18 February 2022

Australian Government Department of Home Affairs
Online at: www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers

Submission on Electronic Surveillance Framework Discussion Paper

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **UNSW Institute for Cyber Security** is a multidisciplinary Institute which focuses on research, education, innovation and commercialisation that has 'real world impact'. The Institute has over 60 members across each of our faculties. We are ambitious (achieving international impact), scholarly, collaborative and inclusive (acknowledging that cyber security is a new and developing field and seeking opportunities to broaden our understandings of the field by welcoming a broad range of disciplines), entrepreneurial (seeking opportunities to empower academics to be creative), diverse (embracing multidisciplinary and working as thought leaders), and generous and supportive (helping to develop and mentor early career academics, recognising vulnerable groups in society).

The **Deakin University Centre for Cyber Security Research and Innovation** ('CSRI') is a Strategic Research Centre that brings together a multi-disciplinary team of researchers drawn from Deakin's four Faculties. CSRI's research program is focussed on the technology, systems, human, business, legal and policy aspects of Cyber Security, and is committed to achieving translational and transformational research outcomes for industry, business and society. CSRI's research program is advised by senior industry and thought leaders through its Executive Advisory Board for Cyber (EABC) and is funded through national competitive grants and industry. More information about Deakin CSRI can be found at https://www.deakin.edu.au/csri.

About this Submission

We are grateful for the opportunity to make a submission on the Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Our main points relate to:

- The guiding principles for reform and, in particular, contexts in which concepts like balance and proportionality are inappropriate;
- The operation of existing laws in challenging contexts such as domestic and family violence;

- The importance of independent oversight as a crucial accountability measure, required for any agency with access to surveillance powers;
- The need for simplicity and streamlining, but not at the cost of the substance;
- The level of protection against geolocation and tracking;
- With reference to earlier research, ideas for policies around information sharing, transparency, industry-government co-operation and the Internet of Things.

We are happy to make them available on request by email to lyria@unsw.edu.au.

Guiding principles for reform

The proposal for reform set out in the Discussion Paper presents a fundamental shift – a paradigm shift – in how surveillance will be regulated in Australia. This Discussion Paper is asking the Australian people to relinquish privacy and embrace access. It uses principles of necessity and proportionality, not to limit access, but to enable it. The reasons given for this shift in focus include rapid change in information and communications technology, the law's (and agencies') struggles to keep pace with technological change, and the evolving, ever-present threat environment. The thrust of the Discussion Paper is to view the problem through this single lens without recognising the broader canvas.

There are some concerning statements in the guiding principles for this reform. Consider:

> [S]afeguards in the framework must reflect the importance of accountability, transparency, the rule of law, privacy and other applicable rights. These must be balanced against the need for law enforcement agencies and ASIO to have effective powers to investigate and disrupt serious threats (p6)

This suggests that accountability and the rule of law would be "balanced" against the need for agency powers. Leaving aside the question of what powers agencies should be granted, there should not be any suggestion that the powers that are granted should be able to be exercised unaccountably or in ways contrary to the rule of law. Indeed, the importance of accountability and (within constraints of operational secrecy) transparency was the centre of the 2022 annual threat assessment given by Mike Burgess, Director-General of Security. While agencies might ask for additional powers, we are not aware of any agency asking to be unaccountable or to suspend the rule of law in order to achieve their objectives. Any discussion of balance or proportionality in these contexts is misguided and is inconsistent with our liberal, democratic society (p3).

Even where there are diverse goals of the kind that might be balanced, it remains important to consider whether *both* goals can be achieved without a need for balance. In earlier interview research conducted by the Data to Decisions Cooperative Research Centre (reports available on request), a noticeable difference between interviews with Australian and UK agencies was the tendency in Australia to set up a dichotomy where the choice was "security" *or* "privacy". In the UK, these were almost always linked together with the conjunctive – "security *and* privacy". Encryption is an example of a tool that can enhance both (cyber) security and (personal) privacy. So while there are circumstances in which security and privacy must be balanced, such as intrusions on the privacy of suspects in the context of warrants, the focus should not be on the intersection but rather the union. Wherever possible, policy should optimise *both*.

Future reform work in this area thus needs to avoid being dismissive of privacy concerns or treating privacy as a barrier to be overcome. The report currently casts privacy is primarily as a problem, for example "the gradual amendments to powers and associated privacy protections have created confusion and legal uncertainty, reducing transparency of the framework" (p5). It suggests that "usual processes for getting a warrant" are a problem in emergency situations (p57). This language minimises the importance of an independent review of intrusive warrant powers, framing it solely as a roadblock to be avoided. While it may be appropriate for different procedures to apply in an emergency, we can have legal protections *and* efficient investigations. This requires care, for example a clear definition of what constitutes an "emergency", an opportunity for independent review (albeit in a different format), and procedures by which the appropriateness of the warrant can be reviewed subsequently when the emergency has passed (with any lessons learnt fed back to future applications). Emergency situations might be managed through telephone warrants or an on-call duty judge. Thinking of such solutions requires an approach that looks beyond *one goal*, instead asking how we can protect Australians, not only from criminals and security threats, but also from the government, including over-zealous or mistaken agencies. In other words, any increase in agency powers (if justified) should be countered by an *increased* concern with strong protections.

Another example of dismissiveness towards important values is the casting of agency reporting and other transparency activities as problematic, as not "meaningful" or "useful". For example, reporting on annual expenditure on electronic surveillance or reporting on warrant registers is described as "not assisting meaningful transparency". We suggest the solution here is not to dismiss the need for transparency (something that the Director-General of Security has stated is of central importance to ASIO), but rather to decide what makes transparency 'meaningful' and then to develop reporting requirements in line with that.

The guiding principles also suggest that the new legislation will be principles based, pushing "matters that are too specific to appear in legislation or are subject to frequent change" into delegated legislation and soft law instruments, such as policies and procedures (p6).[1] This weakens transparency and accountability because it avoids parliamentary scrutiny. While delegating legislation may be appropriate in some contexts, important matters should remain in legislation and any delegated legislation should be subject to consultation and made disallowable.

In addition to our concerns about the guiding principles for reform set out in the Discussion Paper, we would also suggest including an additional principle. The Discussion Paper is silent about the potential disproportionate harms of the proposed changes on marginalised communities. Electronic surveillance practices entail discrimination harms (as marginalised people are more frequently and extensively being surveilled)[2] and have disproportionate effects on minorities.[3] The proposed changes must be reconsidered in light of their potential discriminatory effects on specific communities, including indigenous communities, people of colour, LGBTQI+, women and the poor.[4] Principles of non-discrimination and awareness of the impact of any changes on marginalised groups should also be guiding principles for law reform in this area. In particular, streamlining surveillance

[1]For a discussion of the use and enforcement of soft law, including policies, procedures and guidelines, see Greg Weeks, *Soft Law and Public Authorities: Remedies and Reform* (Hart Publishing, 2015) 15-17.
[2] Mary Anne Franks, 'Democratic Surveillance' (2017) 30 *Harvard Journal of Law and Technology* 426 (2017)
[3] Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press, 2017).
[4] Danielle Keats Citron, 'A New Compact for Sexual Privacy' (2021) 62 *William and Mary Law Review* 1763.

and simplifying access to surveillance data requires putting in place protections against the discriminatory effects of this intensified surveillance.

Ultimately, our concern is that the Discussion Paper, on our reading, suggests a fundamental shift in thinking about surveillance in a democratic, rule of law country like Australia. There is a suggestion that privacy, transparency and even the rule of law do not matter as long as agencies can access the data they need to keep us safe. This is a superficial kind of safety. Replacing the rule of law with 'security' is usually a path preferred by failed or authoritarian states. In Australia, we can and should strive for security *and* privacy, all without compromising fundamental principles such as the rule of law.

Existing prohibitions and offences (questions 1 and 2)

UNSW has recently completed a research project exploring the intersection between technology facilitated domestic and family violence and privacy protections (both direct and indirect). We can make our report available on request. In essence, we found that privacy can sometimes be a double-edged sword when viewed from the perspective of victim-survivors. We made a series of recommendations including amending surveillance device legislation, harmonising information sharing rules among agencies, and ensuring police protect the privacy of victim-survivors while investigating perpetrators using under-utilised laws (such as computer offences).

Access to information (questions 3, 4)

Oversight is an example of an accountability measure that should be linked to the grant of powers. In other words, with the grant of greater powers (particularly powers exercised in secret) comes an expectation of greater oversight. Any agency that can access electronic communications should be subject to independent oversight similar to that provided by IGIS. The allocation of powers to agencies might therefore be linked with questions of what arrangements exist (or might be created) to provide for sufficient oversight. If the role of the IGIS is to be 'uplifted' then its budget should be increased commensurate with its increased workload.

Simplifying the framework and withstanding rapid technological change (question 16)

Thus, while we agree that legislation shouldn't be unnecessarily technologically specific or complex, we are also concerned to avoid short-cuts that may undermine individual privacy, identity and dignity.

The idea that legislation can "withstand" rapid technological change is not realistic.[5] It is never possible to contemplate what might be and, even if we had the imagination to do so, it is not worthwhile to craft laws for every imaginable future. Consider, for example, whether government would consider it a priority to ensure that road rules were applicable to flying cars merely because that would ensure the rules can withstand possible technological change.

[5] Lyria Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 7 *University of Illinois Journal of Law, Technology and Policy* 239.

Neutrality is often simply about what the default ought to be. In the context of surveillance, the default can be that new types of communications will be surveilled or that they will be protected until their surveillance can be specifically considered by parliament.[6] But a default of surveillance is not necessarily better. For example, consider a world in which human minds could "communicate" with otherwise paralysed limbs through the means of an electronic signalling device – would it be appropriate that these communications were made subject to surveillance given that communications within a human body are not otherwise subject to surveillance? To do so would be to target those with a particular physical disability. The same point goes for something like Elon Musk's Neuralink proposal. By pretending legislation can "withstand" technological change, we pretend that we can make choices now about things we don't yet understand. In the end, all we can do is choose a default (say, surveillability) without the facts necessary to make that decision. In that context, it may be preferable to allow future parliaments to consider future technological developments and make thoughtful decisions about how they should be treated.

Simplifying the framework is not as easy as it may seem:

- Privacy harms – and the type of information captured – are not easy to classify in advance. Interception of a specific communication may include unexpected information. While the technology-type classification is not perfect, it is conceptually clear and therefore easier to implement. In contrast, it is unclear how a content-based approach can be applied and implemented. For example, a work-related communication may unexpectedly include private, personal, and even sensitive information (such as sexual preferences).

- It is claimed that an information-type approach should be preferred as it is focused on privacy outcomes (while the existing approach focuses on method). However, the connection between information-type and privacy outcomes is unclear and unsubstantiated. Outcomes cannot be easily or accurately determined in advance, and both classification methods – information and technology – may have unexpected outcomes depending on the actual communications that are intercepted. Moreover, the assumption that an information-type classification improves privacy outcomes (in comparison to a technology-based classification) is unconvincing. Research into the typology of privacy and privacy harms suggests that interception or surveillance devices have additional, severe, harms, including a variety of autonomy harms.[7] Similarly, visual data may cause different privacy harms than audio or textual data. Therefore, a move toward information-type classification will disregard the unique privacy harms resulting from the interception method or the level of intrusiveness of the technology used.

- The Discussion Paper suggests that as part of the warrant application, an agency may be required to satisfy the issuing authority that the proposed methods of access are the least intrusive means available that would be effective in the circumstances. We welcome this suggestion in principle but propose that the level of intrusiveness will play a more significant part in the authorisation process, including serving as a stronger basis for classification than

[6] Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' (2010) 88 *Texas Law Review* 1685.
[7] Danielle Keats Citron and Daniel J Solove, 'Privacy Harms' (2022) 102 *Boston University Law Review,* available at SSRN: https://ssrn.com/abstract=3782222 or http://dx.doi.org/10.2139/ssrn.3782222; Rachel Finn, David Wright, and Michael Friedewald, 'Seven types of privacy', *European data protection: coming of age*, (Springer, Dordrecht, 2013) 3-32.

the information-type. As opposed to the changing content of evolving communications, the intrusiveness of the method can be determined in advance and can better reflect the potential privacy harms.

Streamlining legislation and transparency (question 17)

Streamlining legislation is important for transparency.[8] *Unnecessary* complexity, for example the spread of surveillance powers across multiple different pieces of legislation, makes it more difficult for the public to understand and engage with surveillance policy. For public transparency, the public needs to understand which agencies can do what as well as, broadly, the policy rationale underlying such powers. The rules should be in one place, clearly set out, and avoid unhelpful or incomprehensible distinctions.

Harmonisation and simplification, however, are not the only elements to consider. There are important distinctions to be made and their framing is crucial. We are concerned about changes to thresholds and tests throughout the Discussion Paper and what they might say about *how* streamlining will occur. Slippage in language from 'prejudicial to security' to 'relevant to security', an increase in scope (in terms of offences *and* communications covered), an association of protective measures with adjectives such as "impractical" and "ineffective", and insufficient attention to the importance of independent oversight all suggest that streamlining could be a Trojan horse for unaccountable, expansive powers.

Geolocation and tracking (question 19)

The intent of the proposal to regulate tracking information 'separately' is presumably to make the thresholds for obtaining a warrant or other authorisation lower than for other types of surveillance. However, the assumption (and justification) stated in the Discussion Paper and the Comprehensive Review that 'tracking information may have less impact on privacy than other surveillance information', and is 'less intrusive', is problematic. Much private and sensitive information can be collected from location tracking, particularly when combined with other publicly available (or otherwise easy to obtain) information such as what business or person lives or works at a particular address eg visits to cancer specialists, women's shelters, brothels, hotels and bars, sexual health and abortion clinics. Tracking geolocation information – especially 24 hours a day over many months – is much easier and cheaper than other forms of surveillance (especially labour-intensive surveillance). Its utility is also significantly increased by the existence of tools to aggregate and discern patterns in information. Therefore, tracking technologies are likely to be used by agencies intensively, particularly if authorisation is made easier, thereby significantly raising the probability of revealing private information. Even though a "person's movements are typically observable to others and less private in nature", no one has a legitimate expectation that they will be observed so closely over a long time period.

[8] Lyria Bennett Moses and Louis De Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41 *Melbourne University Law Review* 561.

Even if tracking devices are regulated separately, the threshold levels for authorisation of this type of surveillance should not be substantially different than those already in place for other types of surveillance.

Necessary and proportionate (question 23)

The way the Discussion Paper conceives of the balance to be struck in the new framework is problematic. As explained above, some things ought not be put into a 'balance'. The idea of proportionality raises similar concerns.

Proportionality has been adopted worldwide as the reasoning tool for managing (for want of a better description) encroachments on rights and freedoms. It has been picked up by our legislature and courts, with some academic discussion and judicial disagreement around the appropriateness of doing this.[9]

In many contexts, proportionality works well, providing clarity in reasoning and decision-making. But it is important to ensure it is used appropriately in the relevant context.[10] Research has shown how the proportionality principle in telecommunications interception and access law has been eroded through amendments that have significantly expanded the operation of warrants without making equal adjustments to the protection of privacy.[11] For these reasons, proportionality, structured, calibrated or otherwise, is only as good as the things it balances, and rests on the independence and reliability of the person doing the balancing. The proposal in the Discussion Paper does not deal adequately with either of these things, allowing proportionality to be further eroded in favour of the agency doing surveillance. The tone of the Discussion Paper also skews how proportionality may play out, by characterising checks and balances as unrealistic and unreasonable while characterising agency action as urgent and essential.

On page 52, the Discussion Paper sets out the "potential future state" of the necessary and proportionate test. It will not always be exercised by someone independent of the agency and independent of politics. Decision-makers include senior officers and government ministers. Agencies can exercise surveillance powers even if they are subject to minimal oversight. The considerations focus on agency objectives, beginning with the gravity of the matter under investigation, with consideration of impact on *individual* privacy but not on the broader consequences of greater surveillance in a liberal, democratic state. While the gravity of the matter under investigation is mentioned as a factor, the Discussion Paper suggests that powers could be used for relatively minor offences.

In sum, our concern is not that "necessity and proportionality" will play a role, it is what the framing of the Discussion Paper suggests about how the test will play out in practice. The Australian proposal

[9]There is disagreement about proportionality in the context of the implied freedom of political communication in the High Court. Adrienne Stone and Rosalind Dixon have both written separately and expertly on the topic. see Rosalind Dixon, 'Calibrated proportionality' (2020) 48(1) *Federal Law Review* 92-122, especially 95-98; Adrienne Stone, 'Proportionality and its alternatives' (2020) 48(1) *Federal Law Review* 123-153, especially 127-131.

[10] Niloufer Seladurai, Nazzal Kisswani and Yaser Khalaileh, 'The proportionality principle in telecommunications interception and access law in an environment of heightened security and technological convergence' (2016) 25(3) *Information & Communications Technology Law* 229-246, 230.

[11] Ibid, 239

is inferior to that operating in the UK, which also has the benefit of human rights legislation and an independent issuing authority (IPCO).

Information sharing (question 25)

We support a principles-based, tiered approach to use and disclosure. The issue, of course, is how these principles are articulated. A series of research reports for the Data to Decision Cooperative Research Centre set out how this approach might be realised. The reports can be made available upon request.

Transparency (question 32, 33)

A research paper by Lyria Bennett Moses and Louis de Koker examines how transparency can be achieved in the context of national security and law enforcement activities, including surveillance.[12] Because transparency is important for public trust, the public should be given sufficient information to understand the operation of surveillance laws and oversight mechanisms. All information, including operational secrets, should be transparent to an independent oversight agency such as IGIS, sufficiently resourced with funding and expertise. In addition, as much information as possible should be disclosed to the public, and operational secrecy should not provide an excuse beyond what it actually requires.

Consideration should also be given to clarifying and improving oversight of the regulatory relationship between industry and government, including reviewing the functions and activities of the Office of the Communications Access Coordinator within the Department of Home Affairs and the Australian Communications and Media Authority.

Industry and Government Cooperation (questions 34-36)

The Discussion Paper does not adequately address the role of the communications industry in the proposed legislative framework, devoting only 3 pages to it. We note that any reforms to industry's assistance obligations depends on the outcome of the parliamentary reviews listed on page 71. However, given that a large portion of Australia's critical infrastructure, which now includes communications infrastructure, is privately owned and operated, any contemporary understanding of the proposed surveillance framework, or the broader canvas, must involve an examination of the regulatory relationship between industry and government.

Lawful surveillance in Australia is characterised by an historical, operational interdependence between the telecommunications industry and law enforcement and security agencies. Since the1990s,[13] interception and access regulation has operated using mix of highly technical 'command and control' legal obligations within a framework comprised of formal and informal negotiation, collaboration and cooperation between industry and government, law enforcement and security agencies. The mechanisms include direct regulation by the Office of the Communications Access Coordinator and the ACMA; business liaison units within agencies, industry working groups,

[12] ibid.

[13] Beginning with the introduction of the concept of 'reasonably necessary assistance' - a requirement that carriers and carriage service providers provide law enforcement and security agencies with assistance 'as is reasonably necessary'. See *Telecommunications Act 1991* (Cth), s63(4)(m).

networks, committees, roundtables and forums.[14] The regulatory tools include legislation, legislative instruments, plans, guidelines, policies, procedures, fact sheets, administrative guidance and other mechanisms.[15]

As noted in the Discussion Paper, the telecommunications industry is no longer the sole provider of communications products and services, the methods and means of communicating have evolved as new technology and innovations have been deployed. The community of industry stakeholders has grown to include multi-national corporations and off-shore service providers, alongside smaller companies and operators. It is understandable that the task of negotiating rules and regulations with this disparate group is increasingly challenging and difficult.

Despite the known challenges, industry and government collaboration will continue to be the most important part of how lawful surveillance will work in practice. A reliable and cooperative working relationship with industry is essential.

There are various options available for industry and government to enhance collaboration and cooperation within the surveillance regulatory landscape, but also across the broader security landscape encompassing cyber security and critical infrastructure. The last major structural reform of the interception and access co-regulatory framework occurred in 2007, implementing the recommendations of the *Report on the Review of the Regulation of Access to Communications* by Anthony Blunn AO.[16] It is therefore timely to undertake a close examination of the advantages and shortcomings of the longstanding co-regulatory frameworks of the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997* for interception and access. Recent reviews and research in the area of telecommunications and broadcasting demonstrate both the strengths and weaknesses of co-regulation in the communications sector, and the importance of review.[17]

Surveillance regulation raises specific challenges and concerns in a co-regulatory environment, particularly around participation, maintaining secrecy and operational integrity. There may also be gaps in expertise and difficulties in meeting timeframes with so many new stakeholders.[18] However, researchers working in cybercrime, cybersecurity and national security have noted that '[t]he strength of [the co-regulatory] approach is that there is a consistent approach to (self-) regulation over time and that the industry has external oversight to ensure progress on issues causing major

[14] See eg, Communications Security Enforcement Roundtable: https://www.directory.gov.au/portfolios/infrastructure-transport-regional-development-and-communications/australian-communications-and-media-authority/communications-security-and-enforcement-roundtable.

[15] For a summary of administrative guidance and other resources, see: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/administrative-guidance.

[16] The Blunn Review's recommended changes to the role of the Communications Access Coordinator and the ACMA were introduced by the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth), which included shifting the interception and delivery capability provisions from the *Telecommunications Act 1997* (Cth) to the *Telecommunications (Interception and Access) Act 1979* (Cth).

[17] See eg, Karen Lee and Derek Wilding, 'The Case for Reviewing Broadcasting Co-regulation' (2022) 182(1) *Media International Australia Incorporating Culture and Policy* 67-80; Karen Lee and Derek Wilding, 'Towards Responsiveness: Consumer and Citizen Engagement in Co-Regulatory Rule-Making in the Australian Communications Sector (2021) 49(2*) Federal Law Review* 272-302; Karen Lee, *The Legitimacy and Responsiveness of Industry Rule-Making* (Hart Publishing, 2018).

[18] See eg, Tatiana Tropina and Cormac Callanan, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security* (Springer, 2015) 46

inter-organisation disagreement.'[19]A challenge for government will be to ensure that industry and government cooperation and collaboration is accountable, transparent, and consistent with the rule of law, without undue negative impact on operational secrecy, business confidentiality and industry competitiveness.

Reviews in the context of the Internet of Things (question 37(a))

Recommendation 5 of the Data Retention Review (DPR) clearly recommends that service providers are **not** required to retain information generated by the Internet of Things and similar devices. The second part of the recommendation contemplates the Government making specific amendments to require retention by service providers in cases where the benefits outweigh the costs. The costs are significant, so minimisation of mandatory data retention should be a guiding principle. In particular, it is well-known that Internet of Things and similar devices can be used to collect, process and share not only a much greater quantity of data than conventional computing and telecommunications devices, but 'data that is much more intimate and personalised in quality'.[20] The problem with this is that individuals' privacy and security risks of all this data collected from smart devices is already significant due to the actions (or inaction) of commercial entities. With increased data collection, storage and sharing comes an increased risk of damaging data breaches (whether due to cyber attacks or misadventure) such as the one experienced by the NSW government in mid-February 2022.[21] However, poor cyber security practices are endemic in the manufacture and configuration of the Internet of Things.[22] Privacy practices are problematic as well, as displayed in the egregious example of Standard Innovation who collected individual usage data from customers who had bought its We-Vibe Internet-connected sex toy.[23]

Government should not be adding to the existing risk of harm by expecting service providers to retain data.

Yours sincerely,

Lyria Bennett Moses

Kayleen Manwaring

Susanne Lloyd-Jones

UNSW Allens Hub and IFCYBER

Shiri Krebs

Deakin CSRI

[19] Ibid.

[20] See eg Kayleen Manwaring, 'Emerging information technologies: challenges for consumers' (2017) 17(2) *Oxford University Commonwealth Law Journal* 265, 277.

[21] Jonathan Kearsley and Clair Weaver, 'Sensitive business addresses among 500,000 published in COVID data breach' *SMH Online* (14 Feb 2022) https://www.smh.com.au/politics/federal/sensitive-business-addresses-among-500-000-published-in-covid-data-breach-20220214-p59wal.html.

[22] Kayleen Manwaring and Roger Clarke, 'Is your television spying on you? The Internet of Things needs more than self-regulation' (2021) 93 *Computers and Law* 31.

[23] See eg Kayleen Manwaring, 'Emerging information technologies: challenges for consumers' (2017) 17(2) *Oxford University Commonwealth Law Journal* 265, 280-281.