JULIE McCROSSIN: It is my pleasure now to introduce our panel. This session is called: Do we need a connected life? We are asking our three panel members initially to reflect on both the benefits and the challenges of a connected life and also, perhaps, get some vision from them of what the future may hold. Katina has just joined us, we have a competition running. There is - what are they called? - drone as a prize. You might want to enter this competition for the most interesting, thought-provoking or fun prediction of what may be ahead. We had an earlier video with The Jetsons intercut with Richard with actual devices in the Jetsons. It was a humorous comic... Okay! I will introduce people one at a time. I will start with Greg Killeen. Greg is a senior policy and advocacy officer with Spinal Cord Injuries Australia. Do you want to make some opening remarks about benefits and challenges and then he has a surprise for us. Take it away.

GREG KILLEEN: The benefits of a connected home?

JULIE McCROSSIN: Have you got - can you speak up?

GREG KILLEEN: I don't project my voice very well so if you can't hear me, yell out from the back, okay? Some of the benefits and issues, I think, obviously the benefits of being connected is that there is not really an option of opting out of being connected if you want to live in a civil society and participate in the social and economic life in the country because, whether you like it or not, a lot of being connected is often being driven by service providers and the banks like online banking and having to pay bills, they charge you for hard copy bills in the mail if you don't get it online.

JULIE McCROSSIN: Can you speak up a bit?

GREG KILLEEN: I will try to. Can you hear me in the back?

JULIE McCROSSIN: Wave if you want.

GREG KILLEEN: Sorry. They are obviously the benefits of being able to do banking, booking holidays, you know, paying bills, those types of things in connecting with family, friends through social media, file-sharing images, all that sort of stuff is available online which wasn't really available many years ago. The challenges? Well, if you are totally reliant on the net for things like Smarthomes and stuff, which requires the internet to be used to connect to your home and operate the appliances and the lights in your home, if the net goes down, well, what do you do? Particularly if you are totally reliant on the smarthome technology. That would be the issue.

JULIE McCROSSIN: Can I ask you, I know you will show us something of your life in a moment but how long have you been, in a way, developing your own smarthome? We just had a presentation from Telstra where we saw both what's happening and what's to come?

GREG KILLEEN: I have been using smart technology since I planned a work-activated home control system in 1994. When I see all the new innovations, it is like everything old is new again. I think it's great having innovation and using all the different platforms but my situation is called The Simplicity from America. It is a stand-alone shoe box. It is connected to the power, it uses infra-red-control devices as well as a protocol called X 10. There is no rewiring of the house. Plug in modules in the light switches, if you want to plug in a fan or a radio, it will turn them on and off, or the infra-red devices. It controls electric bed, door devices. Operating curtain tracks, air-conditioning, it has an in-built telephone. I have been using this stuff for many years. It is just as important to me as my power wheelchair is for my mobility. It gives me autonomy, spontaneity, self-esteem is greatly increased because I can do what I want when I want, don't have to be reliant on people. It is a big part of my life, actually.

JULIE McCROSSIN: Do you think it would be good to have a look at the video and open up questions to the audience? You are, in a sense, living the future.

GREG KILLEEN: I will pre-empt it by saying the system is made where it is listening all the time. You have to prompt it by waking it up with giving it a name. The more sill syllables in the name, it is harder to trigger. My assistant called Geronimo. It has a male American voice. I did call it Priscilla for a while.

JULIE McCROSSIN: Why Geronimo?

GREG KILLEEN: I have no idea. My father used to watch a lot of Westerns. Four syllables, that's it. That's what I kept it as.

JULIE McCROSSIN: Will we have a look now?

GREG KILLEEN: Sure.

JULIE McCROSSIN: I want to see the Internet of Things going.

VOICEOVER: An environmental control unit can bring you more choice, privacy and spontaneity. Many users claim the potential is under-estimate ed. They are great reliance on family and allowing you to use your attendant care time better. Operate your television, phone, front door, heater or any other electric appliance from your wheelchair or even in bed.

GREG KILLEEN: The use of the environment control system not only provides me with my own independence, it frees up the time not having to rely on other family members who might be at home at the time. Geronimo?

>> Yes.

>> Light three shut off. The environment control system operates lights and appliances using X 10 modules, which plug into a standard power point. They are given a number. Each light or alliance is given a separate number and when you nominate that number through the environment control system, it will turn it on and off. Geronimo?

>> Yes.

>> Television. Turn on. Television. Volume. Up.

>> Curtain. The environmental control system not only makes it easier for me to operate things and operate things that I actually can do, it makes it easier to do that and it makes it possible to operate appliances that are out of my reach. Phone call. Dial the number. 9.

>> 9.

>> 6.

(phone rings)

>> G'day, Tanya, it's Greg here.

>> Hi, how are you going?

>> I also use the universal eight-in-one remote control which is not a disability-specific remote control, it is an off-the-shelf product. As each TV and video all comes with their remote controls including air-conditioning and other devices, this can replace them by programming this so you just have the one remote control instead of six others and it also operates the X-10 modules using radio frequency to operate lights and appliances. Dial new mail message. Hi Corinne, new paragraph, just letting you know the restaurant has been booked and I'll see you tomorrow. 6pm full stop. New paragraph. All the best comma, new paragraph regards comma new paragraph Greg. I have two electric door operators. One for a security door, one for a wood door. The standard pendant is a small operator like this. If you have difficulty controlling it with this, you can get an adaptor controller which has jelly bean switches. As I've got two doors, I've got two jelly bean switches and these can simply be put into a much closer position to make it easier to use and put the controller in a different place. I can also control the doors with the environmental control system as well.

JULIE McCROSSIN: Can you give that a round of applause?

(APPLAUSE)

JULIE McCROSSIN: I'm going to come to the other panel members but are there any questions or comments on what you've just seen? I will just whiz over to you. Can you hold your hand again?

>> My name is Phillip Montecello. I'm a volunteer teacher on STEM robotic to a primary school. My question is how do you balance innovation against security? A classic scenario, I could go to the internet, buy a $5 device and $3 worth of wi-fi system and then $11 worth of IP camera and then put them together and put a program and then what happened then is I could go to the internet and register using a dynamic DNS and for me to cover my track, I will pay them with bitcoins. Effectively now I have access to the device that could run through internet, through my mobile phone. That's innovation but it's also a problem for security. What sort of procedures do you have in place to ensure this thing doesn't happen?

JULIE McCROSSIN: You are clearly a smart man, what would you put in place to stop you? Is it required to stop you?

>> Well the question is because, effectively, this is all available. You could register using dynamic DNS and create a controller using a $5 device and then continually update that DNS which effectively now have an IP address I could access externally via the internet. As I said, because you can always pay it with bitcoin, no-one can track you how you do it. So the question is what sort of procedure? For me, seems to be a question mark for me how you will put the procedure against that. That's an open system.

JULIE McCROSSIN: If I may, if you could hand the microphone to Professor Vijay because I think he was talking about these issues. How would you respond to the question?

VIJAY SIVARAMAN: I think that's a tough question in terms of - to what extent does security stifle innovation? That was the crux of your question, if I understood it correctly. I don't think there is an easy answer to that. On the one hand, you'd say innovation means you have to reduce all the variables possible. On the other hand, consumers need to be protected, especially those who are most vulnerable. It requires a combination of action by consumers, something that ACCAN is doing here, regulators, policymakers, insurers and manufacturers too to have that dialogue. There is no one universal answer because the costs are different for every IoT even. Take an analogy of cars. Still a certain date, seatbelts were not mandatory. Until then the convenience was more important than the safety and security but why it matured to a certain stage, seatbelts were mandated, every car needed to have seatbelts because consumers had to be protected because cars had matured to that stage. Is IoT at that stage of maturation where we have innovation now, let's focus on maturity? Or is it still in the early days where we let more innovation happen and safety and security can wait a bit longer? I don't know. There may be no one answer to it. It's a complex question.

JULIE McCROSSIN: I will introduce Professor Katina Michael from the Faculty of Engineering and information Sciences. How would you respond to that question?

KATINA MICHAEL: I would be really considerate of doing a threat analysis of the potential dangers, especially where we have vulnerable people of any type. I'm talking here potentially and mainly about prosthetic devices in the home. There's a big push at the moment by service providers and manufacturers to connect these devices through the Internet of Things, brain implantables, pacemakers, so there is a constant feedback loop coming in the product life cycle management system which says if there is a cyber security threat - Two weeks ago we heard there were 750,000 pacemakers of St Jude vulnerable, now owned by Abbott, to cyber security threats. Their response, if you are asking me for a response, I will talk about the ones that I have seen, the industry response was, "Those people who have these types of pacemakers, please visit your specialist and get a firm ware update which would happen through a wand which would be waved in front of the pacemaker and information would be uploaded to the pacemaker". If we take that one step further and we have an Internet of Things scenario where prosthetic devices can be updated like the information on the smart TV, you can imagine the potential for predatory hacking in the sense where interference issues of an electromagnetic nature could muck around with the prosthetic device or even the household system. So I'm seeing a repurposing, and as Greg rightly said, these technologies have been around since, well, early '90s, I worked for a company called Motor Networks that was based in Canada that was running a French and English translation system for voice and interactive voice recognition so we know the systems were available and house automation systems were available but the repurposing is for everyday things. We are seeing companies like Amazon launch their Alexia conduct...

JULIE McCROSSIN: What's that?

KATINA MICHAEL: Cylindrical device where you can do voice-activated searches on the internet. For example, keep lists or ask the device to play your favourite songs. The commercials are interesting. The device costs $300, you could put one in every room. We have devices like the Google Nest device which was purchased for $3.2 billion 3.5 years ago, the drop cam system, a purchase from Google is being. A poster said it is lovely somebody is watching over your home or you can do it from work over your mobile phone device. This is a fine line between wonderful innovations that support Greg in the prosthetic way we can definitely commercialise them further so we can all enjoy these things. I would, however, suggest that things that we are dependent on to open doors, whether it is in vehicles, whether it's in houses, are not on the grid, are not on the internet because that opens you up to attack.

JULIE McCROSSIN: Can you outline what might be the risk of such an attack? If we were outlining key challenges as we move forward, it might affect the ordinary consumer, can you outline what are the concerns?

KATINA MICHAEL: First is corporate social responsibility for ensuring that the data that you share is kept secret. I'll give you an example. You know, in that search box that we think nobody reads, and we enter things like "depression", things into there like "very bad flu" or "husband cheating on me" or "divorce" or "litigation" or "civil court proceedings ‑ how much does it cost to do A, B or C?" I could let my mind wander, and a lot of us do a lot more in that search box than we imagine. I want you to think about something for one second. When we're typing, it's a very controlled thing. It's limited. When we're speaking, we say a lot more. You can see the screen on the left‑hand side here, that is replicating everything I'm saying. In the future, with applications like Dragon Anywhere, it's this kind of application but anywhere ‑ so I have it on my mobile device, my voice biometric is stored in the cloud, and I want you to think about future surveillance cameras ‑ you're going about your business, having a private discussion in a public space, which a lot of us do during lunch breaks, and it's voice‑activated... Your speech becomes text while you're roaming in public. Maybe I said the word "fertiliser" and maybe I said the word "bomb", but in a joke, and nothing to do with terrorism. My concern is that, once we start placing IoT devices in public spaces ‑ and they're already there, by the way, doing behavioural biometrics and other things ‑

JULIE McCROSSIN: Give us examples of where they are.

KATINA MICHAEL: Toowoomba local council, which has behavioural biometrics. Councils are now investigating the potential for CCTV to record ‑ but beyond recording, looking at scenes like, if someone drops bag and then leaves it unattended, or facial recognition, in particular in these systems, which look at hit lists, for instance, if you're a suspect in a case, if you're a person on a list that's wanted for questioning, potentially you can match against this list. These technologies are here today. I'm not telling you something from Minority Report ‑ I'm telling you about companies locally here in Sydney ‑ in Chatswood ‑ that have this capability. I want you to think about your privacy, the privacy of your home, and weigh that up against convenience, then ask yourself a very important question. How much more secure am I by these technologies monitoring my house 24/7, as opposed to not? Haven't we all lived since day zip without these surveillance cameras constantly monitoring our home locations 24/7? Haven't we gone around for the longest of times without wearable devices like this, or phones, or smartphones? Incidentally, I forgot my phone at home ‑ worst day for me to forget my phone ‑ but I had an interesting feeling walking through from Central Station this morning, which was, "I don't have something that everybody else has." And I'm an alumni of UTS but I couldn't remember, from memory ‑ I had been to the Aerial Building previously, but I couldn't remember... Am I better off or worse off because of all of this tech?

JULIE McCROSSIN: You're posing it as a question to us as if you're King Canute, the king that tried to command the sea to go back. The flood's on. I suppose ‑ I will open to questions ‑ I've been asked to do an interview with each person, then I'll open to questions and comments from the floor. I guess the question I'd like to ask you ‑ what are the public policy challenges that those of us here interested in being active in this space need to be bringing to the public in the democracy to discuss to our community leaders? Because it's ‑ one level, it might be advisable not to use the words "bomb" and "fertiliser" anywhere... But what are the public policy issues that we need to be thinking about and becoming active about to stand for the public good and consumer rights in a scene that's changing so rapidly?

KATINA MICHAEL: I use Greg as great example here, because his devices, for me, are life‑enhancing and lifesaving.

GREG KILLEEN: And it's not connected to the Web.

KATINA MICHAEL: It's not connected. In fact, most people with brain pacemakers tell you they never want their brain pacemakers connected to the Web. When your system is not working ‑ what happens?

GREG KILLEEN: It's only failed twice in all the time I've had it, and it's been, um... ..and it's currently working fine, except it takes two microphones ‑ one on the bed and one on the desk ‑ and the input for the one on the desk is not working, so the voice input module is faulty, so I need a new one.

JULIE McCROSSIN: Just speak up again, if you can.

GREG KILLEEN: There's only been two problems I've had. On one occasion ‑ because I'm not supported in Australia ‑ it took me a month to get it fixed. And so that was a very long month.

JULIE McCROSSIN: What's your emergency backup if you're alone?

GREG KILLEEN: I've now got a smartphone which ‑ it's set up with a switch which allows me to make phone calls and send text messages, and ‑ yeah. I'm also using it now with an app to control all the infra‑red devices so I don't have to get all the different remote controls to operate the different TVs and stuff at home as well.

JULIE McCROSSIN: Is it expensive?

GREG KILLEEN: Which ones?

JULIE McCROSSIN: Everything.

GREG KILLEEN: I was lucky enough to have the Simplicity ECU given to me back in 1994. I actually don't know what they cost. I've tried to get an estimate, because I would like to bring them into the country. Particularly with the rollout of the NDIS. I see a lot of potential for a lot of people to benefit from this, as I have used them for so many years. But it's difficult to get the company to consider it being brought into Australia.

JULIE McCROSSIN: I'm not telling you anything ‑ poverty is the biggest disability of many people with disabilities. I've got a friend with disability, but she's got money. It's all about money, isn't it, in the end?

GREG KILLEEN: Look, I don't know. I mean, people say a unit is expensive. I say, "Expensive in relation to what?" At the time, the system might have been worth $10,000 installed in 1994. It's been operating 24/7 since 1994. When I'm in bed and I require to be able to access the phone, open the door to let people in, turn on and off the air‑conditioning, make a phone call, open the curtains ‑ all these things, I can't physically do... You ask yourself ‑ well, what's the cost of NOT having it?

JULIE McCROSSIN: So what are the public policy questions, Katina, that we need to be asking in the years that go along to have some co‑design‑and‑trust capacity? Close to your mouth ‑ the reproduction's on the top of sound...

KATINA MICHAEL: The first thing is I would not connect things that don't require connection. I think we're all on this bandwagon that technology's a fantastic tool till kingdom come. The first thing we have to step back and say ‑ it's an innovation game. Of course it is. That's how companies create economic change for the positive in a nation, in a sector. But how much of this do we really need, and in what aspects? I'm going to say something ‑ I think it's brave. Everywhere we need technology, we don't have it. And there are teachers in high school systems that are teaching blind kids ‑ the kids have no access to the technology they need, and that is available today. I point them to the ACCAN site. I point them to the University of Southampton that has excellent resources. But the teachers have no training. Or limited training. There was somebody I met in the States that had an apex machine from the '70s. And then she said, "Kat, ever since I spoke to you, I learned about the iPod and the iPad and all of these other tools." So where we should be really concerned, in a social sense ‑ we're not doing it. We're just too busy creating even smarter homes. I think the smart public policy issues is about how smart we really want smart devices to become. Do I really want them diagnostically to track me everywhere I go? Do I really need the 15 different sensors in the products that I sell because I can, and because it's cheap, and because the component unit comes with it when I assemble it together? So I was asked this very question by IEEE last week ‑ there's a blog post coming soon ‑ about what we do. I'm not saying "Regulate this space." You're never going to get companies like OzSpy in Australia to get less devices like key fobs with cameras on them and audio recorders and location trackers ‑ you're never going to get these companies to buy less. And consumers will just buy more. And mostly, they buy more not for convenience, but for nefarious purposes ‑ tracking whether their wife or husband is cheating on them. Maybe that's not so nefarious, you know? It depends who you are and what context you're in.

JULIE McCROSSIN: What if it's your husband?

KATINA MICHAEL: What if it's your husband, or what if you're the victim of a domestic violence attack? We did learn very recently 98% of women suffering domestic violence are suffering tech violence. 98%.

JULIE McCROSSIN: We've already had a little bit of discussion about that this morning, Katina. Do we know of any models anywhere in the world ‑ and I'll ask you this too, Vijay, if I may ‑ I'll start with you, if I may... I'm basically looking, do we have any models anywhere in the world of a comprehensive policy response to the use of these technologies in the domestic sphere with domestic violence? Because that's such a major capacity. Do we know, is there any information to share?

KATINA MICHAEL: We've responded to these situations by creating Amnesty International ‑ had done so in 2008 for women, looking at safe homes, alerts in the home. Just like we have, perhaps in Greg's case, a voice‑activated home, we might have a home that can at least protect you in a room. So it's a safe room in a home. Mind you, it's a lock‑in, not a lock‑out. There potentially could be lockouts ‑ amnesty, we're talking about strategies at the time of how women can prepare and move on ‑ or men, for that nature... But we need to create these. I mean, the only amendment I've seen is to the Northern Territory legislation, which says, "Law enforcement can film women if they've been victims of domestic violence so that bruising or other things can be kept on record." At the time that a call‑out is made by the police...

JULIE McCROSSIN: Yes, I think that's happening in a number of states and territories. I'll come to this gentleman, then to you, Vijay.

>> My name's Gerard Brodie with the Consumer Action Law Centre and the Consumers' Federation. You say that you can't regulate these businesses, so what can be done? Is the responsibility on us to protect ourselves? Is there something to stop I guess, the onslaught of surveillance, which seems like it's never‑ending?

JULIE McCROSSIN: Do you want to go first, Vijay?

VIJAY SIVARAMAN: I'll start by saying that I'm not a policy person, I'm the technical nerd who plays with these gadgets. That said, it's a complex area. I don't think there is a simple area. I'll not very qualified to answer on the policy side, but there has to be some consumer education on the products they are buying and using and how that data is being used. There has to be some kind of regulatory oversight of what is happening. Unfortunately, that's not easy, because technology is moving really quickly. And even as we were doing the project ‑ certain firmware changes the posture of these devices. Lastly, I think there could be a role for insurance so that you don't pre‑emptively stop stuff ‑ to some extent you do, but not everything. When bad things happen, there has to be some clampdown of liability around it. I personally think there has to be a combination of these various stakeholders somehow coming up with solutions that can keep pace with the change of technology. But again, this is not a concrete answer that we can all go on action right away. It's going to take some work.

JULIE McCROSSIN: I'll come to the panel members, then to the audience if you have something.

KATINA MICHAEL: Gerard, we've met for the consumer federations of Australia previously. We have laws ‑ surveillance devices acts, workplace surveillance acts, the Privacy Act, the ASIO Act... A lot of Acts. Telecommunications Interception and Access Act. What we find, however, in most cases, is that the Acts are there, but they're not really enforced. And here's the conundrum ‑ that our own law enforcement is possibility in breach of some of the laws we have in Australia. So how can they enforce? How can we enforce if our own law enforcement is depending on breaching these without warrants on occasion? And you might come and say to me, "Tell me about one case." Well, for those of us who know, there are lots of cases. You just have to go back. Now, there are penalties for people who are found in these situations, but there's a chasm between laws and regulations and the enforcement of these laws and regulations. Until we make examples of where this doesn't fly, then it'll just keep happening. Labelling is a good example ‑ I visit lots of websites in my research, and most of them say "Buy this product, but please understand you are responsible for the state that you use it in." It reminds me of the time I had a Google+ exchange with one of the makers of Google Glass. Somebody had taken the Google Explorer device ‑ when only 1,500 or so people had it ‑ and gone to Europe. And I said to her, I think her name was Sarah Price, "Sarah, somebody's just taken the device and is filming in Europe where there's massive data protection laws" she said, "Well, that's their problem. They're breaking the law, not us." I guess she had a point. Her terms and conditions, or Google's terms and conditions, stated A, B. C. OzSpy states A, B and C for the products ‑ make sure you use them when you're supposed to and it's convenient. But it's hard not to. It's very hard to police covert devices and unobtrusive devices that you can't see. Increasingly, our panels will become smart. Our lighting will become smart. Cameras will hear, not just see. And so, what do you do? I didn't mean to sound like King Canute ‑ yes, the floods have come and the horse has bolted, so to speak, but actually, as a community ‑ as a society ‑ we should be talking about these issues more, raising awareness of them.

JULIE McCROSSIN: Katina ‑ I'll remind everyone what we're talking about here is the benefits and the challenges of this highly connected life, and particularly going forward ‑ what are the policy issues or actions we can be taking part in for both individual consumers, but also at a public policy level? I'm going to come to some people in the audience, if I may, and then I'll come back to the panel. Do you want to introduce yourself?

FRANK ZEICHNER: Hello. My name's Frank Zeichner from the IoT Alliance in Australia. We represent about 330 organisations, and we care about not only the distribution of IoT through the economy and society, but also responsible and trusted use. To shine a positive light on a huge problem ‑ we have a work stream both on data privacy and a work stream on security. On the privacy side, it's evident that not only are the legislation and acts in the various states and federal areas not aligned, but they're poorly understood and they're not understood well by consumers and they're not even well understood by businesses. Part of our role is to try and get that information out in the simplest possible way. We're produce guidelines to do that. And I think we ‑ it's only by agglomerating our common views across broad communities that we can make a difference. And so, we're trying to lift the industry part of that, and we want to be in that conversation, because it's only when it's trusted that it'll be successful. On the security side ‑ and I'll be mentioning this later in my panel session ‑ we absolutely believe that it's so complex that consumers need simple devices to recognise whether something is secure or not. Not just "Here's a list of 10 principles or 50 things you need to do," but, "This is a device that has gone through some accreditation." It has a mark, or something. These are... ..I actually think they're opportunities for Australia, to tell you the truth. I think we could be branded as a secure country in advance of those overseas. Because the legacy we've inherited from the Wild West internet days is the one that we can't afford to continue on with the Internet of Things, because then the problems will just multiply by another order of magnitude.

JULIE McCROSSIN: As an outsider, the two things I'm hearing in my head are the trust rating ‑ that's already been mentioned ‑ as a way of helping consumers have some sort of trust rating around their degree of security, and also the role of the insurance industry. Do we have anyone from the insurance industry here? No. Might be interesting to have speakers. If you notice, people keep speaking about the role of insurers, as an outsider, too, IoT ‑ I had to check what that acronym stood for. This is a conference, obviously, with some very sophisticated people, but we're also inviting outsiders ‑ students and so on. Just, if I could ask people to unpack their acronyms, even if you feel they're obvious to you ‑ it stops me from having to interrupt you. But the Internet of Things... 12‑year‑old kid ‑ never heard of it, curious and reasonably bright. What's the Internet of Things?

FRANK ZEICHNER: The Internet of Things is the network of data that's generated through sensing anything and everything, and how it's then used. So, how it's collected and shared and analysed and used.

JULIE McCROSSIN: Who'd like to have another go?

(LAUGHTER)

My 92‑year‑old mum is a really intelligent woman, but she wouldn't ‑ that doesn't... It's just interesting, isn't it? So conceptual. I used to be a community educator in a legal context, and if there's one thing I learnt ‑ most people don't think conceptually. What's the Internet of Things? Who wants another go? I love it ‑ he's at the back of the room. This is good, because incidental exercise reduces my mortality...

(LAUGHTER)

>> Yes, good morning. It's using the internet to connect a whole bunch of devices. It's as very simple as that.

JULIE McCROSSIN: Thank you. One more definition ‑ what's the internet of things?

>> May I have a go?

JULIE McCROSSIN: Please.

VIJAY SIVARAMAN: I'm a very visual person ‑ it's a bunch of gadgets ‑ your smartwatch, your kettle, it's connected and monitored and controlled from everywhere.

JULIE McCROSSIN: Is it a gore good or a bad thing? Vehicle as an academic, I'll never say black or white ‑ there are always shades of grey. There are many good things it can be put to use to.

JULIE McCROSSIN: Imagine you're on the ABC and you're talking to the general public and they've never heard of it. What's the good thing about this Internet of Things?

VIJAY SIVARAMAN: Simple example ‑ let's say I'm letting out my property using Airbnb or something, and I want to open the right go when the right guest comes by. I don't want to physically open the door, or leave the key under the map. Through the app, they signal they're there, and I unlock the door based on a code I send them while they're standing there. That's one simple use case of how an interconnected door lock can help me manage my property better.

JULIE McCROSSIN: Examples work. What's another one?

VIJAY SIVARAMAN: A smoke alarm, you mentioned. If it detects smoke, it sends me an SMS message, no matter where I am ‑ at work or wherever I am. I know that there's smoke in the house, then I can investigate why that happened by accessing my video camera, seeing if there's a fire blazing or something...

JULIE McCROSSIN: What's this academic from Wollongong on about? What could possibly go wrong?!

(LAUGHTER)

KATINA MICHAEL: What if we added to this definition? You asked me in the beginning where I see this going ‑ it's the internet of us, the internet of you. You're not a thing, by the way, you're a person. But you might be just a thing on the network in the future, equal to the microwave oven that's connected to the toaster ‑ that, by the way, if hacked, could burn your house down, and then your Nest could let you know if there's smoke... But that's what we're talking about ‑ the internet of us. Please don't think, if we go down this track ‑ and we are already down this track ‑ that we're not going to become embroiled in that web as a subject. And an object and subject will have, perhaps, different gravity levels and different types of ID, but what if we were all just things?

JULIE McCROSSIN: Just spell that out for me a bit more, the distinction between the Internet of Things and the Internet of Us, and which term to you promote we use if we're trying to raise public/consumer awareness?

KATINA MICHAEL: I think Internet of Things is the correct and original term, as coined by Kevin Ashton working in 1999 at Auto ID Labs at MIT. Internet of Things and People has developed. The Internet of Us, I've been talked to a keynote in a few weeks at RADCON, the Radio and Communications Group. Whether that develops into wearables or luggables or an NFC pendant that's currently being used in some places in India for health inspection of young babies, for instance...

JULIE McCROSSIN: NFC?

KATINA MICHAEL: Near‑field communications. That's pretty much similar to RFID ‑ just does different things. So... What if we had embedded technologies? Then you just didn't need the embedded technology for prosthesis, but you opted for one for convenience? You didn't need keys ‑ you didn't need to carry tokens like Opal cards ‑ the next talk I'm going to this afternoon is with Meow-Meow, who implanted his Opal card into his body, then was fined because the inspectors didn't acknowledge that the chip in his hand actually carried stored value, even though it did and it was scanned. So it's very interesting where we're going, and I'd love not to carry keys, perhaps, and I'd love not to carry a lot of things. But then I perhaps know too much about cases...

JULIE McCROSSIN: Do we have any data on how many people are embedding things on themselves for convenience?

KATINA MICHAEL: It's definitely over about 5,000 people. I've started tracking back in 1997 when I was doing my PhD thesis at Wollongong on smart card innovation. The company I worked for invested $100,000 for the first cyborg 1.0 project at the University of Reading. I was working for Nortel, turned to the back and read about Kevin Warwick, now a friend and the provost at Coventry. He took an implant space for his laboratory, walked through corridors at the cybernetics lab ‑ his favourite html page would open, lighting would turn on by the wave of a hand or him walking through an area... His 1.0 example was getting an RFID token and implanting it. His 2.0 was looking at more, ah... ..applications to support wheelchair‑bound people and to have a median‑nerve interface that would allow people to communication directly with the internet. And he received 100‑electrode implants in the median nerve in his forearm, then connected a whole lot of gadgetry, but was able to demonstrate very, very coarse Morse code brain‑to‑computer interface things at the time. He communicated with his wife in the laboratory ‑ they were blinded up, it was all surveilled ‑ when he moved his hand, she felt a sensation in the other part of the room. So there's a lot of technologies that are beyond just IoT and convenience, and they're a moulding and repurposing, perhaps, of our traditional prosthetic devices, but now internet‑enabled to do other things.

JULIE McCROSSIN: I wanted to do two things with the panel, and a gentleman here has a question… ..Greg, I wanted to ask you this issue of ‑ what are the questions we, as activists or seeking to influence public policy or the rights of consumers ‑ what are the questions we should be asking? Do you have any suggestions in relation to people with disabilities and advocacy for access, or any other issue?

GREG KILLEEN: Yeah ‑ in Australia, we do not have a telecommunications standard. We have access to premises standards. We have transport standards. We have education standards. But there is no telecommunications standard. Which means that software and hardware that's been developed doesn't get created to meet the needs of people with disability. ATMs and other software, or apps ‑ a lot of people with vision‑impairment can't access them. As you know, going through the '80s, phones continued to get smaller and smaller and smaller ‑ notwithstanding that the smartphones now are becoming tablets and fablets ‑ the keypads were getting so small that people with a physical disability without the dexterity couldn't actually easily use those phones. So there really needs to be a telecommunications standard that's called up by the Disability Discrimination Act that makes developers, suppliers and all the stakeholders required to develop them to meet the needs of people with disability. When they meet the needs of people with disability, it improves the access for everybody. We have an ageing population. So... ..yeah. That's what I would be calling on.

JULIE McCROSSIN: I don't know if you saw Australian Story, or anyone else did, this week ‑ it was the story of a young woman ‑ can you remember her name, Greg? Did you see it? Someone Google it, would you? Australian Story. She was a dwarf, or a little person...

>> Kiruna Stamell...

JULIE McCROSSIN: I can't remember her second name ‑ apart from being a fantastic performer, NIDA said they wouldn't take her. She's gone overseas and had a very extensive theatre and film career.

GREG KILLEEN: I saw it.

JULIE McCROSSIN: Brilliant performer. She's taken the post office in Britain to court successfully and they've had to change the placement of the way we pay... ..help me, guys. EFTPOS machine, thank you. So it's on a long enough cord so a small person could reach it and bring it down. They'd fixed them to the desks.

GREG KILLEEN: I successfully sued taxis to ensure they're wheelchair‑accessible. From October 2011, they all need to meet what was the protocol, the new transport regulations, the transport standards...

JULIE McCROSSIN: Vijay, you know how you presented yourself as, "I'm just a technical person, not a policy person" ‑ I just wondered, is that a sustainable position? Not just for you, but for everyone?

(LAUGHTER)

You know when Katina was talking about embedding the chip and the person could open everything and then they could make someone feel in the next room ‑ you were laughing and nodding. I can see you'd embed yourself within 10 minutes, given the opportunity! I'm partly joking, but can we just enjoy the development without the eye on social responsibility? Or will the market always speak? Or do we have a role in interacting with the market?

VIJAY SIVARAMAN: We definitely have a responsibility and it's... I think there is a responsibility for those who are innovating in technology to at least think about the possible consequences and the impact but, at the same time, I think knowing what the consequences are is very difficult beforehand because, once you put something into use, it gets used in a different way and that is very difficult to foresee, no matter if you are a technologist, regulator or an insurance company. So, in some sense, I don't quite know how much you can kind of hold yourself back and say you don't want to innovate - if the nefarious use is very obvious and dominates, then, of course, use but, otherwise, if you believe you are doing something good by innovating, but then it gets taken up in a different way or gets taken up by the mass market for recreational purpose that becomes a prime economic driver for it, then -

JULIE McCROSSIN: I'd be amazed if anyone was against innovation in this room. Amanda Long from Consumers International, it would appear they are putting trust, co-design and consumer engagement up front and centre so when that regulators and consumer movements have to be nimble and responsive. What I'd like to do is come to the audience now for any questions or comments. Mr App I'm thinking of you as, he is waving at me, I will come to you. You can ask or say anything but if you could turn your mind to what is our role as consumer advocates to be active in the public space in a constructive way as we enjoy but also endeavour to co-design the innovation, that would be great. But I will come to this gentleman.

>> I will wrap a couple of things together. We moved from Internet of Things but to me the internet was invented to enable commune communications between people. It has now moved on to enable communication between devices. The first example I heard was at Carnegie University where they worked out how to connect their computers to the vending machine to work out if there was anything in the vending machine downstairs. The internet I am a part was created by the people who created the internet. I have an interesting debate with them, I will raise the question and be howled down by a couple of people in this room. It is fair enough to say that these incredibly intelligent, forward-thinking people could not possibly have been able to envisage the bad things that the internet would be used for and, to come back to Vijay's point, I don't know you can, as a technologist, any more say, "It's not my fault". It is time for the people who invented the internet to solve the problems of the internet. They couldn't thought we would have people trolled, we wouldn't have had the dark web, all the other things wrong. It is time for technologists to put their hand up and say, "We don't just build the devices and hope nothing goes wrong".

>>

JULIE McCROSSIN: If you can't hear, will you wave? I am becoming a little bit deaf due to health problems. If anyone can't hear, wave, I feel like turning the mic up.

>> It is vin sent Yu. If I can summarise what the Internet of Things are, they are internet addressable things. Most things have internet addresses coming through to accept the command. In the early 1990s, my company responsible for providing firewalls for the AMP privatisation and we are putting the security for those people responsible for the privatisation is that nothing is going in and out without being protected. Those days, we protect against mostly IP addresses and, at the time, IP addresses were running out and we said IP address is not enough, had to reconfigure the IP addresses and the internet providers are reluctant and hesitate. They think the IP address is enough. But I thought the IP address needs to be protected for people who are supposed to be legalised to use them and has authority to use them but nothing has actually come forth in that area. Is that right? Some work has been carried on to, say, protect the IP addresses?

JULIE McCROSSIN: IP addresses. Can someone explain what they are and then respond to the question whether there is a need to protection.

VIJAY SIVARAMAN: An IP address is a 32 bit, bit binary digit, it is a number given to you on your device and that's how data and messages get sent or routed to you wherever you are on the internet. I'm not sure if there was a specific question in there. When you say "protect IP address", many things come to my mind and also the previous gentleman as comment, security was never built into the internet in the beginning. As the research community, we are starting to realise more and more over the last 5 to 10 years. For better or for worse, the original internet was built purely for connectivity and it was built purely so that America could respond to a nuclear attack from Russia and the network will stay connected so they could launch what they call the second strike back into Russia. That was the original intent. That's what they built it for. It gave them that robustness, even if part of it is nuked out, the rest is connected.

JULIE McCROSSIN: I thought it was academics around the world wanting to talk to each other.

VIJAY SIVARAMAN: Academics were funded to build the resilience. Academics like their intellectual stuff but they were funded by the defence to build it with that purpose. Security was never on the original agenda. It's something that has surfaced more and more over the last five to 10 years. Everything we are doing is a retrofit. Today I can use any IP address I want in the world and send it back into the internet. That's called spoofing. I'm spoofing somebody else. Some of the attacks we have shown uses spoofing. Even the most protections are no at the internet. It is the recommendation in the RFC, which is a standard, that the internet provider should check the source address you are putting on the packets you are sending out but it is not implemented in practice by many internet service providers. It is not mandated. Security is a massive retrofit and with all these retrofits come a huge cost which people say who will bear the cost? If I give you a more secure product, are you as a consumer or an enterprise willing to pay much, much more money for that product? I mean, not that I want to make light of it but look at our own activities on online social networks or look at apps, for that matter. That's a good example. There was a study done by colleague, you are much more likely to download a free, version of the app rather than a paid version. Even though you are willing to take in ads, you are losing a lot more taking the free app rather than the paid app even if the paid app is $2. For better or for worse, that's the way also consumers look at the sticker price in the beginning and they don't realise the cost that follows on later.

JULIE McCROSSIN: Can we go so far as to say the only people who really care about security are people who are trying to do something nefarious or wrong?

VIJAY SIVARAMAN: Not at all.

JULIE McCROSSIN: The people who are trying to catch people trying to do something wrong?

VIJAY SIVARAMAN: Not at all. Security is not affecting all of us.

JULIE McCROSSIN: You just said there is evidence people will give away everything for free so that tells me there is a significant part of the population, even if you say you'll pay for it, you'll will have more security, "No, I'd rather have it for free". Is there a lot of people who don't care?

VIJAY SIVARAMAN: People don't realise the implication. Frankly, it is never very clear what a Google or some large entity is doing with your data and how it is affecting you. Maybe subconsciously you are more inclined to click on certain advertisements. You may not realise how you are being affected or worse things can happen.

JULIE McCROSSIN: I'm trying to drive you towards public policy. Should we be active in trying to communicate in a comprehensible manner to the broad population the dangers of the internet as well as the strengths in an informed way, plus strategies they can use, or not?

>> I'm Kirrie Weller. I'm a carer of a child of disability. I am semi-smart in my house. I mainly use it to manage my life and have a child with a disability who is integrated into life. I think it's too late for me not to use Smart technology because I would have to hire in more care workers. Yes, my son is a recipient of the NDIS but the budget is not unlimited. Having Smart in my house, helps us use the budget really effectively. I am investigating more and more options so that I can further stretch that budget. I think that is probably going to be the way of the future for a lot of people who are carers or helping their family member with a disability and I think we need to educate people like me and the whole community about how to manage the technology because we are now - IP address stops working and it doesn't recognise it any more, I have to figure out how to set up again, I have meltdowns in my house. My child can't cope because it manages his time when he needs to be calmed down. So things like that. I think that we need ability for people who are carers and who have a disability or who need technology for enabling anything, whether it's access to education or work, we need social policy and we need help and we need accessible education as well, so affordable.

JULIE McCROSSIN: Why did you come to the conference?

>> My work encouraged me, Greg Killeen invited my work to come along.

JULIE McCROSSIN: Greg, would you like to respond to that? Only if you want to.

GREG KILLEEN: I agree that it might be too late for those who are currently using all the Smart technology and different technology to use it for the benefits of supporting people with disability and their family and their carers for various reasons, let alone the cost-effectiveness of it. Yeah, I'm not sure if we can step backwards. I don't know what it would be like to make the choice to try to opt out of using technology that people have been using for so long. We were talking earlier about the security and accessing or people infiltrating and taking maybe control of people's homes, accessing the doors to get in or about having embedded devices but you don't really need to have an embedded device. If you are carrying a smartphone, I'd like to do a quick straw poll here, put your hand up if you don't have or use a smartphone or mobile phone. Okay. That's 100%. Everyone uses one. When you are carrying it with you, you can be tracked with GPS and all sorts of things to actually know where you are. You are not at home when you are carrying your phone so people can track where your phone is may not you are not at home.

JULIE McCROSSIN: I guess what I'm struggling with, guys, is this young woman is really saying, "Teach us how to understand its capacity and use it in our lives". I wonder if the concern about the troubles many of you is not something - are you concerned about security in your use of technology?

>> Yes. Recently I was encouraged, once we received our NDIS funding to sign up to a website to get care workers. I had to post a photo of my son who has a disability. I couldn't do it because I don't trust how his image will be used and I couldn't see anywhere on the website where they told me the rights to that image so I didn't sign up to using that care worker agency. It has meant it has been harder to get a carer because I had to find an old-fashioned agency who will meet me in person, not a virtual one. So that was really interesting. I would have liked some - that was a new thing for me. I hadn't come across that before. I think there needs to be a lot of education for carers and people themselves who are managing their care workers with the internet so that concept of having a virtual care worker agency as well and your photos and images and information.

JULIE McCROSSIN: Thank you very much. I have a gentleman here and then a gentleman down there.

>> Hi, my name is Tristan, I'm with DAPA. Disability able People's Association. I'm with Vincent. I have a question regarding personal data. We have in Australia no laws that protect a consumer's personal data which means that companies and industry can collect and sell that data without any regulation and they are also able to sell that to others and they are - they let people - have no monetisation right to their own personal data so they can't use it themselves, they have to go through court cases, for example, to gain access to their phone history so there is no policy in place to protect consumer data or to have people be - have that legal right to recourse to reject companies from using their data against their wishes. There is no protection in place for that. I was wondering if there are any solutions that the government can have in place for our protection?

JULIE McCROSSIN: Thank you. Is there someone in the room or on the panel who could respond to that? Control of personal data? Can you yell at me? I can't see the hand. Thank you.

>> My name is Kayleen Manwaring, I'm from the UNSW Business School, School of taxation and Business Law. It is not quite technically true there is nothing that protects personal data. The problem, as has been identified by Katina, is the protections under the Privacy Act is the loopholes have been weak and principles general. To ask a general consumer to enforce their rights against Companies is usually fiction. The other issue is consent protections are very weak. If you consent, they can do almost anything. The problem with consent, as has been identified, a lot of issues with consent mostly we don't get told enough, even if we do get told, we don't understand. We talk about privacy policies that say, "We will use your data to help improve your preferences", we are not told how or why or anything. The issue around saying the Privacy Act exists, not enforcing it and dealing with the loopholes is a big difficulty. I'd also like to say there has been a dominant dialogue about we don't want to stifle innovation. That's important. When you look at law and regulation, there is a time too early to regulate, you will stifle innovation but the flipside is there is also a time when it is too late to regulate. When the people who have invested this money and technology will fight against even reasonable regulation because they want to protect their business models so talking about consumer policy is very important, talking about consumer education is very important but education can't solve everything. The issues around disclosure and privacy is one of the important things because one of the things we have worked out in disclosure and privacy is it doesn't work. A lot of the times empirical data says it doesn't work to protect consumers. There has to be minimum standards to protect consumers. A lot of people won't agree with this but consumers can't always be expected to look after their own interests. We have Australian Consumer Law, people dodging around saying minimal regulation of security is - means we are avoiding a lot of the problems that will continue to exist that can't be solved by consumer education. Looking at the people presenting today, we are talking about protecting vulnerable people. People who can't realistically enforce the weak protections we have already got.

JULIE McCROSSIN: Is there anywhere in Australia or internationally where you can point to some examples of good initiatives, the private sector, the government sector or the non-government sector that go to some of the challenges you have identified.

KAYLEEN MANWARING: There is initiatives in the UK and Europe now around trying to get decent IoT security standards. That being said, the IoT Organisation is doing some work there as well. I'm not saying it doesn't exist. I'm just saying we are slow. When looking at issues of consumer regulators tend to throw it to the Privacy Commissioners who are going - there doesn't seem to be much being done around that. We are so far behind - unfortunately, in relation to regulation, we are so far behind the technology. For example, if you look at the Australian Consumer Law, last year there was an opportunity to review the Consumer Law. Some people were smart and made submissions on the Internet of Things and it turned up in the interim report but, in the final report of the Australian Consumer Law, that disappeared. We said, "We will look at emerging technology in two years' time" or something like that. It's really hard, it's really complex but -

JULIE McCROSSIN: Is part of the challenge who owns the problem and who is the advocate? I've got some panels tomorrow where I'm going to have to ask each regulator to explain who they are and who their constituency is because we have a plethora of them, yet you paint a picture of inaction?

KAYLEEN MANWARING: The problem is we haven't seen action that's been published. There may be a question the regulators, they are like ducks in the water, paddling very hard but we haven't seen it and it's trying to find it. We are trying to find out what is actually happening. My concern is - is it happening too slowly to protect vulnerable people? We have huge take-up, wonderful devices, some organisations are being very careful with security et cetera but there are a lot of organisations who know nothing about security, privacy because they are consumer goods organisations, they are not tech companies, and they are not doing what they should be doing because they don't know or don't care or they are not experts in these fields and creating things like kids' dolls that can be easily hacked which is something that's just happened quite recently. Dolls that can be hacked by me. I'm not a tech person, I even understood the most recent My Friend Kayla doll because it used a smartphone.

JULIE McCROSSIN: There is a gentleman who has been waiting, I will come to him.

>> Keith from Energy Consumers Australia. I'd like to support almost everything the last questioner said. I thought that was a fantastic intervention. In a former life I used to have a bit to do with some of these issues from a policy perspective. In response to your question are there places where you can point to better practice? I don't know if it is skill still the case but the Scandinavian countries used to be 10 years in front of Australia, I don't know if that's still the case but it might be worth looking at. I wanted to respond to your earlier question do Australians really care about security and I wanted to draw a distinction between security and privacy. There is a lot of evidence around that which suggests that Australians, particularly younger Australians, just accept that they are doing a trade-off when they use internet-based applications. They accept that they are actually giving away data, they trust that it won't be misused but they're basically doing a trade-off and they are conscious of it. They may not like it but live with it because that's the way the market is. When it comes to security, it is a different equation. People care about security once you explain the dangers.

JULIE McCROSSIN: Can you explain the difference between privacy and security.

>> Privacy of information versus security of your systems and in particular security of your bank accounts, security of your personal details, that sort of thing. The two crossover to an extent but the reason I'm drawing the distinction is because, in one case, I think people are either pessimistic, fatalistic or just accept the trade-off. In the case of security, once they understand the risks, they are genuinely frightened but individual consumers haven't got the first clue what to do about it which is where so many of the advocacy groups in this room come in because we have a very important role, first of all, to raise awareness where we can but, secondly, engage with policymakers to get them to become more active where they can because it is the case that there's always a potential policy response once you wake government up.

JULIE McCROSSIN: Can I say, as someone who is only in this space intermittently, this thing of defining terms is terribly important because when you say "security to me security" to me, when something happens in London, I have my best friend and her four children, some close family, every time we text each other or message each other through Facebook. I think you will find a significant proportion of our population have got connections in London or other capitals where dangerous things are happening fairly regularly now so we have the population being sensitised to security. When you said Toowoomba Council has activation, if I said bomb and fertiliser, there is a part of me that thought of my friend in Britain. I'm going to London in a couple of weeks. When you are in Mitch Fifield, the Minister's shoes, security is as much about keeping the people safe, isn't it? Can you respond to that? Where is the trade-off we should be talking about as policy influencers?

>> One of the trade-offs is what are the simple things people can do to protect their own systems, protect their own bank accounts, protect their own personal information and also finding ways to give individual consumers the ability to make these choices and to make them in an informed way because anything to do with technology is awfully bloody complicated and most people don't have the time to become experts or even partial experts in these areas.

JULIE McCROSSIN: Thank you. We are going to finish very shortly so a final comment, Katina, and to each of you.

>>

KATINA MICHAEL: Thank you for the audience contributions. I've been thinking about the clash between personal security, corporate security and national security. These three different types of securities where we get muddled. National security will always want access to the Internet of Things during crisis events, even more generally. Your personal security, however, is compromised by these national security regimes. I'm not going to say that national securitisation or social securitisation of the State is not the job of our government and not the job of our law enforcement authorities or Defence Forces. But I am saying, just like Tim has said, "Far out, if I knew what I had created, I never would have created it". Find his Guardian reports -

JULIE McCROSSIN: What did he create?

KATINA MICHAEL: The World Wide web, he is leader of the W3C. If the IoT will divulge much more information, devices won't only have an IP address, your location will have an IP address, think about that. Your house will have an IP address because your house will be on the complex of complex systems will be a system in subsystems and there will be subsystems within that so when your location as an IP address or where you visit as an IP address and you can ping that location plus ping your device plus whatever you want, then we are basically open for a surveillance state. If I sound extreme, I'm sorry, but these things of better connectivity and better convenience, do you really need it? Do you have enough of it? I know who needs it - the lady who was talking down the back about her child, my brother who has a child with autism, Greg perhaps but you mentioned stand-alone systems, I think there are people in society, the aged who are living alone at home and require assistance, I think we have top places to be putting IoT but I don't want us to be putting it willy-nilly in every single light fixture, lamp post down the street, every single whatever.

>>

JULIE McCROSSIN: What is the WTTC?

KATINA MICHAEL: The worldwide web consortium.

JULIE McCROSSIN: Do you have a final comment?

VIJAY SIVARAMAN: It is still early in the journey with regard to IoT. There are a lot of implications we do not quite understand. I think, because of the big business that's happening in IoT, obviously another business entities have a big incentive to push it. Like Katina said, as consumers we have to be more conscious of what we want and in some sense we need a stronger voice and that requires us to engage more and articulate what those concerns are and push back on the manufacturers and the suppliers who are trying to push it towards us. I think we are slowly in the journey and there is a lot of work yet to be done, in both understanding the landscape and the implications and coming up with the right mechanisms to control it.

JULIE McCROSSIN: Thank you. Greg.

GREG KILLEEN: I'd just like to say, from my perspective, I'm all for innovation, although, the system I'm using might be considered old-school technology, it's actually the ability to meet my goals and my needs is the most important thing, so when any new innovation, look at what the person actually wants to do as opposed to, "This is the latest technology". The technology that's been developed, it really needs to be future-proofed because it's too expensive to be buying an environmental control system - the Google Home will be ditched in two years' time because they'll bring out Google Home 2, then Google Home 3, then all we've got is landfall. We need to be able to adapt and add things to your current unit so you can develop things in the house to make it more cost-effective and user-friendly. The final thing I want to say is that when it comes to developing these things and aimed at people with disability, you need to consider them not to be gadgets and gizmos. They need to be considered as tools to independence. Because that's actually what they are, not a gadget or gizmo. If we think of them as a gadget or gizmo, you'll be thinking, "He doesn't need that, it is something for the mass market" but look at it as a tool of independence.

JULIE McCROSSIN: Ladies and gentlemen, would you thank our panel? Thank you to you as well for your participation. Just before I send you to lunch, there is an nbn store with two women there dying to talk about the nbn with you, please make friends with them. Copies of this report that we heard about from Vijay are available out the front so there's free copies available. No doubt it's on the web as well. Ladies and gentlemen, we will start again promptly after 1:30. Please enjoy your lunch.

VIJAY SIVARAMAN: The posters are up in case anybody wants to have a look and our students will be there to explain them in more detail if you care. Thanks.

(BREAK)

JULIE McCROSSIN: Ladies and gentlemen, if you could take your seats... Early start, early finish - that's my motto. Could you have your numbers ready? I'll draw in just a second. Shhhh - everybody stare at me! Guys, you remember at the beginning of the day - we talked about the prediction competition, where you predict something to do with technology and communication in the future and the one that is most thought-provoking, intriguing or fun - or all three - wins the drone? We're giving you some suggestions. In 1999 - examples to inspire you - some bloke called Bill Gates said, "Payments and financing online, and better healthcare through the Web." Gates' prediction - "People will pay their bills, take care of their finances and communicate with their doctors over the internet." He could have got the drone, let's be honest.

(LAUGHTER)

Could we have another one? Have we got another prediction, Wayne? Small technical hitch...? Great. Social media. Gates' prediction: "Private websites for your friends and family will be common, allowing you to chat and plan events." 1999! You can see why he made some money. Can we have one more? Automated promotional office - Gates' prediction - software that knows when you've booked a trip and uses that information to suggest activities at the local destination. It suggests activities, discounts, offers, and cheaper prices for all the things that you want to take part in. I'm sorry, but I'm still amazed by this man. Are you amazed, or are you used to all this stuff? I need a trailer. I'm 62, 63 in a couple of weeks... I've never had a trailer, I've never reversed a trailer. This is an experience every woman needs to have!

(LAUGHTER)

So I went on a few Web searches - I have inundated, in all my devices, pictures of trailers. I'm in a state of permanent trailer arousal.

(LAUGHTER)

I actually am picking one up this weekend. I'll see if I've got a photo on my phone to share with you later. Ladies and gentlemen, this is our next - help me, what is it again? A Bluetooth speaker. Thank you, Peabody... What's going to be hard, of course, is going home without Peabody and just having two cavoodles, which I've now learned I can control remotely and I intend to set it up...! Red F6. Get it out. I told you to be ready. It's redraw on the third call...

(APPLAUSE)