This is an electronic version of the transcript of a live event.

All reasonable endeavours were taken to assure the accuracy of the content.
However, due to the nature of capturing a live speaker's words, it is possible that it may contain errors and mistranslations.
Ericsson Broadcast and Media Services accepts no liability for any event or action resulting from this transcript.
The transcript must not be published without Ericsson Broadcast and Media Services' written permission,
which may be withheld at its absolute discretion.

Day 2, Thursday 15th September

1:30-2:15pm: Connecting the Future Consumer

TERESA CORBIN: We have a couple more Google Cardboard VR glasses – F51! F51...? No? OK. Another one. F68!

Still not...? OK, one more. F89? F89...?

>> F98?

(LAUGHTER)

TERESA CORBIN: OK – F90! OK – F93...

>> One more go. Come on...

TERESA CORBIN: F92...? Nup... Come on, Laurie – you can't win it! There's hardly any numbers left! F27?

Someone's looking... No winners?! No numbers? F88...?

Everyone's lost their numbers. You're playing a game on me now! F88? No? OK, I feel like I just changed professions...

F14? Hey!

(APPLAUSE)

Alright. There you go. Alright.

Um – F33? No?

F35?

Alright. I can guarantee there's no privacy ramifications with this prize.

(LAUGHTER)

Alright, now I'm going to introduce Laurie Patton, and he'll introduce the speakers for this afternoon's session. I'll leave it in your hands, Laurie.

LAURIE PATTON: Thank you. Hi, everybody. Panel, please join me. So, this panel, we're going to give you a vision for the future for how consumers will be equipped to stay connected in the future. I thought that I'd start by

noting that 2016 is the National Year of Digital Inclusion, which is an initiative of InfoXchange and funded by Australia Post. Along with Nan Bosler, who was here earlier – not sure if she's still here – and a number of others, I'm one of the Go-Digi champions. This is a year for making sure that people, in remote areas or people with disabilities or people who just have not had the opportunity to acquire the skills to use the internet are being given special focus. And there are events happening all around the world... Probably do, but all around the country, to bring digital skills to people who don't have them. My main game as the chief executive of Internet Australia is to campaign for a decent broadband network, but the point, of course, is that it's only part of the equation – there's not much point giving people access to the internet if they don't have the skills to use it. So, um, we're going to talk – each of our panellists is going to talk for about 10 minutes. I'd like to ask you to indulge us by keeping questions to the end. And then we're going to spend time in a didactic arrangement, so I'm not going to apply the rule that you can't just make a statement, 'cause there might be people out there that know things we don't know. Hey, who cares? So, questions are certainly accepted, but also statements, but if they're statements, please keep them reasonably short. Now, um, I'm going to actually ask each of our guests to introduce themselves, and to also say why they think it's important for them to be talking today, and I'll start with Alex.

ALEXANDER VULKANOVSKI: Hi, I'm Alexander Vulkanovski. I was the 2015 Google ACCAN intern. As part of my responsibilities as the Intern of Things, I like to call it, I produced a report for ACCAN and Google on the Internet of Things on Australian consumers, titled Home, Tweet Home: Implications of the Connected Home, Human and Habitat on Australian Consumers.

Why it's important here today? When I produced this report, it was probably one of the first of its kind in Australia, in particular. I think the Comms Alliance beat me to it and put something out late last year, but no doubt this was one of the first out there for this country. So, um, hopefully we'll see more.

KATE CARRUTHERS: Hi, folks. I'm Kate Carruthers, the Chief Data Officer for the University of NSW. I'm also an adjunct senior lecturer in computer science and engineering. I research the Internet of Things, and I'm particularly interested in privacy and security. And I will have a few things to say on that today.

LINDA LEUNG: Hi, I'm Linda Leung, an honorary associate of the UTS Business School, and a consultant in human-centred design and digital user experience. Um, so I guess I'm here today because of, the um, 14 years I've been here at UTS and the research I've done around digital divides and looking, particularly, at marginalised communities and groups, and how they appropriate technology.

LAURIE PATTON: Alex is up first – to the lectern, sir.

ALEXANDER VULKANOVSKI: Thanks, Laurie.

Good afternoon, esteemed guests. Welcome to the final quarter of the conference. Last week, my boss wanted to give me some advice on speaking to a conference. He basically said, "On the day, flick through the news, try and find something relevant, try and find something engaging" – relevant to your topic that the audience can relate to. So this morning, I did that. I tried to find a relevant story on the Internet of Things and consumer risks. And I found a little gem. The headline was "Smart Sex Toy Company Sued for Tracking Users' Habits."

(LAUGHTER)

I thought, "No, I'm not mentioning that one." So I didn't.

(LAUGHTER)

Last year, I had the honour of being the 2015 Google ACCAN intern. I produced a report on the Internet of Things and Australian consumers. Today, I hope to provide a high-level snapshot of my findings, focusing on the connected consumer and the connected home human and habitat. Let's start with – what is the Internet of Things? A beginner's definition focuses on pretty much everyday objects being connected to the internet. An intermediate definition focuses on the network of these physical objects and how they intercommunicate and interoperate. But my report chose the complicated definition. By the IERC. Let's go through this one together. "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable

communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities, and use intelligent interfaces and are seamlessly integrated into the information network." Sorry about that. Now, my presentation will go through the who, when, how, what and why of connected consumer issues, before providing some high-level findings and consumer recommendations. First of all, who is the connected consumer? A good place to start is our very own ACCAN. ACCAN's six principles of a connected consumer involve access to voice and data services that are affordable, that are standardised, that are accessible to all, and where the consumer is engaged with online services, particularly e-commerce, and they have sufficient digital literacy and empowerment. In an IoT ecosystem, some of these traditional consumption principles will change. For example, citizens will be consumers of smart cities, patients will be consumers of e-health and wearable services, consumers of smart cars and autonomous vehicles may not be drivers, but passengers. And finally, one of the biggest IoT consumers will be vendors themselves, as increasingly, consumers and their data become the product. When will this occur?

Most research and literature on IoT seems to use 2020 as a significant milestone. By 2020, the number of connected things is really set to hit scale, with Cisco's 50 billion connected things by 2020 being one of the more popular predictions. In Australia, IoT is expected to be worth billions, while predictions from Telsyte include a large increase in connected home and wearable things. The following graphics summarise the evolution of data exchanges, from a single transaction between two people to the complex world we live in today. They were taken from Microsoft's presentation to a 2013 FTC IoT workshop. Let's take a look. As we can see, the exchange of personal information involves dozens of players, platforms and ecosystems. This is where IoT is taking us. By connecting more things, it means more data sets, more sharing, and more intimate data. Examples of new data sources include smart cars, smart homes, wearables, and smart cities. How will connected consumers consume? As the barriers between the physical and digital break down, e-commerce will become more autonomous and more interactive. For example, smart appliances can be programmed to make autonomous purchases. If you're running low on milk, your fridge can order you some more. Weight censors and bar code censors will make sure that you and your health insurer can track your diet.

(CROWD GROANS)

An example of interactive e-commerce is the Amazon Dash. Effectively, a button that, when pressed, places a preset order with Amazon. If you run out of shaving cream, just... I think I've gone too far. ..hit the "Gillette" button, and another one will be on its way. Personalised marketing – as things get smarter, so too will marketing. For example, eye scanners can be placed in items or billboards and track your eye movements as you view these things. Did you take a second glance at that pair of shoes? Maybe a discount code sent to your smartphone or smartwatch can help your decision.

Finally, smart retail spaces – tags on products can track inventory. Bluetooth beacons can track customers around the store. A few tags, an app on your smartphone, and a linked account can make autonomous checkouts a reality. This is best summarised by Ric Merrifield, an IoT consultant writing for the Harvard Business Review: "You can know when customers come into your store, how long they are there, what products they look at and for how long, then you can view the data by the shopper's age, gender, average spend, brand loyalty, and so on." Now, the crux of it – what are the consumer issues of IoT? One of the biggest issues is interoperability. It's great having those 50 billion connected things everywhere, but what's the point if they don't get along? Will these things communicate? What if my Fitbit doesn't talk to my espresso machine, and doesn't make a single shot instead of a double when my heart rate drops below 75?

(LAUGHTER)

Certainly First World problems. Not everything will run on wi-fi. The right network is needed for the right device. Will they interconnect? Or will they be connected to a single hub? Affordability – a fundamental consumer issue. The freemium business model – goods and services are provided for free, with the data it collects. IoT will push the collaboration of hybrid goods – a smart TV, for instance, is equal parts tangible property and intangible software. You may own the tangible TV, but not the copyrighted software. Does this limit your exclusive rights over the TV? Insurance implications are an indirect affordability issue. An activity tracker will know your sleep, exercise and dietary patterns. A smart fridge will know your diet. A smart car will know your driving habits. This data may be very useful to your insurer, where good habits can be rewarded and bad habits penalised. One of the benefits of a connected home is expenditure tracking. Utility meters, water leaks, energy usage – a

connected consumer can maximise the efficiency of their smart home, and minimise their monthly bills. Accessibility. IoT has enormous potential to assist the more vulnerable consumers. Children, for instance, are able to be monitored by worried parents. Their whereabouts and health can be tracked accurately and remotely. This also goes for the elderly and sufferers of chronic diseases, who'll be one of the biggest beneficiaries of wearables and e-health. Wearables will be able to replace fixed medical alarm systems, which will give more information, including location, heart rate, slips and falls, and other physiological factors. People with disabilities will benefit from new user interfaces. For example, people with visual or hearing impairment can benefit from gesture search, voice control, wireless sensory networks, to interact with new technology. Consumer protection. This will be challenged in five ways. Firstly, identifying liability or a defect in a good, in a complex chain of responsibility. Clarifying the court's position on faulty software. And finally, the responsibility for autonomous contracting. For example, that fridge I mentioned earlier that made autonomous orders. What if the order was not verified, and only based on a recommendation? Serviceability – with more connected things comes more responsibilities. Here are some questions. Will all my things need updating? When will they be obsolete? How is everything going to be powered? With all these things to consider, do I have the cognitive bandwidth to worry about all this? Isn't this meant to make things easier?

(LAUGHTER)

Finally, the two biggest IoT consumer risks – privacy and security. At this point, it's good to refer back to Dr Newham's diagram with a whole bunch of dire exchanges flowing between individuals and organisations. More connected things will mean more data collection points, more vulnerabilities, more intimate information from inside your home, car, or even your body. Why should we care? IoT is unlikely to create many new consumer issues. These were one of the conclusions I drew in my report. Most mentioned earlier are already present in some form or another. Instead, I concluded that IoT is likely to exacerbate pre-existing issues in five ways. Firstly, scale. 50 billion connected things by 2020 means 50 billion data collection points, attack platforms, vulnerabilities, and opportunities. Secondly, method. IoT will change the means of collecting data. Examples include connecting everyday objects, wearables, and connected cars. These things were not around a short time ago. Thirdly, reach. IoT data is inherently more intimate. It is now able to reach inside our homes, inside our cars, and even inside our bodies. Fourth, nature. IoT by its nature is more covert. Automated and subject to machine learning. Which is an evolution from where we've come. And finally, depth. All of these, when combined, will create a synergetic effect. Where the creation of an Internet of Things is greater than the simple sum of its things. I'll conclude with five connected consumer recommendations.

Firstly, stay informed. Know your device, know your service, know what it does, how it does it, and how to gain as much control as possible. Choose uses carefully and opt out of features that you don't want. Second, protect your privacy and security. Once you're informed about your device, get informed about these. Be aware of how your personal information is collected, how it's protected, how it's handled and what that means for you. Update it regularly and only buy from secure and trusted sources. Thirdly, avoid communication breakdown. Make sure your IoT ecosystem will intercommunicate and interconnect. And related to that, build a smart home that is manageable, serviceable, and user-friendly. A smart home is meant to make life easier, and energy usage lower, so don't let it burden you. And finally, know your consumer rights and your limitations when it comes to IoT products and services. If you're unsure about your rights, get in touch with ACCAN, Choice, your state Fair Trading Department, or the ACCC.

You can find my full report on the ACCAN website, or you can simply Google it by searching "accan home tweet home" – go and check it out.

(APPLAUSE)

LAURIE PATTON: Please thank Alex. A lot of issues there that I'm sure we will come to in a moment. Linda is up next. While Linda's heading to the microphone, um, I'll just note, ah, for the record, that I'm very pleased to be able to note that we have gender diversity on this panel, which is a really good thing.

LINDA LEUNG: Thanks, Laurie. OK. Right, in the very brief 10 minutes I have, my proposition is that connecting the future consumer is going to be contingent upon, and the responsibility of, service providers. And those service providers understanding the customer experience, being user-centred and human-centred in the way they provide products, services and experiences. In a technology landscape that's becoming increasingly

diverse, the traditional language and discourse around digital divides is neither appropriate or suitable, because it perpetuates these binary representations between haves and have-notes, the included, the excluded, between those who are seen as champions of technology and those who are seen as losers or people we should feel sorry for. Here, we see Roger's technology adoption bell curve. I hope you can see that properly. It shows innovators and early adopters on the left. On the other side, the group known as laggards, those who are right at the end of the spectrum. There's actually an even worse category, known as sloths...

(LAUGHTER)

..non-adopters, people who avoid participation in technology, or they might also be called Luddites. In research terms, much of the attention has been on the left-hand side of the bell curve. On the new and emerging technologies that are being introduced and the early adopters, or the heavy users of technology. So, young people on social media come to mind. So we see in this EY Sweeney report, Digital Australia, from 2014, a lot of stats and infographics, but what they've emphasised is, for example, 1 in 5 people surveyed spend more time on their smartphone than talking with their partner or friends. And up to 23% said that their social lives would be nonexistent without a smartphone or a tablet. So again, what is highlighted is actually a minority – that one end of the bell curve, the heavy users, the addicted users, the extreme users. In last year's Australian Digital Lives Report by the ACMA, to qualify as being part of the 92% of Australians who use the internet, you simply had to answer "yes" to the question, "Have you used the internet any time in the last six months?" This suggests only a small minority of Australians are not using the internet. But if you accessed it once in the last six months, that qualifies you as being an online participant, regardless of your frequency of use, your level of digital literacy, your level of activity, the level of assistance you needed to, um, go online. If we want to advocate for future consumers, we need to look at these reports and similar statistics. We need to look at what they don't emphasise or what they don't tell us. For example, the report emphasises that 92% of Australians – approximately 20 million – of that 20 million, around half go online more than once a day. What's happening with the other half? They're made invisible. Are they going online once a day, once a week, once a month, once every six months...? Similarly, the data clearly shows that traditional desktop and laptop computers are still the most often used devices for accessing the internet. Yet what is highlighted are those who are using mobiles and tablets to do so. So underlying this and other research on digital divides is an assumption that, to be part of the 8%, and probably more, who can't or don't use the internet very much or haven't done so in the 6-month duration of the survey, is to be socially disadvantaged or excluded. There is a small paragraph in the report that notes that age and income were factors associated with never having been online, including older adults, those on low incomes, those who are not degree-educated, and women.

When you look across all those groups, and across other studies of digital disadvantage, all these groups and communities have been framed as being on the wrong side of the digital divide. Now, surely if these are the groups and communities who are laggards, the sloths, Luddites, then it can no longer be considered a minor or minority issue. We're talking about implications for the wider community and consumers in general when you consider that 1 in 4 Australians are from non-English-speaking background – over 1 million Australians are from non-English-speaking background and have a disability, and 20% of Australians self-identify as having a disability. So, future organisations – whoops...

So, future organisations and businesses and service providers really need to interrogate how they think about low participation or non-participation. Is it really something to be pitied, or can we consider it an active position? A demand for proof that a technology be demonstrably useful and meaningful before it's adopted? Or perhaps it can be regarded as a critical stance, one which highlights who's been privileged in the design of a technology and who's been, um, ignored. In other words, the attention needs to shift from the left-hand side of the bell curve to the right, to those who are demanding proof, to the conservatives and to the sceptics. In that same... In the, ah, same report, the um, Digital Australia report, they devised seven categories of online participants. Now, of those seven categories, four would fit that left-hand side of the technology adoption bell curve. They are the natives, the lifestylers, the connectors, the workaholics. So these are the early adopters, the heavy users, the extreme users, the ones who get the attention. The other three make up the more neglected categories, but nevertheless constitute that other end – possibly the other half – of the bell curve. They are the cruisers, the inadvertents and the drifters. So, some might say I'm making quite a claim. That a good chunk – maybe up to half of the population – fall into these three neglected categories. But this is actually backed up by their own data, which indicates that 37% of those surveyed struggled to keep up with the rapid increase in digital device capabilities. And furthermore, 31% cited the government sector, out of all sectors, as having the worst digital

experiences. So what can be concluded from this? I would suggest it actually shows a wilful misunderstanding, if not ignorance, of how people use and participate in technology. We have research and stats and infographics that focus attention on the early adopters and on those who are using the newest, shiniest devices, and what then is overlooked are conventional practices, more traditional or older technologies that are being used. And as a result of that, online services and digital experiences are then designed without consideration to what most of us use, what most of us find familiar, and comforting and perfectly usable. When nearly 1 in 3 respondents are saying that government online services – services that have to be used by everyone and so must designed for universal use and access – are amongst the worst they have experienced, then there is a compelling basis for shifting our attention to that 30% who are struggling with the proliferation of devices in the technology landscape. And that shifting our attention to that other end of the bell curve.

What can we learn from those who don't, or can't, use the internet? Their reasons for being offline. Their alternative information and service-seeking practices, in order to design social solutions to more inclusive online services. It really means critically evaluating how the design of online environments may reinforce the existing age/gender class and education bias, and it means being open to the possibility that this may not be a minority of stick-in-the-muds, but a significant number of us and people we know. How many of us know someone who falls into this 46% of Australians who don't have the literacy skills to meet the basic demands of everyday life and work? Now, that's not people, necessarily, who can't read, but people who can read but have a little bit of difficulty getting through, understanding a newspaper or, um, following instructions on a medicine bottle or figuring out what a letter from the ATO is asking them to do. Now, no amount of digital literacy training is necessarily going to overcome this. So instead of putting, um, the onus back onto individuals for access, with minorities supposedly representing those who are disadvantaged and deprived of devices, the onus must be on inclusive access and service design that considers users as part of a spectrum – a spectrum of affordabilities, a spectrum of literacies, and a spectrum of technologies through which services are accessed. So in short, connecting future consumers will be about service providers acknowledging, accommodating and designing for diversity. Thank you.

(APPLAUSE)

LAURIE PATTON: Thanks, Linda. Kate is next. While Kate is making her way to the microphone, I thought I would tell you a story about my experience with the need for connectivity. A couple of years ago, I was in Melbourne at a black-tie dinner when my mobile phone went off. It was on silent, of course, and it was one of my teenage children who had called me. I thought it might have been an emergency because I knew his mother was out and the two teenagers were home on their own, so I thought I'd better answer the phone. When I did, the response was, "The wi-fi's not working, Dad."

(LAUGHTER)

So we played around, turned it off and on, and got it working do. You think I was thanked? The response was, "Dad, if we didn't have wi-fi in this house, why would I live here?"

(LAUGHTER)

KATE CARRUTHERS: I'm actually sympathetic to that, because I had some young – a young teenage friend – one day I was complaining about how bad the wi-fi is in Sydney, and he just looked at me blankly and said, "Isn't it everywhere?" Because it's in the bus he gets to school, it's at school – he's just in a connected universe. He expects it to be there. And that's the digital revolution that we're living through right now. And we're moving into the Internet of Things revolution. It's going to change because – previous speakers have talked about interacting with the internet as a thing – you know, you go online and stuff. It's going to be woven into the fabric of our lives. I mean that quite literally. So, at the moment, what we've got is this – this is from 2013. It's from the US, but it maps to Australia relatively well. What we're finding is, increasingly, people are not using computers to go online – they are using mobile devices. They are using mobile devices while they're watching TV. Increasingly, they will be interacting with their TVs and things like that. So, that trend has moved very, very fast, and it's going to keep moving. So, les and les people will actually have a computer at home, and this whole notion of getting online won't be a thing – you'll always be online. It will be ubiquitous. It will either be through the mobile phone network, wi-fi, or other emerging technologies, but you will always be connected. This is going to be a fact of life in the future. Our house will become fully connected. And it will be something that – everything

will be. This is a diagram from a company that's actually making this stuff in the Philippines. So they are building connected homes. We are starting to see the 3-D-printed homes with electronics built into them. So we're already moving fairly fast into a world where always-connected homes are a thing. This is something that we are seeing now – that we are having... You don't subscribe, you won't have a smoke alarm put in, it will be part of your house. It will report back. So we have things like the nest, which is a thermostat. What it means is companies are needing to change the way they provide support for the products that they're putting in. So in the past, you used to be able to build a thermostat and ship a thermostat and sell it to people who'd put it in their house. Now, you need to be able to update the thermostat's firmware with the latest version. We have Philips Hughes light bulbs which need the firmware updated, which you need to be able to do through your mobile phone. We're increasingly seeing things like this. This is leaving us open to security issues. When I talk about the Internet of Things being woven into the fabric of our lives, I literally mean woven into the fabric. So we have things like this fabric here and, increasingly, it's going to be literally woven into your fabric of the clothes you wear. There is already prototypes of this type of fabric. It's doing things like monitoring your health and wellbeing. It's reporting on your exercise. So you won't be wearing a smart watch, necessarily, to do it. You'll be wearing smart clothing in the future. The smart clothing will be reporting back on you. Just think about this – insurance will change. Because you won't need a bunch of actuaries sitting around calculating the risk of you doing X, Y or Z, because they'll be able to work out the risk of you doing X, Y or Z in real-time based on real-time feedback from what you're doing right now. So, we're moving fairly rapidly into a brave new world. This technology here is interesting. This is an ingestible. So, not only are we talking about implanting devices into the body, but also taking and swallowing devices so that medical tests can be done, so they can track and treat health conditions. This is a prototype from MIT. It's going into production next year. The real issue with a lot of this stuff is that it is ubiquitously connected and it's very insecurely connected. This is going to be an emerging issue for us. It's already starting to emerge with all of the things that are in your home, so if you have one of these wi-fi-controlled light globes that change colour, I can hack it, so can many other people. And it's probably on the same wi-fi network as you do your banking at home. So there are real issues emerging. This is something, also. The Jeep was hacked last year. Some hackers remotely killed a Jeep driving down the highway. As we move into autonomous vehicles where they're self-driving, the connections with the car and the car-to-car connections... With autonomous vehicles, we will have cars talking to each other. Without us involved. So the cars will be driving along and they'll be talking to all the other cars on the road. And at the moment, if you have one of the self-driving cars, you actually have a variety of security vulnerabilities built into it. They're actually built into a number of existing, non-autonomous vehicles as well, but they're less of a risk with us at the wheel. The other thing is, increasingly, we are seeing the connected home as a vector for attacks. This is a case in America where the baby monitors – they had the baby monitors so that the parents could listen to the child while it was sleeping. Hackers hacked into it and were yelling obscenities at the child. So, everywhere in the household is going to be at risk. The other thing that you may not have thought of is, as we move to electric vehicles, we'll be subject to Digital Rights Management. I drove an electric car at a conference a couple of years ago. The one thing I didn't realise was the battery is on Digital Rights Management. If you didn't pay your bills every month, that car won't go. They turn it off. They don't turn it off while you're on the highway, they turn it off when you pull over and park, but you can't start that again until you pay your bill. Now, let's transpose that into your implantable device, like a pacemaker or your insulin pump, and you're behind on your payments. Potentially, you could have it turned off. So these are the real issues that are facing us. This means that the companies that are shipping these devices are going to have to start thinking about how they support them, how they monetise them, and how you – as consumers – are going to respond to some of their demands. So it's really interesting to think that we've got all of these connected things, and they could be fabric and ingestible, implantable, whatever – there are a whole raft of issues with them around security and personal information. The interesting thing that I'm involved... I'm involved with the data analytics centre for the NSW Government. One of the dawning realisations with us is that de-identified data, the more data you have, the less easy it is to keep it de-identified. So it more and more data that we get, even if we have de-identified it, it's really hard to keep it that way because you can zero in on individuals. We are really working on that at the university. These risks to personal information and privacy are real. The points that Alex made about being informed about what products that you're using – that's really hard. Because who reads the end-user licence agreement when you download an app? Or you put a thermostat in your house? Or the TV can listen to you that's got the voice recording on by default? All of these things are real. They're happening. And it's really almost too much for an individual to keep up with. So, these are the challenges that we're facing. We're going to have to come up with some solutions. We don't have any yet. Thank you.

(APPLAUSE)

LAURIE PATTON: Thanks, Kate. Please thank Alex, Linda and Kate for their presentations, and let's move into a bit of discussion. Who in this room has a Fitbit? Does it not bother you that every piece of information that goes into that machine goes off to somebody in the company that owns it? And do you know that that happens? Do you think most people who have a Fitbit are aware of that? That's a question that I think we should just dwell on. Look, I'm a bit obsessed with the Internet of Things. I like to call it the Internet of Opportunity, because I think it is going to give us so many avenues for both economic development and social development. The first question, though, to the panel – what is the biggest risk?

KATE CARRUTHERS: Initially, I think there's issues around, um, Digital Rights Management on devices, especially devices that are inside of us or inside of our, um, vehicles and things. Because they can be held hostage for payment. So if you get a pacemaker and it has Digital Rights Management, they can turn that off. And you can die. There's real issues like that – that is a right that companies have now, to just say, "We're going to unilaterally stop this service." There's no consumer protections on this stuff.

LINDA LEUNG: I think there's risks to adoption. These particular concerns around privacy are very real risks to adoption. And, um, I think when service providers have that level of control, then we get to a point where, um, and we do see it now, what I call platform discrimination – that is, there is an expectation that, um, that this is available and you have access to it, and therefore other services are reduced or eliminated altogether in anticipation of that. And therefore, whole segments of consumers are no longer served.

ALEXANDER VULKANOVSKI: Yeah, I think I agree with Kate. I think privacy and security, as I noted before, are probably the two biggest consumer risks. If you – one of the things which I concluded in my report is that, if you weigh up the opportunities and risks for both consumers and industry, industry tends to have a few more benefits in that they can automate things, they can make things a lot more efficient, and they're generally better prepared for these kinds of risks, such as privacy and security. With the consumer, other than a few specific case studies, a lot of the benefits to consumers are quite novel. So, like I mentioned, the Fitbit telling your espresso machine to do this or do that – most of it's fun and games. But the security implications are far more severe. If everything in your home is connected – including your locks, including your toaster, all these things – not only can this data be compromised from a privacy perspective, but these devices can be controlled remotely, either locking you out of your home, locking you into your home and then...the rest is all up to your imagination.

LAURIE PATTON: I'm always of the view that there's not much point in pointing out problems if you don't come up with a solution. I'll open this up to others to talk about in a second, but just very quickly, if we could just...fast-forward. We're here next year. What should we have done, as individuals – what should ACCAN, Internet Australia – what should we do over the next 12 months? Because this is an issue that is just starting to come onto the radar.

ALEXANDER VULKANOVSKI: That's a good question. I think a lot of it comes down to, if consumers are informed – and I know it's hard to be informed, but it doesn't necessarily have to mean going through and meticulously reading the terms and conditions – it can very much just be knowing how devices operate. If your smartphone, you know, can change its screen display, it's good to be aware that that's as a result of a sensor. I know that's probably naive coming from a millennial, but it's about – once consumers get informed, they can make informed decisions. Once they make informed decisions, the market has to respond. I believe the market will be the quickest responder and the most effective respondent, second, possibly, to the public sector.

LINDA LEUNG: I would say the flipside of that is educating service providers around being customer-oriented, and the consumers that aren't being served.

KATE CARRUTHERS: I think that there's a real issue with education of start-ups, especially. A lot of the time they do things just because they can, and they can monetise them – not because they ought. And they're not always aware of privacy legislation, they're not always aware of consumer protection legislation, and then there's the jurisdictional issues. If you're consuming services provided in America, you're consuming under the terms and conditions that they offer, even though you personally are covered under our consumer protections. But they're very hard to claim from here, so trying to get harmonisation in global privacy – which will be never happening... We can't lose hope on that and trying to understand what the risks are.

LAURIE PATTON: I once wrote an email to Microsoft saying," Please find attached my marked-up copy of your services agreement with my suggested track changes." I didn't send it. 'Cause you don't get much choice. Do we have another microphone, or do I have to... Just wanted to make sure.

>> I hear you talk a lot about service-centric design. It comes with a special app that has its terms of service agreement and its way of providing you access to that device via the web, and the company controls it. That is essentially a firmware issue in how the firmware and the security of that firmware relates to a device and, indeed, perhaps standards involved in the device itself that allows you to control that device. I wonder if there's investment activity whatsoever in developing alternatives that are human-centric types of firmware in Australia that you're aware of at all?

KATE CARRUTHERS: There's a fair amount of standards development in the Internet of Things space, but it's more at the interoperability and protocols level than that sort of service design perspective.

LAURIE PATTON: Just probably worth noting, at the moment, that just recently, we – using the collective – have created the Internet of Things Alliance of Australia. It began, I think it'd be fair to say, as a bit of a discussion between a number of groups, but largely the Communications Alliance. ACCAN is involved, and Teresa is involved, as am I. One of its tasks is to look at setting standards, but without offending anybody associated with it. The danger is that it's going to be very much vendor-based. So I think there's a real role for consumer groups to get involved and make sure that we actually do have people thinking about the downsides.

>> Hi, Nigel Waters from ACCAN. I'm going to tell you a little bit of a personal experience. Is Alan Copeland still here? He's gone? Anybody from Choice? Because this will end up with a request to Choice.

TERESA CORBIN: Xavier's down the back!

>> OK. Two months ago, I bought a smart TV. I looked at the Choice comparisons – lots of useful information about the different features. Nothing about the privacy settings. I switched it on, got it to work – eventually; no 13-year-olds around to help – and I found that I basically had to accept the terms and conditions before I could use it. The terms and conditions had a terms-and-conditions section, but also a privacy policy, which I started scrolling down and the tiny print I eventually gave up on. I did get to the stage – and I'm supposed to be, I guess, the most privacy aware person in the room – I did get to the stage of actually going online and eventually getting off the website a printed copy of the privacy policy. Two months on, it's still sitting in my "pending" tray, waiting for me to read. So I've got no idea what I've signed up for. What would have been really helpful is if Choice, as part of their comparison, had actually looked at the privacy settings and rated the different smart TVs that were available on that feature as well. So...

LAURIE PATTON: I think we will take that as a comment. Please thank Kate, Linda and Alex. I'm sorry, Teresa, I stole two minutes.

(APPLAUSE)