Submission for Department of Home Affairs Consultation
Strengthening Australia's Cyber Security Regulations and Innovations

Dr Ian Warren, Senior Lecturer, Criminology, Deakin University, Geelong, Victoria – [redacted]

Dr Monique Mann, Senior Lecturer, Criminology, Deakin University, Geelong, Victoria – [redacted]

Dr Diarmaid Harkin, Senior Lecturer, Criminology, Deakin University, Geelong, Victoria [redacted]

August 23, 2021

This brief submission focuses on the labelling of smart devices, which is often viewed as a key issue to improve transparency relating to privacy, security and consumer protection issues. We put this submission forward having recently completed a report for the Australian Communications Consumer Action Network (ACCAN) that examines icons as a method for enhancing consumer awareness for privacy issues associated with the Internet of Things (IoTs). The full report can be accessed at the following web address: https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer-privacy

Of the three options proposed in the *Strengthening Australia's Cyber Security Regulations and Innovations* discussion paper, we favour Option 2, Mandatory expiry date label supported by the Cyber Security Strategy Industry Advisory Panel, over maintaining the status quo or a voluntary labelling system. However, we also recommend:

a) The Panel's findings on all devices it scrutinises be made public;
b) This option should incorporate an issue from Option 1, which requires moderate testing of device security. This cost could be displaced back onto industry to ensure more rigorous compliance with relevant IoT security standards. Without an independent testing regime of this nature, we do not support Option 2 in its current form.

Our view is based on a survey of 1052 Australians, comprising 844 IoT consumers and 208 non-consumers, as well as interviews with 32 key stakeholders with expertise in digital security, information privacy, regulation and consumer advocacy. Our research suggests an icon system will only be viable if it is tied to more holistic legislative reform associated with IoTs, privacy and data security. This is because these devices are not constructed with security in mind, and there are concerns regarding the security standards amongst both large multi-national companies, and many small startup companies that develop these devices for the commercial market.

Our sample of survey respondents and interviewees showed very strong approval for an icon system if it can be supported by stronger privacy regulation. This kind of regulation should be in

the form of graded fines or other substantive measures that consumers are made aware of, rather than the current national IoT voluntary code of practice, which is seen as being ineffectual and having no independent oversight or related penalties for non-compliance. Recommendations 5 and 6 of our report indicate any icon system must be situated within a stronger privacy and consumer protection framework supported by adequate enforcement mechanisms, and potentially supplemented by direct involvement of the CIoT industry.

A particular risk with an icon system is that it will place more responsibility on consumers to make themselves aware of the privacy and security risks of IoT devices, without adding to the burden of responsibility for government or the commercial IoT industry. This has particularly problematic effects for certain vulnerable groups, including children, their parents, people with disabilities (who might avoid engaging with the benefits of this technology because of the lack of awareness of the risks), and people from CALD and Indigenous communities. In other words, lack of adequate regulation risks limiting safety and protection for people who might benefit most from these technologies. An icon system without sufficient accompanying regulation will simply provide a notional endorsement that a product is safe. More substance is required to satisfy consumers that an icon or trust mark system stands for something and is backed by a regulatory system to justify that endorsement.

Both our survey and interview findings indicate substantial law reform and greater industry engagement are required before icons can have meaningful impact in addressing the privacy issues relating to CIoTs. Were a star rating system be devised, as recommended on p. 36 of the *Strengthening Australia's Cyber Security Regulations and Innovations* discussion paper, the ultimate question is: which body would oversee the integrity of the system or its enforcement? At present, pinpointing responsibility on any Federal agency would require matching financial support to ensure the system has sufficient capacity to oversee device and data security practices, and to enforce these in a meaningful way for the benefit of consumers.

Similarly, any form of non-government or industry oversight requires some form of independent review, a system for lodging complaints and enforcement processes to give integrity to an icon system. Our report recommends industry support is needed for an icon system to operate adequately, but this can risk industry endorsing its own products, without independent review or scrutiny. We believe this function is better served through a government department with independent statutory authority. We favour this approach because of the high privacy and security risks associated with IoT devices, and the current focus of Australian consumer law which places most of the burden for finding out about these risks before making purchasing decisions onto the consumers.

We therefore propose that of the three options presented in the discussion paper, Option 2 is preferable. However, our support for Option 2 is qualified as our survey and interview data strongly suggest more holistic reforms to privacy law, security practices and consumer protection laws are all needed to deal with IoTs, largely on the back of the rapid growth and relatively lax regulation of this industry to date.

To make an icon or trust mark system viable requires expanding the powers of an existing government department, or creating a new one, to systematically review the security and privacy sensitivity of IoTs. This will develop a trust mark system that reflects trust in both the device and the agency overseeing its approval. In our view, this approach should replicate the Californian model to provide robust form of consumer protection (Cranor, 2021). Ideally, an icon system needs to operate in line with stronger government or self-regulation. An icon system is not a substitute for regulatory reform but can have an important supplementary role in any reform process.

For further details about our report please visit the ACCAN website https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer-privacy and do feel free to contact any of us should you feel this would assist in your review of IoTs, icons and current Australian regulation.

References

Cranor, L.F. (2021). 'Informing California Privacy Regulations with Evidence from Research', *Communications of the ACM*, vol. 63, no. 3, pp. 29-32. Available at https://cacm.acm.org/magazines/2021/3/250700-informing-california-privacy-regulations-with-evidence-from-research/fulltext.

Warren, I., Mann, M. & Harkin, D. (2021). *Enhancing consumer awareness of privacy and the Internet of Things*. Sydney: ACCAN. Available at https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer-privacy.