Is my home spying on me? As smart devices move in, experts fear Australians are oversharing

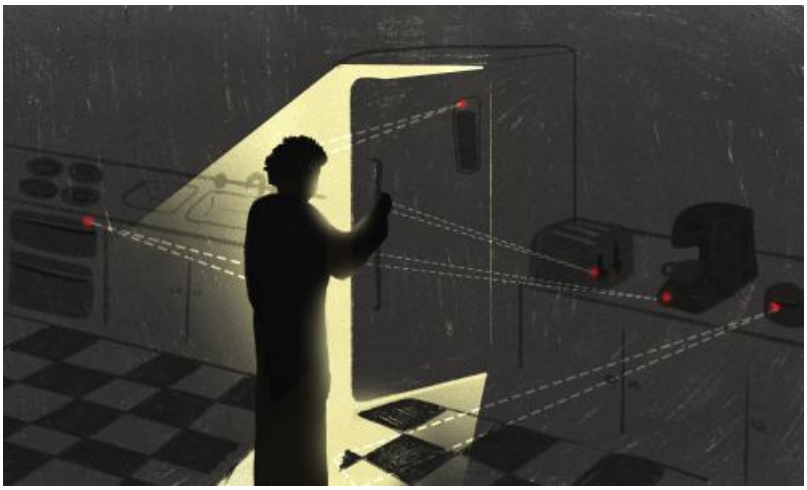
Publication Date: 2024-02-10

Author: Jordyn Beazley

Section: Technology

Tags: Smart homes, Privacy, Data protection, Law (Australia), features

Article URL: https://www.theguardian.com/technology/2024/feb/11/is-my-home-spying-on-me-as-smart-devices-move-in-experts-fear-australians-are-oversharing



Take a look around your home and chances are you have one, or at least you have considered the convenience of having one. They are the devices and appliances that can be remotely controlled – otherwise known as smart devices – which over the past decade have become core features of the modern home. Think of the TVs that allow you to flick through various streaming services, the smart fridges that can have their temperatures moderated and contents checked from afar, the robot vacuum, air purifiers, or one of the big tech companies' virtual helpers to play music or dim the lights. But as the technologies gather, share, aggregate and analyse the data collected, that convenience has come at a cost: privacy. Experts say consumers should be aware of how much personal information they are trading, and what that information is used for. "I think it's very concerning, particularly because we don't have up-to-date privacy legislation in Australia, and for that matter, it's a big problem globally as well," says Katharine Kemp, an expert in law and data privacy at the University of New South Wales, who warns that little is known about where the collected data ends up. Sign up for a weekly email featuring our best reads "We don't know the full extent of the ways that information is used because we still have privacy policies that are worded very broadly," she says. There are obvious advantages to smart devices, Kemp says, including creating a more environmentally conscious home. But she doesn't think that is the main objective of the companies selling the products. "I think the main objective of the smart devices is to collect more information and sell us more things," she says. "There is an intricate advertising technology ecosystem which feeds on this kind of data because it targets advertising on the basis of people's behaviour and attributes. "If you think more broadly about who would be interested in information about our private behaviour and our attributes, then potentially there are going to be insurance companies or even, in some cases, foreign governments." While anonymised data about what is in your fridge or what you watch on TV may seem harmless in isolation, Kemp says this data can be matched under a unique identifier to create a more detailed profile. "[Data brokers] collect and buy data from other sources, they analyse it or cross-reference it in certain ways and they sell it to other people," she says. "We've got a law in Australia that says that organisations must not collect information about you from third parties unless it is unreasonable or not practicable to collect it directly from you, but that law is not enforced." 'The consent model is tricky' Sam Floreani, the head of policy at Digital Rights Watch, shares similar concerns, but says some smart devices are seemingly more innocuous than others, with many using the data for positive means, such as informing health initiatives. "It's not a given that data collection is necessarily evil in and of itself," she says. "It comes back to what the underlying incentive is, and whether that's a profit motive or based on invasive surveillance practices." Earlier this month, Dyson released a study that tracked the indoor

air quality across 3.4m homes in 39 countries. The study, which is not nationally representative, found all 39 recorded above the average safe standards for indoor air pollution. The company, which adhered to privacy laws and de-identified the data after consumers opted into taking part of the study, said it was a world first at this scale. “We have this philosophy and engineering of solving problems that others ignore … the better you understand the problem, and the more factual and quantified data you have around it, the better you can design engineering solutions to solve those problems,” says James Shale, an engineer at Dyson. Other collections of data have drawn widespread alarm, including the suggestion in 2017 that the maker of the Roomba robotic vacuum, iRobot, might begin to sell floor plans of its customers’ homes to Amazon, Apple, and Google. The company’s planned acquisition by Amazon was abandoned last month after being vetoed by the EU. Or the sex-toy maker We-Vibe, which faced a data collection lawsuit after it was found to have tracked the use of its “smart vibrator” without users’ knowledge. The company settled and agreed to compensate its customers up to C$10,000 (A$11,200) each. Australia’s current privacy laws do require consent, however Floreani says customers are not always properly informed. “The consent model is tricky because it does rely on individuals to fully understand and be able to make choices about their data, which a lot of people just don’t have the time or the expertise to do, so you end up consenting,” she says. Kemp says the definition of consent under Australia’s privacy laws includes implied consent, which she says is one example of where the laws are not stringent enough – or where laws do already exist, such as banning organisations from collecting data from third parties, they need better enforcement. The federal government plans to overhaul the laws , after a wide-ranging review into the Privacy Act last year that made a series of recommendations. In its response to the report, the government noted the need to bring the laws into the “digital age”, and that this would include consideration on improving the consent law and rights in relation to personal information, as well as increasing the enforcement powers of the privacy watchdog. “The government has agreed in principle to a number of proposals and noted others, so to a very large extent we still don’t know what the government will propose and what will ultimately pass through parliament,” Kemp says. Convenience vs privacy For others, the trade-off in privacy has been worth it to an extent, particularly where it has improved accessibility. “When I turn on my air conditioner, I have to ask someone what it is set to, but there are a number of people buying smart air conditioners that connect to these things and say ‘turn my air conditioner to 22 degrees’, says Chris Edwards, head of Vision Australia. Vision Australia has found the devices have played a crucial part in reducing social isolation for the vision-impaired community. “We had a person that loved cooking new recipes, but with their loss of vision, they lost that,” he says. “They learned how to just ask Alexa for a recipe and it gave them that information but also the confidence to be able to cook, as well as simply read books through Alexa.” Still, he doesn’t think that convenience should come at the expense of privacy. “I think one of the challenges, like with a lot of these things, is that there’s not very many people [who] read the privacy policy connected with these devices,” he says. ‘It’s just too tempting’ Kemp says there were earlier concepts of what was known as “closed loop smart homes”, which would collect data purely for the purposes of their residents. “[That] didn’t eventuate because there was this discovery that behavioural advertising services could be so lucrative,” she says. “It’s just too tempting for all of those organisations that have the technological capacity to collect that information and use it for their own commercial purposes.” But it could be restricted with a change in privacy laws, Kemp says. “There are very limited ways people can restrict the impact of smart devices at the moment,” she says. “We would be a lot better off if the privacy laws set stricter standards on how companies should behave.”