and innovation exists. And there is a complementary and similarly pressing need to recognise and improve the role played by law and the role played by design. With law, for instance, one oft-overlooked focus is enforcement. Recent activity in multiple jurisdictions has shown that existing laws can be applied to protect privacy (often by policing consent), as long as there is regulatory capacity and an appetite to take on offending parties. Our approach thus combines three elements: the key prescriptions set by the law; the supporting role of design; and the core component of individual consent. Each of these elements demands attention if our consent is to protect us and not entrap us.

[95] Micheli, "Emerging Models of Data Governance."

Bibliography

Abbas, Roba and Katina Michael. "COVID-19 Contact Trace App Deployments: Learnings from Australia and Singapore." *IEEE Consumer Electronics Magazine* 9, no 5 (2020): 65–70. https://doi:10.1109/MCE.2020.3002490

Ahmed, Nadeem, Regio A. Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke and Sanjay K. Jha. "A Survey of COVID-19 Contact Tracing Apps." *IEEE Access* 8 (2020): 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226

Attorney-General's Department. *Privacy Act Review: Issues Paper*. (Attorney-General's Department, October 2020). https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

Australian Competition and Consumer Commission (ACCC). "Correction: ACCC Alleges Google Misled Consumers about Expanded Use of Personal Data." Last modified July 27, 2020. https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data

Australian Competition and Consumer Commission (ACCC). "Google Misled Consumers about the Collection and Use of Location Data." April 16, 2021. https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data

Ba, Zhongjie, Tianhang Zheng, Zhan Qin, Hanlin Yu, Liu Liu, Baochun Li, Xue Liu and Kui Ren. "Accelerometer-Based Smartphone Eavesdropping." In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. New York, NY: Association for Computing Machinery, 2020.

Bagrow, James P., Xipei Liu and Lewis Mitchell. "Information Flow Reveals Prediction Limits in Online Social Activity." *Nature Human Behaviour* 3, no 2 (2019): 122–128. https://doi.org/10.1038/s41562-018-0510-5

Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UC Davis Law Review* 49 (2015): 1183–1234.

Bannerman, Sara. "Relational Privacy and the Networked Governance of the Self." *Information, Communication & Society* 22, no 14 (2019): 2187–2202. https://doi.org/10.1080/1369118X.2018.1478982

Barocas, Solon and Helen Nissenbaum. "On Notice: The Trouble with Notice and Consent." In *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, 2009.

Barocas, Solon and Helen Nissenbaum. "Big Data's End Run around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender and Helen Nissenbaum, 44–75. Cambridge: Cambridge University Press, 2014.

BBC News. "Is Your Phone Listening In? Your Stories." *BBC*. October 30, 2017, https://www.bbc.com/news/technology-41802282

BBC News. "Grindr Faces £8.5m Fine for Selling User Data." *BBC*. January 26, 2020, https://www.bbc.com/news/technology-55811681

Bietti, Elettra. "Consent as a Free Pass: Platform Power and the Limits of the Informational Turn." *Pace Law Review* 40 (2019): 310–398.

Bornschein, Rico, Lennard Schmidt and Erik Maier. "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices." *Journal of Public Policy & Marketing* 39, no 2 (2020): 135–154. https://doi.org/10.1177/0743915620902143

Brignull, Harry. *Dark Patterns* (website), 2019. https://darkpatterns.org/

Burkett, Ingrid. *An Introduction to Co-Design*. https://www.yacwa.org.au/wp-content/uploads/2016/09/An-Introduction-to-Co-Design-by-Ingrid-Burkett.pdf

Calo, M. Ryan. "Against Notice Skepticism in Privacy (and Elsewhere)." *Notre Dame Law Review* 87 (2011): 1027–1072.

Cate, Fred H. and Viktor Mayer-Schönberger. "Notice and Consent in a World of Big Data." *International Data Privacy Law* 3, no 2 (2013): 67–73. https://doi.org/10.1093/idpl/ipt005

Channick, Robert. "Nearly 1.6 million Illinois Facebook Users to Get about $350 each in Privacy Settlement." *Chicago Tribune*, January 14, 2021. https://www.chicagotribune.com/business/ct-biz-facebook-privacy-settlement-illinois-20210115-2gau5ijyjff4xd2wfiiow7yl4m-story.html

Charmaz, Kathy. *Constructing Grounded Theory* (2nd ed.). London: Sage Publications, 2014.

Cho, Hyunghoon, Daphne Ippolito and Yun William Yu. "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs." *arXiv preprint arXiv:2003.11511* (2020).

Clark, Liat. "Google's Ad-Tracking Just Got More Intrusive. Here's How to Opt Out." *Wired*. October 24, 2016. https://www.wired.co.uk/article/google-ad-tracking

Cohen, Julie E. "Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20, no 1 (2019): 1–31.

Conger, Kate, Richard Fausset and Serge F. Kovaleski. "San Francisco Bans Facial Recognition Technology." *New York Times*, May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Couch, Danielle L., Priscilla Robinson and Paul A. Komesaroff. "COVID-19: Extending Surveillance and the Panopticon." *Journal of Bioethical Inquiry* 17, no 4 (2020): 809–814. https://doi.org/10.1007/s11673-020-10036-5

Crompton, Malcolm and Chong Shao. "COVIDSafe: A Turning Point for Privacy?" *Information Integrity Solutions* (blog). April 30, 2020. https://www.iispartners.com/blog/2020/4/29/covidsafe-a-turning-point-for-privacy
Delacroix, Sylvie and Neil D. Lawrence. "Bottom-up data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law* 9, no 4 (2019): 236–252. https://doi.org/10.1093/idpl/ipz014
Dillet, Romain. "French Data Protection Watchdog Fines Google $57 Million Under the GDPR." *Tech Crunch*, January 22, 2019. https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/
European Union. *General Data Protection Regulation 2016/679*. May 25, 2018. https://gdpr-info.eu/
Fischer, Sara. "Google Says it May Have Found a Privacy-Friendly Substitute to Cookies." *Axios*, January 25, 2021. https://www.axios.com/google-privacy-friendly-substitute-cookies-test-05c2c28e-77f1-4921-9a99-1ef0c009b064.html
Forbruker Radet. "Deceived by Design." June 27, 2018. https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
Frier, Sarah. "Facebook Paid Contractors to Transcribe Users' Audio Chats." *Bloomberg*, August 14, 2019. www.bloomberg.com/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio
Garcia, David. "Leaking Privacy and Shadow Profiles in Online Social Networks." *Science Advances* 3, no 8 (2017): e1701172. https://doi.org/10.1126/sciadv.1701172
Garcia, David. "Privacy Beyond the Individual." *Nature Human Behaviour* 3, no 2 (2019): 112–113. https://doi.org/10.1038/s41562-018-0513-2
Garcia, David, Mansi Goel, Amod Kant Agrawal and Ponnurangam Kumaraguru. "Collective Aspects of Privacy in the Twitter Social Network." *EPJ Data Science* 7 (2018): 1–13. https://doi.org/10.1140/epjds/s13688-018-0130-3
Giannopoulou, Alexandra. "Algorithmic Systems: The Consent is in the Detail?" *Internet Policy Review* 9, no 1 (2020). https://doi.org/10.14763/2020.1.1452
Goggin, Gerard. "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology." *Media International Australia* 177, no 1 (2020): 61–75. https://doi.org/10.1177/1329878X20949770
Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt and Austin L. Toombs. "The Dark (Patterns) Side of UX Design." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. New York, NY: Association for Computing Machinery, 2018
Greenleaf, Graham and Katharine Kemp, "Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing." 2020. https://ssrn.com/abstract=3601730
Guinchard, Audrey. "Our Digital Footprint Under Covid-19: Should We Fear the UK Digital Contact Tracing App?" *International Review of Law, Computers & Technology* 35, no 1 (2020): 84–97. https://doi.org/10.1080/13600869.2020.1794569
Hill, Kashmir. "How Facebook Figures Out Everyone You've Ever Met." *Gizmodo*. November 11, 2017. https://www.gizmodo.com.au/2017/11/how-facebook-figures-out-everyone-youve-ever-met/
Kröger, Jacob Leon and Phillip Raschke. "Is My Phone Listening In? On the Feasibility and Detectability of Mobile Eavesdropping." In *Data and Applications Security and Privacy XXXIII*, Lecture Notes in Computer Science, edited by Simon N. Foley, vol. 11559, 102–120. Cham: Springer International Publishing, 2019.
Lacey, Cherie, Alex Beattie and Catherine Caudwell. "'It's Like the Wild West': User Experience (UX) Designers on Ethics and Privacy in Aotearoa New Zealand." 2020. https://informedby.files.wordpress.com/2020/09/privacy-dark-patterns-with-authors.pdf
Larsson, Stefan. "Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets." *Internet Policy Review* 7, no 2 (2018): 1–13. https://doi.org/10.14763/2018.2.791
Lynskey, Dorian. "'Alexa, Are You Invading My Privacy?' – The Dark Side of Our Voice Assistants." *The Guardian*, October 9, 2019. https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants
Maple, Carsten. "Security and Privacy in the Internet of Things." *Journal of Cyber Policy* 2, no 2 (2017): 155–184. https://doi.org/10.1080/23738871.2017.1366536
Martin, Kirsten. "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online." *First Monday* 18, no 12 (2013).
Martin, Kirsten. "Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online." *Journal of Public Policy & Marketing* 34, no 2 (2015): 210–227. https://doi.org/10.1509/jppm.14.139
Marwick, Alice E. and danah boyd. "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society* 16, no 7 (2014): 1051–1067. https://doi.org/10.1177/1461444814543995
McDonald, Aleecia M. and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." *A Journal of Law and Policy for the Information Society* 4, no 3 (2008): 543–568.
McKercher, Kelly Ann. *Beyond Sticky Notes: Co-Design for Real: Mindsets, Methods and Movements*. Sydney: Beyond Sticky Notes, 2020.

Metz, Rachel. "Yes, Tech Companies May Listen when You Talk to Your Virtual Assistant. Here's Why That's Not Likely to Stop." *CNN*. August 19, 2019. https://edition.cnn.com/2019/08/19/tech/siri-alexa-people-listening/index.html

Micheli, Marina, Marisa Ponti, Max Craglia and Anna Berti Suman. "Emerging Models of Data Governance in the Age of Datafication." *Big Data & Society* 7, no 2 (2020). https://doi.org/10.1177/2053951720948087

Molitorisz, Sacha. *Net Privacy: How We Can be Free in an Age of Surveillance*. Sydney: NewSouth Books, 2020.

Molitorisz, Sacha and James Meese. *The Consent Trap: Australian Focus Groups on Privacy, Smartphones and Consent.* Centre for Media Transition, University of Technology Sydney, 2020. https://www.uts.edu.au/node/247996/projects-and-research/digital-privacy-and-smartphones-finding-consent-sweet-spot

Obar, Jonathan A. and Anne Oeldorf-Hirsch. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23, no 1 (2020): 128–147.

O'Connor, Sean, Ryan Nurwono and Eleanor Birrell. "(Un)clear and (In)conspicuous: The Right to Opt-Out of Sale Under CCPA." *arXiv preprint:2009.07884* (2020).

Office of the Australian Information Commissioner (OAIC). *2020 Australian Community Attitudes to Privacy Survey*. September 2020. https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

Peters, Jay. "Apple Defends Upcoming Privacy Changes as 'Standing up for our Users'." *The Verge*, December 16, 2020. https://www.theverge.com/2020/12/16/22179721/apple-defends-upcoming-privacy-changes-standing-up-for-users-facebook-data

Reuters. "NSA Surveillance Exposed by Snowden was Illegal, Court Rules Seven Years On." *The Guardian*, September 3, 2020. https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules

Sarigol, Emre, David Garcia and Frank Schweitzer. "Online Privacy as a Collective Phenomenon." In *Proceedings of the Second ACM Conference on Online Social Networks*, 95–106. New York, NY: Association for Computing Machinery, 2014.

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: WW Norton & Company, 2015.

Sloan, Robert H. and Richard Warner. "Beyond Notice and Choice: Privacy, Norms, and Consent." *Journal of High Technology Law* 14 (2014): 370–414.

Solove, Daniel J. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126, no 7 (2013): 1880–1903.

Stevens, Hallam and Monamie Bhadra Haines. "TraceTogether: Pandemic Response, Democracy, and Technology." *East Asian Science, Technology and Society: An International Journal* 14, no 3 (2020): 523–532. https://doi.org/10.1215/18752160-8698301

Susser, Daniel. "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even if Consent Frameworks Aren't." *Journal of Information Policy* 9 (2019): 148–173. https://doi.org/10.5325/jinfopoli.9.2019.0037

Tene, Omer and Christopher Wolf. "The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent." *The Future of Privacy Forum*. January 2013. https://wiki.laquadrature.net/images/7/7f/Future_of_Privacy_Forum_White_Paper_on_Consent.pdf

Viljoen, Salomé. "Democratic Data: A Relational Theory for Data Governance." *Yale Law Journal*. Forthcoming.

W3C. *Report from W3C Workshop on Permissions and User Consent*. (2018). https://www.w3.org/Privacy/permissions-ws-2018/report.html

Waldman, Ari Ezra. "Power, Process, and Automated Decision-Making." *Fordham Law Review* 88 (2019): 613–632.

Watson, Penelope. "You're Not Drunk if You Can Lie on the Floor without Holding on: Alcohol Server Liability, Duty, Responsibility and the Law of Torts." *James Cook University Law Review* 11 (2004): 108–131. http://www.austlii.edu.au/au/journals/JCULawRw/2004/6.html

Zhang, Melvyn, Aloysius Chow and Helen Smith. "COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies." *Journal of Medical Internet Research* 22, no 12 (2020): e21572. https://doi.org/10.2196/21572

Zhou, Naaman. "ACCC Sues Google for Collecting Australian Users' Data without Informed Consent." *The Guardian*, July 27, 2020. https://www.theguardian.com/australia-news/2020/jul/27/accc-sues-google-for-collecting-australian-users-data-without-informed-consent

Zuboff, Shoshana. "A Digital Declaration." *Frankfurter Allgemeine*. September 9, 2014. https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html

Zuboff, Shoshana. "The Coup We Are Not Talking About." *New York Times*, January 29, 2021. https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html