The Privacy Catch

TERESA CORBIN: OK, we're going to start our next session. I'm going to introduce you to Malcolm Crompton, who manages the information integrity solutions, but his full bio is obviously in our program. He also was our privacy commissioner from 1999 to 2004, so he is one of Australia's experts on privacy. So I'm very pleased he will be facilitating this. To kick off the session we've got a very short video.

(Video)

NEW SPEAKER: If the boneheads at New York magazine can figure out that privacy is dead – it's dead and buried. People put things up on their MySpace page today that, when I was a teenager, when I was 25, I wouldn't have dreamt of telling my closest friend.

NEW SPEAKER: I just think it's important pointing out that the people who care about privacy – this is why I say it – the people who care about privacy are consumer watchdog groups like Consumer Watchdog, which are paid to go after the...

NEW SPEAKER: What about individuals? I care about my privacy – I'm an individual.

NEW SPEAKER: OK, consumers do care about privacy – let's not fool around with that. They care about a couple of things – they care about their security. They don't want to see their passwords hacked, they don't want things to leak. They care about identity theft – they don't want someone else pretending to be them. And they care about kids' safety. What they don't care about is companies building profiles about them online. If people cared about profiles being built about them online, 900 million of them wouldn't join Facebook. You know, they wouldn't use those fidelity cards that you get in supermarkets or credit cards or banks, which all know everything about you and where you spend your money and where you live and how much you are spending. We're talking about banks, you know? And these are corporations that have all this data about you.

NEW SPEAKER: I think it's important to recognise that you can't have 100% security and also then have 100% privacy and zero inconvenience. You know, we're going to have to make some choices as a society.

MALCOLM CROMPTON: So, welcome, everybody. The talk that we've just had, for me, has been quite remarkable, because, while I have seen futurist talks and other discussions of these issues for an incredibly long time, very few of the discussions that you hear about have some balance in there that are actually seeing the excitement of the future, but how do we harness the excitement of the future in a way that creates a society in which we might want to live?

So thank you very much indeed for setting the scene for us so well, Gerd, and we're privileged to have Gerd on the platform with us as well. We have three panellists with us, as well as Gerd, now to try and take the discussion forward. I'm going to ask each of the panellists to very quickly outline one, two or three of the big issues as they see them. We will then commence the discussion, if you like, amongst ourselves, and then we'll be opening it out to the floor.

Now, I believe this is going to end up in, hopefully, managed anarchy, in that there's going to be some pretty lively discussion one way or another. I will introduce each of the panellists in a moment. Just in terms of setting the scene, let me add a couple of points to what Gerd was saying. The big oil – Big Data analogy works incredible le well. There was a paper that came out only two or three months ago that draws up the big oil/Big Data comparison, and the concept of externality and how you harness that and bring it to internalisation and that is an important debate on data we've hardly heard. Yet the big oil analogy provides you with the lessons on how some of the issues with big oil were dealt with once external economics were dealt with and the methods used to bring that in-house. Not perfect, but better than doing nothing. A very good point.

But there is another analogy that I think has not been talked about enough, which is the sore that says that the law doesn't move fast you have in. That is, in fact, the beauty of the law – to live in a country where there is a stability of law sufficient that we can actually understand it and see it enforced and find ways of living with it. So the issue is not that the law can't keep up – the issue is, what is the law

that provides that stability, that creates for the innovation and still creates a society in which we want to live? And it is possible, hence the motor car analogy. When Ralph Nader wrote "Dangerous at any speed" he was really talking about how dangerous the motor car industry was in designing and building motor cars. The response of the government was not to design laws that banned motor cars. It did pass laws that said "There shall be standards" and anything that builds to those standards must be testable. So you therefore had a standards setting process and a standards testing process. The stable bit of the law said, simply this, "You shall not sell motor cars that fail the standards test". That is a piece of stable law. Designing the motor car is unstable. We cannot have a parliament designing cars fast enough, let alone with enough political objectivity. So what are the equivalents in our digital world as to where the law should and should not bite is just one of the many questions that I think we will have to come up with.

My last analogy is the beauty of James Watt's invention, going further than Gerd said. The other big invention that James Watt came up with was how to harness that power. And that's with the James Watt governor, and that is a little mechanism that sat on the steam engine with a little spinning gimbal and if the machine slowed down the gimbals would rotate less quickly and they would fall in and let more steam into the engine to pump harder and if the engine was moving too fast they could choke the steam going into the steam engine and slow it down. Because the problem being solved for the steam engine was how to pump water out of a coalmine that sometimes flooded and run the steam engine at constant speed under varying load. The James Watt governor had two components – (a) it gathered information, and (b) it acted on the information that it knew in a very simple way. So James Watt gave us not only power but the harnessing of power and it's going to be governance that matters as much as the technology in exactly the same way in what we do in the future.

Just pulling the pin on a couple of hand grenades! The last remark I wanted to make was actually to come back to the theme of what ACCAN is here for, because it is such a beautiful theme. In the world that we're in, it's about connecting customers, not disconnecting customers. You say the word "Privacy" to so many people and they think that privacy is about keeping secrets. It is, in fact, about the controlled sharing of personal information – how much, when, with whom, for what purpose, and so forth. And that is where the beauty of Gerd's talk was in that he tried to find some of where those balances might be.

What I'm going to do now is to ask each of our panellists to at least say their name and where they are from. But then I'm going to go back and ask each of them to put on the table two or three of the big issues as they see them, either inspired by Gerd or otherwise, and then we'll start our discussion. So, first of all, panel, please introduce yourselves.

JON LAWRENCE: My name is Jon Lawrence, I'm the executive officer of Electronic Frontiers Australia.

LIZ SNELL: Snell from Women's Legal Services NSW where.

NEW SPEAKER:

KATRYNA DOW: I'm Katryna Dow the founder of NICO.

MALCOLM CROMPTON: And I think we know who Gerd is! In the interests of all sorts of democracy I'm now going to ask the table to again go down there and again give us their quick, short thoughts. Jon, would you be able to tell us from either your personal perspective or an EFA perspective what you think the three big issues are. And you have three minutes! Your time starts now.

JON LAWRENCE: Well, I think certainly from our perspective, the whole conversation about government surveillance is really at the top of the list for us. There is, of course, proposals coming down from the Attorney-General's department to introduce a mandatory data retention scheme, which we have pretty grave concerns about and I think that's certainly something that needs to be discussed, perhaps not at length in this context, but it is certainly a high priority issue for us. One other thing which is a little bit out of left field, but I think there is a fairly clear connection, is the – the other thing that the Attorney-General's department is working on at the moment, which is around copyright enforcement and what's interesting is that the wishlist of data points that has been released – slash leaked – for the mandatory data retention scheme includes upload and download volumes

and nobody has yet been able to give me any explanation of why that would be included except for tracking copyright infringements. So there are some interesting leaks there and I think some interesting privacy risks. The other point that I think is pretty interesting is what's happening in Europe around the right to be forgotten, and I think there are interesting challenges there in balancing free speech and accurate information about public figures and the right for privacy. So they would be the ones I would nominate.

MALCOLM CROMPTON: And Liz?

LIZ SNELL: I think one of the most pressing issues is the misuse of technology to perpetrate domestic violence against women. And this happens in a range of ways. We're finding that partners and ex-partners are monitoring and keeping women under surveillance through GPS tracking and also through other monitoring devices, including by putting spyware without the knowledge of the woman on their phone or computer or some other device. By doing this they are able to follow their computer strokes and so also break into their social media sites and emails and so be constantly monitoring them 24 hours a day. And also by being able to break into the social media, we're finding that often they may impersonate the woman as well and in doing so send offensive comments to family and friends as a means of trying to ostracise her from her family and further isolate her.

Another form of this, where there has been quite a bit of media coverage also, has been in relation to the sharing of intimate sexual images without consent. And all these forms of violence that we're finding have been perpetrated against women are for the purpose of control and for the purpose of shaming and humanitiating women to cause fear and also to punish the women. And it's omnipresent, it's all-pervading, and it's causing devastating impacts.

In terms of two sub-issues around that, about what do we do, the first issue would be that perpetrators of this kind of violence need to be held accountable and we should stop blaming the women. And in terms of holding the perpetrators to account, I think some of the issues are around strong laws, both enforcing those laws that exist but perhaps also looking at other laws as well. And also having technical developers be able to provide some further training for police and other law enforcement people, so that the laws can actually be enforced and the evidence gathered.

A second part is that we often hear – and it's interesting, in Gerd's comments he was talking about how being connected is very much like air and water. But unfortunately women who experience this kind of violence are often told "Get off this social media", or, "Get off being connected". And we kind of like to challenge that, insofar as perhaps another way of focusing on this is, how can it actually be safe? What privacy settings and other mechanisms can be really clear and upfront so women can engage and stay connected. If we're telling them to get off social media, for example, given it is a dominant form of communicating and staying connected with family and friends, this is further isolating them and compounding and extending the abuse. And lots of ways in terms of how to enable that is through education programs – and I particularly just want to mention the women's services network's – just last week along with their sister organisation in the US, they launched Safety Net Australia and also the domestic violence resource centre down in Victoria has been doing great work with Smart Safe. So there are a lot of education programs out there and it is about building on that and everyone kind of has a role to play in those kind of education programs, so that women can learn more about how technology is being used, but also how they can use the technology to enhance their safety.

MALCOLM CROMPTON: Thank you, Liz, very comprehensive!

Now, Katryna?

KATRYNA DOW: I think just building on what Liz and John have raised and absolutely following Gerd's presentation. Social ethics, our responsibility, how that connects with laws. Transparency, specifically our legal system as it stands right now, how that then translates into the digital world. And, if time permits, I think there's also an environmental – there's a planetary impact to the storing and overstoring of the same data and there is actually a cost from an environmental point of view and I think that is an interesting discussion that we are not really having at the moment.

MALCOLM CROMPTON: That is a new one, that's good. Gerd, did you want to make a remark at this point or shall we roll on?

GERD LEONHARD: I think we should roll on. I've said a lot already!

(LAUGHTER)

MALCOLM CROMPTON: Now, one of the things that I thought I would do in the light of those first remarks is to give you a very short scenario and then suggest that we go up and down the table on many so of the questions against the scenario, and then take the conversation there.

Here is where we've got to remember, people aren't always empowered. We actually start our lives almost completely disempowered as babies, and we often end our lives pretty disempowered if we had a long, slow decline into extreme old age. Many people at particular points in their life will have extreme moments, or periods, of less than full ability, and there are other people for whom there are other stresses and strains in life that mean that they're not always in full control for various reasons. So let me give you this example.

A person called Kate, and her activities and preferences and accomplishments have been chronicled online basically since birth – and my point is, it is by her mother. So it is beyond her control. Instagram provides thousands of pictures and commentaries on little Kate's activities to many of her followers. Many of whom she has not met. In the future herself Kate will become a prolific user of social media. By this time, of course, most faceting of Kate's life will have an online component from her use of dating sites to her reliance on Google Maps for directions to her personal files being stored in Cloud systems around the world. Everything we heard from Gerd. However, after a bad experience, which is the point that Liz was making, we see Kate reassess her values and life direction and she will decide to retreat from having such a public presence. One of the points that Liz made was, why should the response have to be retreat? Now, part of her online presence which was voluntary, such as the dating website, and others were involuntary, such as her mum's Instagram account, and other parts, such as her use of email, were merely a product of social norms. How do you communicate in today's world without using email or some other form of digital connectivity? After all, who can participate in society without an email account or other forms of conductivity?

So now to jump over to what Jon was saying and the point that Jon was saying. In this world where we change our minds, for whatever reason, how do we deal with it? And in particular, I want to ask each of our panellists, not just Jon, to look at this first question: How effective will the European Court of Justice's right to be forgotten be in Kate's quest to make it more difficult for others to find online information about herself? The subtlety by the way in the ECJ judgment, was not a taken down notice against the original data. It was simply about providing some obscurity of access to that data by removing the ease with which certain search terms produced a term that got you to the underlying data. As an article in the Guardian pointed out with regard to one of the take downs, if you mention the particular Scottish football coach's name in the search term, you won't get the articles up that show you about the nasties that happened in that football club. However, if you ask about the football club, you can get to the articles. So it's very subtle what the obscurity is, but that is what has been produced so far by the European Court of Justice decision. So what I want to do is to ask for some opinions on, is simply some increases in obscurity of the form such as the ECJ ruling sufficient? Or should we be doing more to let Kate have a private life, but still engage? Jon?

JON LAWRENCE: Erm, yeah! This is a really interesting question. I think, just to start, I think clearly the way the decision has been made and implemented is sort of not terribly good public policy-making. I think there needs to be a sort of proper process of discussion and deliberation as to exactly how this – how such a right should be implemented. I think, in terms of obscurity and so forth, I think, you know, taking it just to the search engine level is perhaps a bit of an easy way out makes sense that if you are not in Google, you kind of don't exist, but I think – you know, that presumes that the current sort of paradigm of search-driven web traffic is going to continue, and it may not. I think, you know, there are situations where, if the information is, for example, really untrue and quite sort of defamatory and so forth, then it really should be removed from the originating site as well. So I think there's a lot more that needs to be done in terms of working through the processes and Google has been pretty heavily criticised for the way they've implemented it, but I think there's also a great danger – and this is the other side of it – that people can use it to essentially rewrite history. Particularly

people that are sort of seeking to go into public office later in life. They may be able to remove things, or obscure things, that perhaps should be out there and available for people to make assessments about their character, and so forth.

MALCOLM CROMPTON: So, in summary, I think you are saying that the concept behind the decision was probably a good start, but not enough.

JON LAWRENCE: Sure.

MALCOLM CROMPTON: And the implementation was a tad questionable?

JON LAWRENCE: Yes, there has been no public process behind it, it has been a court decision and Google is being told to go and do it and they've kind of done it in a certain way that some people suspect is trying to drive a – you know, highlight particular issues, and so forth, and they may be doing that. They may not. But I think, you know, I think there are real dangers with it in terms of public persons that choose to be in the public sphere and rewriting their back story, but I think there's also – you know, there are genuine situations where, you know, this is an appropriate thing to do and it's obviously a very, very tricky and quite delicate balance to find, I think.

MALCOLM CROMPTON: Thank you. Liz, is it a contributor or not?

LIZ SNELL: I think I would agree with Jon with respect to, it is a start. I would also agree that there may be other mechanisms too. So, for example, in Kate's scenario – and I mean, it's not really clear what happened that kind of precipitated her withdrawal, but, for example, I can't see there being any public interest or other reason why, if there are images of a sexual intimate nature that have been posted on the internet without the consent of the person, why an immediate request for that to be taken down can't be actioned. I think that would be consistent with the policies of the different organisations and what have you. So I think, irrespective of this, that that could be another mechanism. I think other things also that complement this as well, depending on the nature of the offensive material, too, it could be reported to police and other action could be taken down that avenue as well. Although, I do note, for example, in Australia, with the criminal code, there's a mechanism that you can use with respect to carriage service providers if you are experiencing harassment or unwanted messages or a few other things. There is that mechanism in the law. But since 2005, there has only been 308 successful prosecutions. So it kind of begs of question, is it not working as well as it should be and, if not, why not? I guess some other mechanisms could also be, if she knows who has put the material up and they've got the power to take it down, can there be some direct conversations around that as well? So I think, yes, there is – I can see some positives around that. I can also see some negatives as well. But I think it's also important to be looking at what other mechanisms there are as well.

MALCOLM CROMPTON: Thank you. Katryna?

KATRYNA DOW: Malcolm, it's really interesting that you raised this question. We actually asked an intern, a young woman, that recently joined us to write an article just last week on a fictitious mother, expecting a child, who decides to share a lot of the pregnancy online and what does that actually look like for the child actually having a digital birth before a physical birth? So we started to research this, and we see that more and more for a lot of women and parents, they're sharing a lot of information and if you look at some of the themes that Gerd spoke about, where I think this right to be forgotten – we're talking about Google right now, but we may find that it is something at a constitutional level that children will assert the same sort of rights to say, well, there was so much information shared about me before I was born or around the first few years of my life, that that may disadvantage me in terms of the school I could get into, the health care I might have access to, the type of social environment that I might be able to enjoy.

So I think we are at this nexus where we want to be connected and the idea of having a family is a time of excitement and we want something where we want to feel connected with the people that we love but at the same time I think we are at this tipping point of, what does that actually mean for the future generation? Are we going to have a generation of children who say to their parents, "Actually, I have some rights to be forgotten, so that I can have exactly the same kind of serendipity and

opportunities in life that you have enjoyed or my grandparents enjoyed". So, I think we're at this precarious time in finding the balance between those two things.

Very quickly, particularly for women that are pregnant, there are so many amazing applications now that are either helping women fall pregnant, or manage their health, the terms and conditions of what those applications do, who has access to that information, how it is shared, who it is shared with, the example that Gerd used in terms of whether or not that automatically goes to an insurer – again, I think these are things that we really need to surface. It's this discussion around transparency and starting the conversation around the implications, I think. So I think the right to be forgotten is not just going to be exclusively from a Google perspective.

The underlying problem of all of this is that, in this world, in order to fit in, we'd have to be 0s and 1s. If you're asking for a yes or no answer, it's an impossible question for us. You cannot just say "Do it or don't do it." There has to be an – what I call an "it depends". How can you answer a question of technology by saying "You're either all the way in or you're all the way out"? That's kind of what the big technology companies are doing – if you're in, then you're all the way in. Basically, it's a 0 or 1. That is not fair to consumers on an extreme level. Only on a certain level, like when they weren't good enough and didn't have fast machines – it didn't matter. Because they couldn't do anything with it. Now that every point of information can and is being saved the 0s and 1s are turning us into an object of this machine, in a way. So this is referred to as machine-the inking. Basically, the answer for that is we need to respond as much time that we spent in investing in technology that we spend in responding to technology. We have to comply with the rules of that giant computer, and there's been lots of dystopian scenarios about this. I don't think that's going to happen, but if you compare the human-machine problem, for example, with various other addictions like alcohol or cigarette smoking, you can argue it is unhealthy and should be illegal for everyone – it's probably correct – but it would not be a good idea. Therefore, the question is, it depends. If you drink a bottle of wine for breakfast, it's not a good idea. But we shouldn't make alcohol illegal as a consequence.

Our challenge is to figure out the "it depends" rules. This will get much, am up worse – you've seen nothing yet. Because in a very short time, we're talking about artificial intelligence connected to people, robots going in our bloodstream to clean our cholesterol, printing organs – this is all going to happen in the next 10 years, and these are all serious ethical questions. Should we allow this? And why, and who? So that, to me, brings up this big question – we are at this Nexus to where things that have been just a pipe dream, or science-fiction – they're real. So therefore, our challenge is not to just say "No, it can't be any of this," because that's kind of what is happening.

MALCOLM CROMPTON: Just following up on what Gerd said – think about this question of a driverless car – the ethics that you have to program that car are. You're in a car with two very young children. A grandmother steps onto the street and the car has two choices – kill the grandmother, or kill two kids. How does a car make that decision? What is interesting is you go to the law and prosecution of the driver how the driver made the decision – if it's a human-made decision. Who do you prosecute if it's the car that made that decision, and how do you program it to make that decision in the first place? The ethics of the driverless car will be upon us within two or three years.

GERD LEONHARD: Another thing that really matters there is, keep in mind that, collecting all the information and having it and making it intelligent is a huge business. In fact, it is the biggest business.

MALCOLM CROMPTON: Yeah. Gerd, Google now is gathering up all this data, analysing it, and feeding it back to you to give you N-per cent of the total value of that data, where N may be less than 10, and the remaining percentage is retained by Google for making money. It's a sharing of the value, but is a fair sharing of the value?

What I've heard from what was said so far is "Houston, we've got a problem." But I haven't heard enough of, "What are we going to do about it?" I want to try and spit out whether it's a problem with the current laws in the sense that a new law is needed or it needs reframing in some way, or whether its modern interpretation of existing laws, as Jon was pointing to – maybe you can use the laws of liable or something else to achieve more than we think in this space. There's then a separate question – regardless of the answer to the first question, the second question is, is it in fact not the law but it's the enforcement that is the issue? Because I really do come back to enforceability. Either because the

regulator – or whoever's doing the enforcing – needs enough bucks, or it's actually just too darn difficult. Third of all, in terms of what was really being said by Gerd – how can we make whatever it is move fast enough to deal with it? I'm going to ask each of our panellists to try and think about that question. I want to know the answer to "Houston, we've got a problem."

JON LAWRENCE: I think there is an enforcement problem. This is something that's come up around the cyber-bullying issue and the government's proposals to deal with that. It's certainly an experience that I've had in my role, where I've been approached by people that have had harassment issues and have fawn to the police and the police have said, "Look, we really just don't have any resources to deal with this." There are clearly issues there, and you touched on that earlier as well.

I think what's interesting – one potential interesting solution which may help – or part of the solution which may help to focus minds here – is the proposal that's just come out from the Law Reform Commission for a statutory tort of privacy, where people could take private actions against people that have been seen to invade their privacy. I suspect that's something that would be of interest to your clientele as well. I think that's something that's worthy of some pretty significant consideration, particularly given the lack of real constitutional right that we have in this space in Australia.

I think, also, what's kind of interesting – there's some legislation in the Victorian Parliament as well around the issue of sexting, and creating some new offences partly to give the police some room to move that don't involve child pornography laws, particularly where there are consenting minors involved. I think there may be some interesting lessons to be learned there that can be rolled out nationwide, potentially, around sharing of sexual images and so forth.

MALCOLM CROMPTON: I am going to go down the table, but I want to ask a supplementary of Jon. The sexting one interests me a lot. When I was the privacy commissioner and the first occasion came up where an SMS message was produced as evidence, Australia went berserk. Because SMS messages were perceived as something being created instantly on your phone that appeared instantly on some other person's phone, and never was instanced anywhere else in the world at any time. Of course, what happened is the message in between those two points was captured somewhere and used as evidence. We've seen how fast these things move. But the thing that interests me now is that, in fact, the sexting law may be a very enforceable because it's so easy – it's so point-to-point that you're actually able to work out where it came from and do something about it. Is that an example of a good little law simply because it's actually enforceable at reasonable price?

JON LAWRENCE: Well, potentially. I'm not sure that's where it's coming from. I mean, I think the driver was largely that there were things happening with minors that were essentially getting potentially caught up in child pornography offences where it really want appropriate. They were looking to create, A – new offences so that they could avoid charging a 16-year-old for sharing photos with their 16-year-old girlfriend with child pornography. But also, to really create an offence for somebody that gets hold of that – a third party that gets hold of that – can and then shares it. I think that's probably quite appropriate, and I think you may want to speak some more about that.

MALCOLM CROMPTON: Yes, slip it over to Liz now, and go back to that question – is it a better interpretation of current law now that we're reading the law again? Is it about new law, or about enforcement and speed of change?

LIZ SNELL: I think it's a bit of everything.

(LAUGHTER)

Also, a problem in Australia is that there are different laws in different jurisdictions, which can also add complications. It's a bit of a patchwork of which legislation you want to use. For example, in the criminal jurisdictions, there are, again, depending on which state or territory you're in, protection orders. For example, in NSW, if you know to ask for it, one of the protection orders can be that you ask that you don't have any further information about you published. The challenge, of course, is do you know that you can ask for that order? In other states and tear – for example, in Northern Territory, you can ask for an order which has a positive duty, which means you can effectively ask for a take-down order, which kind of addresses the issue I've been talking about with respect to the intimate sexual images that have been shared without consent.

There are some mechanisms for take-down, but not necessarily consistent. That's the problem.

In terms of civil jurisdiction, I'm just picking up Jon's point about the Australian Law Reform Commission's proposal for a privacy tort. Women's Legal Services NSW and, indeed, many of the other Women's Legal Services around Australia, and many of the DV services who've responded to this inquiry, are very supportive of a tort around serious invasions of privacy, and specifically we were articulating the kind of serious invasions of privacy that I've kind of been speaking about in terms of violence against women. The problem, however, with a tort is it's not necessarily accessible for all. You need something that is quick and something that is cheap. Another proposal that was included in the Australian Law Reform Commission's discussion paper also included a possible suggestion of expanding the privacy commissioner's powers. This could extend – we would like it to extend – so it also covers individuals. If the privacy commissioner has the power to make declarations, then that effectively could be a take-down mechanism as well.

There are kind of a range of mechanisms out there. As I also pointed to, in terms of the Commonwealth, there is the carriage service provider – you can – sending a message that is harassing through a carrier service provider. In 2005 when it was first introduced, since then, there's only been 308 prosecutions, which begs the question around some of the other things Malcolm has been asking about. If the law is there, why isn't it being used? Is it an enforcement issue? Is it an evidence-gathering issue in so far as the technology is a bit complicated and we need training in that? Is it that it's costly? If so, how can that be addressed? Really, we need to be holding the perpetrators to account. I think there's a range of different mechanisms. Jon also talked about the sexting offence. We were really pleased to see the Victorian government recently responding to the sexting inquiry back in 2013 and saying things like they want to introduce a criminal offence whereby there is that sharing of those kind of sexually intimate images with third parties without consent. And also, as Jon has alluded to, if it's been further breached too.

MALCOLM CROMPTON: That's interesting. What's interesting about passing a law – it's almost like dropping a stone into a pond by the time it's finished in parliament, parliament knows that it's done it. After that, the media have distributed it to at least a portion of the population. But is it actually remembered and used by the whole of the population? The ripples take a long time to get out there, to the real world. That's one of the advantages of the stability of law – that if you keep on stirring up the pond, you never understand the waves. Katryna?

KATRYNA DOW: Where do we start? If I flip it for a moment – everything that Jon and Liz have talked about, there is a clear either misuse or change of context. I think this is a really interesting concept for us, maybe, to explore in the interim. That is, privacy is contextual. When everything is wonderful in a relationship and something seems completely appropriate in the moment, there's a context around that. Then, all of a sudden, the context changes. It may be that we can go further faster from a legal perspective if we can say, you know, when a relationship changes context, then there is also some contextual protection that sits around that. You know, I don't know how easy that is, but it speaks to Gerd's kind of "maybe" – it doesn't stop, 'cause we're never gonna stop a lot of these behaviours. What it may do is change that switch. Which brings me to the next point in terms of our current legal framework, and certainly in Australia, the other side of it is the surveillance economy or this idea of government wanting to collect our metadata, which is the flip side where maybe something – there isn't an issue, we're just going about living our life. All of a sudden, the things that we enjoy in the physical world, we no longer can enjoy in the digital world. I think for me, that's probably the bigger concern, because we currently operate under the idea that we are innocent until proven guilty. All of a sudden, we're hosting a behaviours from an enterprise, or an organisation that means we're some kind of product or an exchange, or whether we're looking at it from a government level, which I really find a concern – that is, it's almost that we are assumed to be doing something wrong, and then we'll have to assert some kind of evidence to the contrary. I think we're in this, you know... I think things will get darker, in some ways, before we'll find some of the answers, because we do have both sides of the coin. We have these situations where you really need a legal framework for intervention that's really quick and really contextual. Also, we need the time, actually, to work through some of these other issues, because if we make decisions too quickly, we won't consider the ethics, we won't consider the next generation, we won't consider the implications. So it's almost as if we need an interim strategy until we can have some more evidence as to what the context is. I think context is really the key thing.

MALCOLM CROMPTON: One of the really important points that you made, Katryna, is that quite often, context that's dealt with is the context of me dealing with my doctor compared with me dealing with the context of my, um, insurance company.

KATRYNA DOW: Absolutely.

MALCOLM CROMPTON: You've put in the other context, which is time – just simply through time, including because the relationship between two parties changes, it's through time becomes another change in context, and we've really struggled with that one. Gerd, I wouldn't mind asking if you could just round up on that 1. I was then going to come up with another question to go around the table. I'm not going to let that one out of the bag yet.

GERD LEONHARD: OK. The "Houston, we have a problem" question, right? My view is that we're entering into a new sort of ecosystem, a new logic. Some people are arguing on this is essentially the end of capitalism in a way that we know it. This actually relates very much to this. This ecosystem is essentially a networked society, a connected society. In this society, you cannot have what has been in the past called ego-systems rather than ecosystems. As you know, the oil industry was heavily one of those ego-systems – they used public property to make a huge profit and give nothing back. Sorry. And then generate a huge amount of profit. If the same thing would happen with data and what we do with this kind of new oil, then we would have a big problem, because we end up with new ego-systems – the large internet companies who do exactly the same, which is take all of our data, use it to their profit and give nothing back. That wouldn't work. Therefore, we are switching to this kind of that been called a circle economy. You take some, you replenish it, you put it back, you start again. It goes in a circle. That's kind of what's happening in a digital economy. That's where all of the new companies are trying to position themselves in such a way. Therefore, there is a mandatory thinking about sustainable in the sense of ethically and socially sustainable – what is going on today is not sustainable, because it's basically abusive. It's not necessarily by intent, but by consequence, it becomes abusive.

It is up to the companies who do this, and of course the users to not use them. But also, politics, to figure out how that ecosystem can be made complete. How to complete the logic of this ecosystem. The companies with this data have a social responsibility to fix the system, and we have the responsibility of reminding them of this, of course, as consumers, and the government has the responsibility of supervising that process. But not by overregulating it, clearly – this should still more or less be a free market, I suppose.

As far as the speed is concerned, I think that we should think about a mandatory thing for politicians and governments as to hire a bunch of people between 20 and 30, and put them in charge of figuring out what's what, because they know this. They can tell you in half a day how this should work. The problem is that most of the decisions are made bay people who are not actually users. They have their emails printed, then they decide what we should be able to download or not. That's just a bad idea.

(LAUGHTER)

Let's make get a bunch of 25-year-olds in there – mandatory, civil workers – and kick their butts to make the right decisions. In Europe, we have many city councils – the cities are the movers on this. Copenhagen, Rio de Janeiro, San Francisco, New York – chief digital officers who are 25 years old. I'm sure we would find volunteers who would do it for free!

NEW SPEAKER: Also, it's their future, too.

GERD LEONHARD: This would go a long way to solve the speed problem – bring in people who know what they're talking about, rather than guys like myself, who are digital immigrants, essentially. That would solve the problem, I think.

MALCOLM CROMPTON: I'm not going to ask questions about the average age of the people in this room, or the people who are in the age group of less than 25 or 35 or anything else. I promise not to.

Just think about it. That may be an issue – the digital maturity of any of the governments in Australia, I think, is something to think about.

JON LAWRENCE: Yeah, I think our Attorney-General has probably demonstrated that most starkly recently.

(LAUGHTER)

MALCOLM CROMPTON: A question for Liz – Teresa, at least – are you able to pull up the YouTube of Brandis explaining URLs to us?

(LAUGHTER)

Sounds like we've all seen it!

(LAUGHTER)

JON LAWRENCE: One point I was going to make – I think Gerd's right – there's a generational issue here. I remember handing in handwritten – or when I went to ANU in first year, I was told, "Look, you can hand in a handwritten essay, but here's why you don't want to." So I was very much on that border and immigrated into the digital space, but I think there's been – I think we've now got people who probably are about 25 who have come through the education system and have learned this stuff from primary school. That's something that obviously we didn't learn and I personally – I went back to university and did a masters not too long ago, and I was surrounded by 23- and 24-year-olds who really knew a lot more about how to behave on the internet than I did, which I found really quite insightful. I learned a lot from them, I have to say, because they'd learned it at school in a way that we never did.

MALCOLM CROMPTON: I'm actually going to start at Katryna and come backwards to make sure we aren't dominating at this end of the table. I'm interested in unpacking some more practical – for Australia – but remember what Gerd is saying, there isn't such thing as Australia anymore, there's only the world. We have to think about it within that context. What are the mechanisms you will put on the table for actually thinking about this at the right speed?

KATRYNA DOW: I think the really simple place for us to start from a self-education point of view and to kind of assess what risk or opportunity it presents in our life – the four ways that our identity or digital life is compromised potentially in some way is – our identity, who we are, the things that Liz has been talking about. The location we're at. Who our partner is. The car we drive. Where we work.

They're the things that are unique and personal to us. The next is our browser history. One of the big problems, particularly with the idea of metadata and our browser history being tracked, is that context is really so important here. A journalist reaching "How do I kill my wife?" is very, very different to having a bad day at work and Googling, "How do I kill my wife?"

It's really important that we understand that in context. The third is our preferences. This is the monetisation aspect. Then the fourth is what we intend to do. There's so much going on, particularly in the machine learning space, around trying to work out – and with a lot of accuracy – what we are likely to want to do next, based on what we have just done. I think one of the practical things that certainly we're very committed to helping people to understand is that when your data or information is accurate, if it's in context, if it's time-bound and it's matched with your intention, it's incredibly valuable. The idea of it being oil or currency or DNA – call it whatever you like, but that combination, and particularly for a generation that may not own assets in the way that we do, may not want to own a car, may want to collaborate in different ways, may want a distributed government, may want to have a shared car, a shared home, a shared career, then the assets that they have are very different to the things that we have grown up with. And to speak to Jon's point, we're starting to see that the younger generation have a completely different view of privacy – not that they are more privacy-oriented, but they realise the value associated with their privacy, and whether or not they understand how to create a persona or to be more savvy about how their digital settings work to their advantage. But if they start to see that the value of that information may help them navigate the world, then we're going to start to see a shift in behaviour.

MALCOLM CROMPTON: OK. Are you just saying, "Let's watch it happen?"

KATRYNA DOW: No! There are things we can do right now, absolutely. But I think the first thing is actually understanding those things in context. Because a lot of the apathy is, "Look, it doesn't matter. I have Google and I know they mine my emails." It's the combination of those things. It starts with understanding, "When I do that and I've saved 25 cents at the grocery store, my medical insurance has gone up by $2.50, "Or, "When I share something from a social point of view, I have now just been put into a particular camp from a political point of view or religious point of view."

MALCOLM CROMPTON: Is that just education?

KATRYNA DOW: The transparency -

MALCOLM CROMPTON: Arguably, we're as transparent as you can get.

KATRYNA DOW: Sorry?

MALCOLM CROMPTON: The internet is covered with all of these stories. It's everywhere. Does that mean you've got to improve the signal-to-noise ratio so it's actually understood? Do you need an education campaign? Does there need to be some leaders? Some law changes? What do you want to see different?

KATRYNA DOW: I think it's a combination of all of those. One of the problems with transparency is there's just too much of it and it's not simple. A 50-page terms-and-conditions document is transparent, if you've got the time to read it. But it's probably only – I'll give you a very quick example. A friend of mine the other day agreed for an app for his 6-year-old child. But 10 minutes later, he received an email with a recording of the children playing. He and his wife were quite freaked out about it. He tweeted me and I said, "Go back and read the terms and conditions." He said, "There's no way we would have agreed for our children to be recorded and then for it to be shared." Anyway, 20 minutes later, he tweets me back. "Yeah. Um, page 30, paragraph 75.2" or whatever – there it was. "We agree." I think part of it is surfacing that one clause so that people recognise this is what's happening – this is the exchange. In exchange for free, this is what it means. Because I think we're not getting enough cut-through with the type of education that we're focused on right now. We need these tiny sound bites that make it really clear when I do this, this is what happens.

MALCOLM CROMPTON: Education and context.

GERD LEONHARD: Can I comment?

MALCOLM CROMPTON: Yes, please.

GERD LEONHARD: I think what we are facing here is this thing that's been referred to as the Faustian bargain. That basically means that, when Gmail was first announced and other products of that sort – it was the best thing you could possibly get. It still is the best possible email you can get. We were so happy to get it for free. I went off Gmail a year ago because of this discussion with NSA and stuff, even though Google is one of my clients. It was a weird scenario. I'm paying $3,000 a year now to run my own email. Google has supplied that for me for eight years. The Faustian bargain is quite simple – we get all the value of the free app and the relationship and the social network and LinkedIn all this juice. It was very tempting. Now what we've seen, as about a year ago, the playing field has tilted. We thought we were getting all this – and we did – but now the exponential curve has fallen down, essentially. It's gone beyond the point of where it's mostly for our benefit. We need to get out of this Faustian bargain scenario and, as I said in my presentation, if you don't pay, you are the content, right? That means we may have to pay.

MALCOLM CROMPTON: Thank you. I want to make sure I come back to Liz. You next, please. Did you want to comment on how we get there, how we think it through?

LIZ SNELL: I think education is key. I agree with what's been said about that too. I think it's really important – this is in terms of everyone in the room – I think we've all got a role to play. I think it's the

technical designers, it's industry, it's government, it's the TIO, it's consumers, it's violence-against-women advocates – it's everyone working together to identify the issues and come up with solutions. Part of that is, as I talked about earlier, education programs that can help women, for example, who are experiencing the kind of violence we've been talking about, to understand more about the technology and also about how to enhance their safety. It's not about getting off. In terms of that, ACCAN has funded a program with WESNET, which I mentioned before, and the domestic violence resource centre, who are working together on an education program so that we have Australian-wide, Australian-specific education on this issue. Also, I think some practical things that perhaps industry and designers of technology can also be thinking about – what I'm saying is not new – it's something that a lot of people who are working in this area have been raising in their research and in their experience of working with clients. But if GPS tracking and all those other tracking devices – that's a serious issue with very serious consequences. Can there be a platform such that you press a button so you're no longer tracked anymore but you can still use your device or whatever to do what you need to do?

It's about being innovative to come up with some solutions about ensuring it's safe to use, but ensuring that you can still use it.

Another thing could be that technical designers or the telcos or internet service providers could also provide a service whereby people can take their device and get it scanned to see if there's any spyware or malware on it, and it's identified and removed. Of course, I'm saying all of this in the context – for victims of domestic violence, it's also important that they're seeking advice so they can spend time on safety planning before they go ahead and do any of these things. But there are some practical things that can be done as well. I think this is kind of possible if we have the dialogue, and if we're all talking, trying to identify the problems and, as I said, trying to come up with the solutions together. I'm of the strong belief that we all have a role to play to reduce and ultimately eliminate violence against women.

MALCOLM CROMPTON: Thank you. On that note, I promised to share the floor time. Now what I want to do, if we've got people with microphones, if we can wait for the microphones to arrive...

NEW SPEAKER: I first started working on the joining of technology and violence against women and it has come such a long way and I'm happy for that.

We've talked about the Big Brother idea and governments looking at our metadata. My experience and the data tells us most of the risk comes from people that people know, so from partners or previous partners. So the question is around not so much what we have to do about privacy but about user accountability when it comes to how we use other people's information, either on that intimate level or on the government level or on the marketing level. How do we get that accountability from the people using the info?

MALCOLM CROMPTON: I'm going to ask Liz to answer last on this so you can sum it up a bit. So first of all, I will ask Katryna, then Jon, then Gerd and then Liz, very quickly, so we have time for more questions.

LIZ SNELL: Very quickly, again I think it comes back to the issue of transparency, context and also permission. I think one of the ways that we all start to navigate things is around some usage rights and some transparency about how information is obtained and then speaking to Gerd's point, whether or not there is an nexus of, oh, I need to pay for something, which then gives me a layer of protection or additional context. But I think it's going to come back to this context around permission – how the information is collected, how it is used and what it is used for.

I also think – I recognise that the issue is specifically around women, but I would also like to draw us back to the idea of humanity. I think gender issues are very, very important, but I think in the not-too-distant future these will become issues from a humanity perspective, because women also have sons their care about their mothers being safe and they have sisters and so I think, you know, it's as much a community issue as it is a specific gender issue.

MALCOLM CROMPTON: Jon?

JON LAWRENCE: I think, just to pick up on that, I think that we really need to create a situation where people can give proper, informed consent. The example you gave earlier of, you know, a clause in a 30-page terms and conditions clearly is not informed consent. I think this organisation and the people involved in this sort of space, there's probably an opportunity for us to – and I know the information commissioner's office in the UK is doing something down this track to set up accreditation of privacy policies, but I think what we need is to get some fairly standardised terminology that's used in a privacy agreement, so that we can then have, for example, some little icons that say, "OK, well, at a glance you can see that this privacy policy is essentially just asking to do the normal things that you would expect and there's nothing else in there, you don't really need to have to go and read it because it is all fairly straightforward". And then, if it is not, that's highlighted upfront and it says, "Look, there may actually be some other things in here that you need to go and read". I think that gives us the opportunity, potentially, for us to have really informed consent and I think it's a food labelling type thing, is the concept. I think that's something we need to work towards.

MALCOLM CROMPTON: Is that something you think government can drive? There are an incredible number of efforts at doing that happening around the world and they are cancelling each other out a bit.

JON LAWRENCE: I mean government doesn't have a good track record of driving things like this effectively, I would suggest. So I think it's the sort of thing that should come potentially from the NGO sector or, you know, privacy professionals such as yourself, and so forth. But I think it's something that we need to work on and perhaps it is something we need to be working on internationally.

MALCOLM CROMPTON: Thank you.

KATRYNA DOW: We need a little symbol for the Faustian bargain – a devil or something!

JON LAWRENCE: I mean they are getting there with apps but there is no standardisation.

GERD LEONHARD: I think one of the problems is we shouldn't be using social technology to solve social problems. People are looking at things happening today and people are thinking "Oh, the internet can help this, we need to just put regulations in place", but these are social problems that are magnified by technology. For example in the US, if you made a campaign contribution it always had to be published. So if I gave $100 to a gay rights group or so, that should be published somewhere. But it wasn't possible to see it until Google developed something, and all of an everybody consist see that. So technology amplifies this. So if I'm going to be an idiot and make a fool out of myself in a bar now I can do this in a grand style on Facebook, right? It just amplifies it. So whether we should devise a technical solution to punish this, I'm not sure. I think these are issues that are probably going beyond the question of regulation or forbidding – these are magnified social issues. But I do think we also have the opposite. We have the possibility of solving some of these things, for example, that are already happening in peer-to-peer funding or crowd lending or all these things that are already happening on the positive side, so it is not all negative. But I don't think this is a technology issue.

MALCOLM CROMPTON: I must admit, in that regard, I do see some hope. One of the things I've watched happen in Australia over 20 or 30 years is the social attitude towards drink driving, in amongst a large part of the community. I'm not going to tell you what I was doing as a young driver, and people my age probably shouldn't be sharing what we were doing as a young driver but we were pretty full driving pretty fast cars at times. What is interesting about my son, who is about 30, it is something that he wouldn't countenance, not because he thinks he will get caught but because of the engagement program over a whole generation has been such that that is inappropriate. You just don't do that. And so it is actually possible to change social morays if you try and I find that a really interesting example for me, anyway.

Liz, over to you. I promised you last go on this one!

LIZ SNELL: I think we've kind of talked about some of the things insofar as we've heard about transparency, but transparency in a way that's easy to understand. I guess an example of that could be that privacy policies can be found with one click in a language that you can understand. But I think also in terms of, if I've understood you correctly, in terms of the user accountability too, I guess it's also about – and I will go out on a limb here. Do we need to be looking also at evidence laws and

how, for example, often we're finding, when our women come to us and say, "Look, all this has happened" and we've asked them what they've done and they've gone and reported it to the police and the police have said "It's just too hard". There may be a whole range of reasons why they're saying it's too hard. Part of that could be the technology and understanding that. Part of it may be, is there an expense involved in trying to access the information? But I guess it's about addressing that issue, so – and possibly in terms of evidence laws, can we have things like presumptions, a rebuttable presumption? For example, if it has come from an IP address that is a partner or ex-partner and you know them to be the only person who occupies that place, can it be presumed they sent it? Can there be other rebuttable presumptions with that respect to try and assist that usability and accountability.

MALCOLM CROMPTON: That should have really caused some controversy because a little bit earlier we heard the idea of perhaps we were moving too much into a society that was guilty until proven innocent and I do wonder whether, in order to produce that evidence more quickly and clearly, it needs to be collected and seen by others more easily, rather than obscured more easily. I'm not saying that I know what the answers are, but it is a beautiful illustration of the tensions of trying to solve that problem. We have the microphone with a gentleman down the back and I certainly see another hand up down here. But we'll see how we go.

NEW SPEAKER: Hi, Len Bytheway from ACCAN. I'm watching with a smile on my face. I'm thinking, for example, I get a lot of ads now about mobility scooters and old age devices because I Googled new batteries for my father's device! And now all of a sudden I'm branded. That's fine, I can live with that, that is not a biggie, but you can sort of see how that might go wrong. I'm sort of seeing this twist. On the one hand we need evidence collected so we can prosecute but on the other hand we need evidence not collected because it can be used. I'm a geek, hands up, on the other hand we want protection against the potential things that we can use it. We say in the old days we had – you know, I fix my Facebook settings, I get my privacy right and I'm good. But that's not like that anymore. Once we have the internet of things, everything is dobbing on you and putting stuff on there. So instead of having a single point of contact, where you can tighten up the screw, we now have a universe. So I think the only single point – well, the single confluence of all of that is yourself. The only place that can control your privacy and either loosen the screw off and let it go because you like the benefits or tighten it up because you don't want to go there, there's only one place you can do that. So that, to me, lends the idea that we need to have a new digital literacy, where people know what's going on. It's no point installing the off switch or the tap at the bottom of Niagara falls, it's too late, the water is coming over and we can't stop it. So we have to stop it at the source. I think the only way we can do that is by some sort of digital education process. I would be interested to hear what you have got to say about that sort of concept.

KATRYNA DOW: Can I just jump in and quickly pick up from what Liz mentioned and to reflect back what you said? We have, in society, mechanisms, again for context and use rights, and that is, you know, when a couple cohabit and then that ends, you know, it's very clear there is a protection in terms of who resides in the house and who doesn't, or who is on the insurance policy or who gets to operate the bank account. So I think we actually have proxies, or we have examples, of this already. And so it may be some of the more intimate things of life, you know, you come off the bank account, you move out of the house, and you don't have access to these sorts of things, and it is contextualised. So I think that's one aspect of it.

But I also think that a lot of this is actually working through the issues around our humanity and the environment that we want to live in and the society we want to live in. That conversation happening – at least in parallel, or as much as possible, into the foreground. Because I think so many of the technical things we want to solve are binary in their nature, and life is much more grey than it is black and white, and all of a sudden, if you go straight for opt-out, there's a lot of convenience factor that is then removed from life and I think we want to try and get away from this either/or and start exploring the "And", because we've made "And" work in other parts of life. I'm optimistic that we can make the "&" work with technology as well.

GERD LEONHARD: Yes, well, I don't agree with your assessment on the situation there. I think the responsibility of being safe and doing the right thing and minding your data and stuff cannot be with the individual primarily, because most of us don't know how to do that and have no north and cannot understand and don't know how to how to use encrypted email and what not. This would be like

saying you are going to vote on the nuclear power plant. Which in principle I don't think is a bad idea but who can decide that? It takes a lot of knowledge to decide that. I think ultimately when you are talking about the dangers of a digital society, which includes the taking over the artificial intelligence and losing jobs and all of that stuff, right, that is down to the platforms and companies who are providing it. That should be part of their mandatory service, that they keep us whole, so to speak, right?

Second, the government and organisations around the government. And then, third, us. But this would be like saying, OK, you are downloading music because you cannot get it legally for the same price and so therefore you are guilty because you have downloaded, right? But it is the opposite that is true. The system is dysfunctional and therefore all I can do is download illegally. We can't reverse this order. That is crucial to understand. We cannot be held responsible for a system that in itself does not allow it to be functional. And that, I think, is an important point.

JON LAWRENCE: One of the things that I find interesting – and sorry to return to the motor car analogy, but it works so well, I think, in many circumstances. The first car I owned was made in 1959. I was rebuilding it in the 1970s and I understood every nut and bolt on that car and how it worked. My current motor car, I'm not even allowed to fill the darn thing with oil – I have to take it in. The point is, that car has more computers in it than can land on the moon. It is beyond my comprehension to understand how that car works. And the decision that I took simply to trust it was a rational decision in the sense that a whole series of third parties essentially assured me that this was an OK car to drive. It goes back to those safety standards again. So there's not necessarily a linear correlation between understanding and what we do. At some stage we do ask society one way other another to step in and put the guidance in place. We did that that way for the motor car. We've made it illegal to sell our own kidneys because again we think we can't make rational decisions about something as intimate as parts of our own body. We can give away our kidneys – we just can't sell them.

We're having the same debate, if you don't mind me saying so, about commercial surrogacy. I don't know what the answers are on that and I don't think anybody has really thought it through properly. We can't yet. We're going to have to have a lot of conversation but eventually there will be laws about it one way or another. So we need to be very careful about transparency.

Now, we have, I think, two hands in the air and I'm not quite sure where the microphone has been delivered. This gentleman has been waving his hand the longest, if you don't mind me saying so. I think this might have to be the last question because we have a couple of little things to do at the end.

NEW SPEAKER: Thank you very much, I'm from the University of Wollongong. I'm just wondering about people with disabilities because in some respects, the technologies they use are very much part of their life and really don't have an option of, say, opting out, if they did want to protect their privacy. So I'm just interested in terms of what the panel thinks some practical solutions to that issue are, like I'm thinking about the Meeco website in terms of is that an answer? But I don't want to try and necessarily put answers in there. I just want to actually raise the question because, up until now, we've talked about young people and we've also talked about women. I mean, people with disabilities are another vulnerable group, and also people of age, but I think I will leave it just to people with disabilities for this point.

MALCOLM CROMPTON: I will run counsel the table really quickly. Jon, please start.

NEW SPEAKER:

JON LAWRENCE: That is a good question. I'm not sure I have a lot to add at this point so I will pass and see if it comes back.

LIZ SNELL: I think it comes to education again, in terms of people better understanding how their data can be used and misused. I take Gerd's point about, obviously, we can't go into the learning and how to use encryption and all of that kind of stuff but if people have a better understanding they can make an informed decision about that. So for me, I think education is a key part of that.

KATRYNA DOW: I think education is important but I think is simple place to start is with some architectural approaches like privacy by design and so many of the products and services that we use

now, the default makes us the product. Whereas if the default was for us to actually explicitly turn those services on, instead of having to be educated as to how to turn them off, it means that we actually start out with a greater sense of social responsibility for the organisations that provide those products or services, and we happen to educate ourselves along the way as well. I think what it means is, for any vulnerable group, you've already designed something with their best interests in mind. So I think that is a simple way to start from an architectural point of view.

GERD LEONHARD: As far as disability is concerned, I think technology has some pretty amazing things coming up to address – well, it already has that, right, but we should give that all the firepower we have, clearly, to solve people's problems if they are disabled or sick or old. And the flip-side of that is that some of the same technology is used for, you know, military purposes and vice versa. It creates a moral dilemma, which nevertheless means that we should still do it anyway, but we have to figure out a way of saying, OK, I can help the quadriplegic walk again using an exoskeleton, but does it mean I should allow a soldier to buy one and become a super human? It is the same technology. So this is clearly calling for some judgment on who should be able to do what. And somebody will have to look at this and this is why we need the 25 year olds to look at this!

MALCOLM CROMPTON: Amazing. Thank you,

Now, Teresa, I think it's over to you, next, isn't it? Aren't we going to play a YouTube? What we're going to do is to play one of the YouTubes that relates to the checkout program on the ABC and then we're going to ask our panellists to come up with what they would want. Can we play the YouTube clip first, please?

(Video played)

NEW SPEAKER: Hi, I'm Timothy Pilgrim, Australian privacy commissioner. If I could say one thing, it's take control of your privacy by asking why an organisation wants your personal information before you give it to them. If you're not sure why they're asking for your personal details, ask them to explain why they need it. Our research shows that one in three people have had a privacy problem in the last twelve months. Don't let it happen to you. They can be long and boring, but it's important to take a look at an organisation's privacy policy to get a sense of how your personal information is going to be used, stored, shared and whether it will be sent overseas. 60% of Australians say that they've chosen not to deal with an organisation because of privacy concerns. In March this year, privacy laws changed to give people stronger privacy rights. Businesses must now be more open and transparent about how they handle your personal information. For example, you must be given a simple way of opting out of being included in marketing lists. If you don't know how a company got your information, ask them. They're legally obliged to tell you where they got it from. Your privacy is important. To find out more about your privacy rights, check out our website and www.oaic be .au

MALCOLM CROMPTON: So that was Timothy's "If I could ask for only one thing" as he put it out on the program a couple of months ago. I'm now going to ask the panellists to give us their, "If only I could ask for one thing" in response to the session we have had so far. And I don't know what I'm going to do this time – I think I might do Katryna and Liz and Jon and Gerd. Go for it, Katryna!

KATRYNA DOW: Me again! I think, in the spirit of anarchy, I would like to see us flip the model. I think we're so used to an organisation issuing us with a privacy statement, I look forward to the opportunity for us to issue organisations and governments with our terms and conditions for the use of our information.

(APPLAUSE)

That's actually something we're very committed to doing. That's where I would start!

LIZ SNELL: I think, in addition to that, the take-home message for me, too, is that we can all work together to try and find solutions to how technology can be misused and it's about taking up those opportunities.

JON LAWRENCE: I was going to give a very practical little suggestion, which is, if you have a smart device, install a battery manager in it that will turn your wi-fi and GPS off when the screen is dark.

MALCOLM CROMPTON: Even though that's when all the updates and patches and everything else gets installed?

JON LAWRENCE: Erm, no, no, you do that at home on wi-fi, so you don't use – but it has the benefit of not broadcasting all your wi-fi information and tracking your GPS location and also probably it triples the length of your battery life.

MALCOLM CROMPTON: Thank you. If I could only have one thing it would be to thank you all for being here, to say that the future starts now, and you have a role in it. Thank you very much indeed to our panellists. Especially to Gerd for coming such a long way to deepen our thinking. And now I'm going to hand it over to Teresa who has one more announcement for us.

TERESA CORBIN: Thank you very much panellists and Malcolm. We have a small gift as appreciation.

(APPLAUSE)

I would just like to invite Deborah Forward from the National Relay Service to come up because the National Relay Service is sponsoring our networking lunch today, so they've got a brief message for us. Thank you very much for being our sponsor.

NEW SPEAKER: Thank you. It is a very brave person who stands between conference parliaments and lunch, I think! So I will make this very brief. I'm from the National Relay Service, the phone solution for people who are deaf or have a hearing or speech impairment, and we've got exciting news and that is that there will be an NRS app launched before the end of the year. You may have known the NRS in various guises through different sorts of technology over the last couple of decades, but we have an app coming.

So, we're very pleased about that, and in fact we're aware that it is the first time that any relay service in the world will be providing access to a range of relay calls through a single app. We're very proud about that and we hope you, as Australians, are proud of the Australian National Relay Service, too. It will be particularly useful for people who use Speak and Listen to make a relay call or people who use internet relay to make a relay call and you can find out more about that at our table outside. Some of the advantages in making those calls through the app will be that you can pre-store messages, pre-store call set-ups that make your actual calls easier and more personalised for you – a big abandon for people, particularly with physical disabilities, where entering information each time can be complex. You will be able to click through from your contacts stored on that personal device, whether you've got 800 or 8,000 contacts, they will each be able to clicked through to insert into the call, rather than needing to be typed in. And there will also be a much clearer sense of when you've got an incoming internet relay call. So this sounds a bit like jargon, if you are not familiar with the NRS, but we are very lucky that we've got a table outside there and some staff to talk to you about the app, and you've got one of these in your bags. The app is likely to be launched before the end of the year, details still being finalised, but I do ask you to go to that table and it is between here and lunch, but go to that table some time today and get some information about the app. Or leave your details and we can make contact with you when that is launched or keep in touch via our website. Our staff can also talk to you about your organisation becoming relay service friendly, inclusive in that way, and your staff being relay service ready – a simple process that we can step through with you. So lots of benefits. On your way to lunch, stop at the table.

TERESA CORBIN: Thanks a lot, Deb.

NEW SPEAKER: Is it go now?

TERESA CORBIN: Yes, let's go and have lunch!