>> We've got four awesome contributors for the topic today, which is looking at social media and children - is a total ban or is age verification the solution? The way I'm gonna kick off is I'm gonna invite each of our panellists just to share a few opening thoughts and remarks. I will introduce each of the panellists as well before we get going. Some protocols - we have the auIGF Code of Conduct, please refer to that. Participants either in the room or online that fail to adhere to our Code of Conduct, we may ask you to be removed. Please log in to Zoom using your first and last name, not your company name and not your nickname, please. We want to be able to identify everybody, particularly where they're coming from and what perspective they're contributing from. So, please state your name and if, indeed, you have an affiliation when making comments or asking questions. The format for the next, kind of, 50 minutes, we're gonna do three or four minutes each opening up. We're gonna go into some deep middle-part conversation. I'd like to invite questions from both online and from in the room. But what I would like to request when you're thinking of your question, simply because we only have about 50 minutes, I would rather not take specific questions for sole panellists. I'd rather take questions where you abstract up and out, and think about, "Is there a big question that I think at least two, if not all the panellists, could maybe make a contribution towards answering?" So, please give that some thought. And then we'll kind of try and bring it to a close in the last 10 minutes or so, looking at some key takeaways. I'll be asking each of the panellists to think about what might be one or two things that they would like you, the audience, online and in the room, to take away. So, with that in mind, I'm going to introduce our speakers, and I can't see... I'm just loading up Zoom and I want to make sure that my two speakers are online, because I can't see them. So, I'm just going to multi speaker. I still can't see them, so I'm presuming that Lizzie and Jenny are both online. Eek! How do I, as the moderator, know that my panellists are online? Andrew, can you give me confirmation that Lizzie O'Shea and Jenny...? I got thumbs up. Hi, out there! Jenny, I'm gonna ask you to kick off. There's Lizzie, thanks. Welcome, Lizzie, from India. Jenny, I'm gonna ask you to kick off with some opening remarks. Jenny, I'm going to ask you to pass the baton straight to Lizzie. Lizzie, when you're finished, pass the baton back to Melbourne here in the room, and I'll get either Pyrate or Zoe to pick up from there. We have four - in fact, five - amazing women. In my 30-odd years, it's been fun to see women grow in size but to run an all-female panel is pretty cool, so happy about that. We have Jenny Duxbury, who's the director of policy and regulatory affairs with the Digital Industry Group. She will be bringing an international but also an industry perspective to this dialogue. Lizzie will be joining us - Lizzie O'Shea is joining us from India. Lizzie is the founder and chair of Rights Watch -- Digital Rights Watch but also a principal at Maurice Blackburn Lawyers. And Lizzie is going to be bringing a civil society perspective. We have Pyrate Passell, first session, first real session that she will be presenting today. She's representing end users - like me - but also is a member of the Dynamic Team Coalition, so brings for us to this conversation a really critical perspective because of her age. So, thank you, Pyrate, representing "all" people that are younger than us, the rest of us!

>> PYRATE PASSELL: No pressure!

>> SANDRA DAVEY: And then we have Zoe Hawkins, the head of policy design at the Australian National University's Tech Policy Design Centre, bringing an academia and civil society perspective to this conversation. And true to the multistakeholder model, we've got a variety of perspectives, and we hope that this will be a dialogue and a discussion, look for some common places where we can land together, looking to also identify any of the pivot points or the constraints or tensions that exist in this topic. If we get straight to it, Australia is looking to impose penalties on social media platforms. You know, Australia is actually looking at legislating a national minimum age for social media access, and according to Minister Roland's address at the recent Social Media Summit, the Government understands that communities and parents are concerned about the harmful impacts of social media, and they want action. I have read that out - that the government understands parents and communities are concerned about harmful impacts of social media and they want action. I've read that out because I can't find the problem statement. I can't find the ban is a solution that we're discussing today, but I can't find the problem statement. That's the closest that I can find to a problem statement. So, if somebody in this room knows what the problem statement is, me, as the moderator, would really like to know! So, I'm taking a guess at it, but the Federal Government is concerned about that parents and communities are really worried about the harmful impacts of social media and they want action, and that a ban on age or some kind of age verification is the solution. Let's, without further ado, Jenny, if I could ask you to share some opening remarks for us, and when you're finished, hand the baton to Lizzie. Thank you very much, and welcome, Jennifer.

>> JENNY DUXBURY: Hi, everyone. I hope you can all hear me clearly. I would just like to begin by thanking the organisers for the invitation to speak today on this very important topic - social media and children - is a ban the answer? And I must say that I do agree, but answering this question is difficult because the problem that we are being asked to solve with a ban hasn't been really clearly articulated, and it isn't clear what the outcome is that we hope to achieve with a ban. Are we hoping to improve the attention span of children within schools, reduce digital distraction and improve learning outcomes? Are we hoping to improve mental outcomes, health outcomes, for young people? Are we hoping to keep younger people safer online by keeping them offline until a particular age? These are all rationales that have been given for the ban. But exactly what it is that we hope to achieve here isn't that clear to me because all of those things that I've just referenced are actually complex social issues. And in relation to online safety, I think it's really important to bear in mind that the work of keeping young people - and adults - safe online is an ongoing task. And, you know, there is a lot to do in developing appropriate regulatory settings, and there's going to be many opportunities to improve how industry responds to the challenges of keeping young people and adults as well safe online. So, it's really hard to have a considered view at this stage as to what is being proposed in terms of this ban, other than that there is a basic rationale which is limiting young people's access to social media and other unspecified digital services is desirable until they are at an age where they are developmentally equipped to deal with the challenges of being in digital spaces. So, we don't know yet what is the minimum age that the Government has in mind, although South Australia has proposed 16 or 14-15 with parental consent. We don't know the range of services in scope. We know social media is in scope, but if we look at what's been proposed in South Australia, there's a very broad range of everyday digital communication services that are potentially covered by these restrictions, including email, MMS, SMS, websites or apps that facilitate user interactions - such as messaging services - gaming services, informational and entertainment services, app stores and search engines. So, that's the majority of services that most people will use to access digital spaces by their smartphone. Most importantly, it's really not clear how the Government expects the ban to be implemented, because - especially if it extends to such a broad range of services - the Government has acknowledged that age-assurance technologies are immature, that there are concerns about the reliability of current technologies, that they have privacy and security implications, and that some of these requirements might actually operate to exclude and disadvantage some groups - so, increase digital exclusion. There isn't an industry standard for age assurance. And while there is an age-assurance trial currently in train, we don't yet know the outcome. What we do know is that this is a very polarised and politically charged issue. We do acknowledge that there's considerable community concern about the issue, especially from parents and carers. And we also know that there's a fair bit of politics around this, and I think Zoe is going to talk to that a bit later. Experts are divided about the extent social media contributes to poor mental health outcomes, or poor learning outcomes. And so I don't really have an answer to the specific question that's been posed. But I do think it's important for people to appreciate that there is a lot of work going on in the online safety space as we speak. There is a statutory review of the Online Safety Act that will be concluded very shortly and we'll know about what changes to the legislation are being proposed to improve safety outcomes for young people. And the industry has also released codes for consultation, which - if accepted by the eSafety Commissioner - will be mandatory. That will be aiming to protect children from a range of harmful content, including suicide, eating disorder, and self-harm content, and pornography. And the last thing I'd just like to say is that one of the things that I think it's important to appreciate that social media has done to benefit young people is that it's given them an opportunity to raise their voices and demonstrate their capacity to advocate for political change on issues that impact them, issues such as climate change, gun control, and abortion rights. And it seems to me that, in this instance, the Government should really take special care to elevate the voices of young people in this debate, to listen to what they have to say and give their views careful consideration. And I hope that the Government can allow enough time and space to allow young people to meaningfully participate in this decision, as the citizens that will be most impacted by the decision.

>> SANDRA DAVEY: Fantastic. Thanks, Jenny. Lizzie, let's go straight to you.

>> LIZZIE O'SHEA: Great. Thank you so much. Hopefully, you can hear me, but someone l I'm sure, tell me if you can't. I am founder and chair of Digital Rights Watch, Australia's leading organisation advocating for human rights in online spaces. And I am grateful that - I'm grateful to be part of this panel and I think civil society has got an important role to play to advocate for better policies in relation to online safety. I wanted to thank Jenny for putting some of the specifics into the discussion because it's not always clear what's meant by age assurance, because it can mean multiple different things. There's no clear alignment on what the technology is. But I would just take the opportunity to give a little bit of background. Originally, the proposal around this was around accessing adult content, and quite particularly pornography, and that was, in fact, what the eSafety Commissioner was charged with doing, in creating a road map for age assurance quite a while ago now - well over a year ago, possibly two, I can't recall off the top of my head. But the point being that this has evolved since then. Originally, the Government rejected the road map to age assurance because the technology wasn't up to scratch and there were a variety of problems with implementation, which I think is interesting. And then since then, have reversed the position, in a somewhat obscure manner - not necessarily with clear paradigms for what age assurance would look like, possibly at the behest of state governments pushing the Federal Government to lead on this. But the point is that we are operating in a space where there's no clear proposal, let alone a clear problem statement, so we are at something of a challenge in terms of responding to it. What we do at Digital Rights Watch is try to bring a human rights approach to the problem. So, that is to say that there may be very serious problems with young people accessing content that they shouldn't be, or don't want to access at that particular time in their lives, and there may be other issues around giving them access to what might be classified as a dangerous product - that's, of course, contentious. But a lot of the proposals around age assurance require an invasion of privacy, and interference with privacy. Privacy is not an absolute right, and it may be that it's worth interfering with the right to privacy in order to allow other people to exercise their rights. However, the problem is you need to justify an invasion of privacy using a human rights approach, it's required that it be reasonable, necessary and proportionate for a legitimate purpose. And, you know, we haven't seen the basic paradigms of the debate set in terms of policy, but I don't think we've seen evidence that kind of is justified. To impose any kind of age assurance regime provides widespread invasion of privacy, interfering with young people's rights as well, which is another set of rights that's not clear that that interference is justified either. But even from a basic privacy perspective, it requires most Australians to have to experience interference with privacy, and we don't think that process has been gone through to justify it. Now, what I would say is substantively the problem, if I could try to articulate it, is what's somewhat discussed by the eSafety Commissioner in her road map. If anyone hasn't read it, I think it is worth reading just to get across the material. She pointed out that this is a very complex issue. The research is often contradictory, about harm caused to young people, or how they experience online life. And where she ended up, I think, is quite a sensible spot. She observed that public perceptions research indicates that there's a broad basis of approval for age assurance technology, but low confidence in the successful operation of it. And I think many people share that feeling. And that's what justifies the political climate that gives rise to this proposal, but then upon reflection I think many people remain concerned about it. What I would say is one of the things that's driving this is that I do think social media companies have not upheld their social licence to operate, and that has created problems. I think we do not see enough transparency in how algorithmic models of amplification of content are designed, and many people remain extremely concerned about that. And there is a need for industry to come to the table and accept that there may be harmful consequences of their products, and do something about it. To that end, we argue that the number-one thing that the government can do at this present time to protect young people is to implement bulk privacy reform for children specifically but also for adults, because that will address the data-centric business model that is focused on extracting information at quite costly consequences for society and people. It leads to... That data-centric business model that is focused on engagement leads to all sorts of negative impacts, such as extended time on devices, prioritising engagement above all things means that more polarising content is promoted because it's more engaging, which creates a spread of mis- and disinformation, extremist content, and the like. So, there's a range of reasons why privacy reform is quite important to cleaning up the information ecosystem that is experienced by young people, as well as adults, and that it's a much less privacy-invading policy solution than what is commonly proposed when we talk about age assurance. And what I would say generally is that the public also support these kinds of proposals. We're about to release a report about the tension between privacy and safety, and we did some polling to go with that report, and it indicated that many people understand that privacy is extremely important, alongside safety, and do not necessarily pitch them one against the other. And what I think that demonstrates is there's an appetite based there for policymaking that is much more sophisticated than what we've seen on the federal and state stage. Not sufficient engagement with the complexity of the issues, not a sufficient courage for dealing with business models that are predatory and harmful, and not enough listening to particularly young people who have got a lot to say about this ban, who have got a lot to say about how they use social media in ways that are useful to them, but also the ecosystem could be improved. And research on that, I think, needs to be elevated and platformed. And so I would really compliment auDA as well for having a young person - I sound like an old person talking about a young person - having youth represented on the panel, because too often I think that voice is excluded. And to that end, I might hand back to Melbourne.

>> SANDRA DAVEY: Thank you very much. And maybe we'll kick off with Zoe, and then we're gonna go to Py. Py is gonna kick us off with a video, so Zoe is gonna make some opening remarks and then I'm gonna cue the people at the back for the video, and then Pyrate will add a few thoughts after we've watched the video. Zoe, over to you for opening remarks.

>> ZOE HAWKINS: Thanks, Sandra. Wonderful to be here today and great to be on such a powerful female panel, and great to hear the comments from Jenny and Lizzie online. Unsurprisingly, both of whom have made excellent points that were some of the ones I was gonna make, but a great opportunity to riff off this. I love the provocative title of this session from the organisers. I think that I want to pick up on this point about, "Is a total ban the answer?" It does depend on the question, which is a topic Jenny touched on. But regardless of what the question is, there's never going to be one answer. So, even just the point about is it THE answer? Even if a ban is one of the answers to the questions we're asking, it's certainly not going to be the only one. So, I think, moving away from a binary sort of mindset on "is this a silver bullet?" That sort of silver bullet mentality, and we all know that that's not gonna work in this space. And I'd actually like to push us all in this conversation a little bit because I think this point has come up about, "What's the outcome we're seeking to achieve?" And then we've listed - and Jenny did a great job of identifying some of the possible harms we might be looking to mitigate, whether that be screen addiction, exposure to harmful content, mental health issues, things like this. But I think we can be more ambitious to talk about the positive vision that we have for kids and their online experiences, and actually all Australians and their online experiences. So, really, I think the first point of call is - and, Sandra, you're not wrong, I don't know that there is a clearer problem statement from the government right now - lots of great research and work done across eSafety and other parts of government, but I think we're all grappling with, "What is this coherent outcome that we're striving for in a positive framing?" And I think that part of the way of getting there, and Lizzie has already touched on this, is moving past the Whac-A-Mole and silver bullet mindset. There's part of the online safety Act review of the need for content take-down only, although that has an important place in the harm minimisation area. At the same time, we need to think about those business models that are fuelling a lot of these harms, that go further up the food chain in terms of where this is coming from, which is what Lizzie was getting to the role that privacy reforms can play. And so it's really great to see how much enthusiasm and speed the Australian Government is willing to put behind these potential age restrictions, but I think some of that energy could be better directed to moving some of those privacy reforms ahead a little faster, as I'm sure Lizzie would agree. But I think just to add to that, another lever that we have that could more fundamentally help us design a positive social media future that we might want to engage in and aspire to, rather than just look to contain, is really tackling that business model also through transparency. I know that this is something that the Australian Government does have existing transparency powers, but they are relatively narrow. And so how do we actually unlock - how do we harness - to Sandra's point about this - understanding of community's consent and parental concern and worry about the state of social media offerings and experiences for kids? Instead of taking that and saying, "OK, we accept the negative outcome of social media as it is, or as we perceive it to be, and therefore the only solution is to put it in the bin," how do we say, "Well, actually, how do we use that as consumer voting power through transparency to unlock that competition? How do we turn the business incentive around through transparency so that parents can choose and help vote with their feet with their kids as to where they can have their online experiences and hopefully drive towards some more positive options for everyone?" I think in this conversation we will get into the devil in the detail, so talking a little bit more, as Jenny already alluded to, as what do we mean by social media? That list can be long, particularly when you add a lot of the other digital services that people are considering. And how do we make sure that this isn't, you know, that this is done in consultation with young people? Which is why I'm really pleased to have Py on the panel as well. I will leave my opening comments there and look forward to the conversation.

>> SANDRA DAVEY: Lovely, thank you. We might roll the video.

>> Hi!

>> Hi, I'm Pyrate, your game host. Today we are at Australia's biggest gaming festival, asking the young people who lived through the dawn of socialising online, also called social media - what they think about possible age restrictions on teens accessing social media in Australia. And probably elsewhere. This round did not end like I expected.

>> Nice to meet you. So, what do you think about the Australian Government putting laws where you will have to verify your age on social media to use certain features or even...?

>> Honestly, social media ruined my teenage life 'cause you're always thinking, "What can I post on there? What are people gonna think of me?" And I think there should be an age limit just so teens can enjoy their life.

>> I think it's good. One of the biggest regrets I have is unrestricted internet access. You get exposed to a lot when you're younger and I don't think it's good for the younger generations.

>> I do think there should be some sort of verification.

>> I think it's probably a good idea for a lot of teenagers, well, especially younger teenagers.

>> Yeah, I'm all for it. Perfect.

>> You need to have a safe environment and know exactly who you're interacting with.

>> I think if the ID verifying is safe from a legal perspective... It is smart. From a public's perspective, it can also just be really uncomfortable. Not in a position to have an ID, or people who don't have, like, access, or anything like that, it's very unfair to them.

>> Probably a good thing, so younger kids aren't getting influenced by social media as much, and just having a childhood. I also had it as a young age. I had access to the internet and it wasn't a good thing!

>> Difficult to think about how they would enforce the verification, how they would do it, what mode would they try to use? It just seems like you can get around that with fake IDs...

>> I have younger siblings. For certain, definitely think this should be a security thing. But anybody 16 and older, they're gonna do anything they want!

>> Social media pretty much ruined a lot of my high school. And it's made it hell. I feel like under-16, if you have... If you're being attacked by people, that's kind of, like, when the worst age is. Because you don't know what's going on and you just, think, "The world hates me."

>> When you're older, you know when to log on.

>> I'm not so sure about that. What do you think? Should teens be restricted from accessing social media online? Tell us in the comments below. the comments below.

>> Thank you. Despite the video, I think it shouldn't be a thing where you should have the freedom of speech to express yourself on the internet, even as someone who is younger, speaks a teen myself. I feel like it's important to have freedom of speech and to have the ability to do what you want on the internet as your own person and I know there's a lot of awful things that can happen there but there's also the fact this is a new generation where people don't, can't really do the things you guys used to do when you were younger. Like, we can't go out to the mall anymore. Well, we could, but it's kind of risky. And I feel like we have the right to express ourselves, even if it might be dangerous. And I think social media apps should work more on their algorithms and work more to make sure the children are safe rather than banning it outright. I personally wouldn't probably be here right now where I'm sitting if I didn't have the opportunity to go online.

>> One of the things you've said a couple of times is how surprised you were at the number of responses from young people agreeing there should be some sort of age verification. When you and I unpacked it a bit this morning, we were talking about to what extent, how do we balance I want access to the internet, I want to be able to roam, but I also want social media companies to take some level of responsibility, particularly for the algorithm? Can you give us a bit more color about what you were talking with me this morning when you were talking about the algorithms and the role that social media companies play?

>> I think it's important for them to moderate their content, as well as have a safe environment for children. And I think it should be more accessible to people, like parents or guardians, to have a bit more of a choice on what their children post. I notice a lot of children who seem to be traumatized, used to have a very popular social media accounts, or some sort of account where they posted super personal stuff and it ended up really biting them in the back later. And I think there should be an option to prevent that but not dan it outright.

>> Thank you. I want to pause back a bit and I'm thinking about if the government has a desire to do something by the end of the year - that's not very far away - we know how complex the policy space is. I want to pose a question to all the audience and maybe because we have two online and two in the room, Lizzie and Jen, we might go to you. If you have anything to say on this question. It seems that age assurance or verification is a solution but I wonder what do we know of other interventions that might address concerns about the impacts of social media on young people? What do we know of other good works that are being done or other interventions? Has Jenny or Lizzie, perhaps Jenny first? Can you comment on that?

>> JENNIFER DUXBURY: What I can talk about is there is a lot of work going on in this space at the moment. Lizzie has rightly pointed out the importance of privacy reform. And the privacy proposals ifclude a proposed children's privacy code which I think hopefully will be an important piece of the puzzle. I mentioned the release of the industry codes for public consultation. And I would really urge people here today to think about making a submission to that industry consultation, because that does cover a range of issues. Some of the worst content which has been of concern, as I mentioned, around pornography, suicide-related material, eating disorder content and so on, self-harm content. Those codes also have proposals in relation to algorithms which is something both of the other speakers have mentioned. So there's a lot that can be done. There's various other suggestions that I've heard and I'm not going to make a comment about those, that go beyond just regulatory interventions. For example, steps that parents can take to better understand their children's social media usage. I recently attended the social media summit that was put on by NSW where one of the American experts was strongly advocating giving younger people a flip phone rather than a smart device to restrict the amount of time they potentially have online. So there's a lot of potential interventions. I also quite like the suggestion from mental health organizations and there's about 100 of them I think that have really, have registered concerns about the proposed restrictions. And that is around initiatives that are targeted at increasing digital literacy across the whole population. So including parents and children. And also potentially around ways that we can think about co-designing social media spaces with the input of young people to ensure that some of the concerns around young people have around their experiences online are appropriately factored in to designing appropriate solutions.

>> LIZZIE O'SHEA: I think it depends on what problems we're trying to resolve. Is it kids spending too much time online and not getting out on the sporting fields. Lots of people live quite fulsome lives online and make friends and do interesting things. However, I understand why lots of young people in particular and if you poll them, say they support a ban because many adults don't like the space. It is interesting to talk about some of these proposals and see how they could be extended tew as well. The online code could be modeled on the UK model. It recommends things like collating notification, those kinds of basic things that should be I think most people would benefit from. And it's interesting that social media platforms have started to respond. It's a shame it took to this point for these companies to put proposals that are specific to young people that would improve or have been called for for a long time and improve their environment. Maybe that's part of the process but that I find to be disappointing because I think it could have happened at any time. Social media companies could have followed the UK children's code. We could do things like prohibit advertising and things like gambling. One thing about young people if we gamified sport and be exposed when they turn 18 to various predatory industries for alcohol, gambling and the like, that's a very serious I think failure on our part to support them participating in online life in a constructive way. That kind of proposal would benefit many adults. There's a whole other scheme around mainly to a large degree what the online safety scheme is looking at which is protection of children, protection from criminal content like pro terror content, child sex abuse material and a whole other issue and potentially also addressed according to some by limiting access to social media but I think a much more complex problem and a range of different policy interventions that are available that are being researched with that issue. Multiple different problems and the political environment is conducive to it and we do need to build up the capacity for Australians to have meaningful conversations about right, proposals, harms and giving young people freedom, while also saying there are too many large social media companies who have neglected to uphold their obligations as a product service provider to be safe, to prioritize safety over profit. That is a problem we're having to deal. With there's no way we're shying away from that and that's what fuels simplistic policy debates. I wouldn't want to walk past that because I think it is a problem. Young people saying how awful it is for them. Let's find ways to promote safety and transparency particularly around making sure we know what it's like to go online and give people meaningful choices. Not impose obligations on them and give them choices that are meaningful about knowing what they're exposing themselves to and working out if they want to see something different.

>> Just as something to mention, having this implicated in their government as well which is Norway. You do the age verification. How would you, if you in the scenario where you moved to Norway and you need a visa to verify there, how would you, if you moved to Norway, how would you - thinking... Yeah. If you didn't have a passport, which I don't, how would you talk to your family? My friend, they use Facebook to talk to their family and if there was a verification for that and they didn't have a visa or a passport - I don't have a passport and I'm 16 - if they didn't have that ability, how would you talk to people that you care about? I know there's always messages but there's people that use other types of apps as well and I think it's important to allow that communication because my friend, as I just said, wouldn't be able to talk to their family anymore.

>> You're raising good questions around the implementation and the how. This will be complex to implement it. I wants to actually, Zoe, if I may move to the process, and talk about the policy process. Partly because of your background and a couple of the other speakers talked about how do we, how might we co-design a process or what indeed does the process look like? I want to unpack that a bit, because there's a bit of a sense of urgency in the timing but I want to get some ideas from the panellists around what does good policy process look like? What constitutes a solid process? If we could wave our wands and go we're going to have a great process to solve one of these problems, what does that process look like? Zoe, given your background, can you kick-off and help us think about process? If you want to intra -- introduce for what is a process or a bad process, now is the time?

>> ZOE HAWKINS: Part of the reason I think we're struggling to embody sort of best practice policy processes is partly, we're sort of stuck in a little bit of a mutual cynical cycle between industry and government. To pick up on what Lizzie was saying before, this real sense of there are recent announcements coming out of some of the tech companies which are really positive and in regards to Instagram and teen accounts or Apple's announcement around nudity content and measures there, I think that we have created a scenario where policy commentators and people in government are reacting to that. You're only doing it as a mitigation mechanism because we're trying to regulate. There's real cynicism about policies if you took the mistrust away, maybe it would be seen as a positive step. On the flipside, in terms of process and the urgency we're feeling right now, I would apply the same disappointment to some of this current politicisization of these important issues and leading up to an election and it's hard to go past the fact online safety is a vote-winning conversation and this breathlessness around the need to sort of ban this before Christmas is kind of a, disappointing because there is important long-term deep research and policy work that's been going on in this space, including not least the sort of diligent review of the online safety act that's been going on and the results of which are due to government in three days' time. I think what we really need is, yes, industry to be more proactive and to build trust by taking action when it isn't being threatened with regulation. And I think government needs to be mindful about avoiding the politicisization of these processes, and being considered when there are such significant implications and I don't know there's huge consensus as much as there's a lot of angst in the community. I don't know there's consensus around understanding how to implement this. That is some of the we need to build trust and build proactivity and some of the ingredients to go into the context that would help do this well. In terms of mechanics of the good policy design process, what we're lacking is it's really commendable the government is looking at so many different tech policy issues right now. The list is incredibly long and hard to do all of that well if it's not well coordinated. There's some mechanisms in government that help with that, and we, tech policy design center have done research around how can we better coordinate these, stitch these different threads of conversation together so that at a country level we have a bigger vision as to what we're trying to create? A bit of more coordination would be something we would call for as well.

>> SANDRA DAVEY: Any thoughts, Jenny?

>> JENNIFER DUXBURY: I agree with everything that Zoe has said. Although I would point out the two initiatives that you mentioned - Apple and Meta - they've been in for quite a long time and not in response to the announcement of the social media ban. It was awkward timing. And put together both of those...

>> ZOE HAWKINS: Even though that might be the case, I think there's an immediate presumption of cynicism and that's the problem.

>> JENNIFER DUXBURY: Correct. What is really important in a good policy process is to make sure that you bring all of the stakeholders in to the room with you. So there are many different opinions on this issue. And you should be aiming to get as many diverse perspectives as possible into the mix. And I also think it's really important for an issue which is as polarized as this one for the Government to be able to demonstrate it's actively listened to those different perspectives and that it is actively considered them as well. So for me a bad policy process is one where you put a piece of legislation out to public consultation with a very short window, and you get 400 or 500 submissions and then a draft bill is then put to parliament very rapidly and quite often before even submissions have been published, and there's no action response given to those submissions. So to me a really good policy process is one where every submission is properly considered and that is demonstrably clear to the participants and it's clear that you have considered those perspectives. I also think that a bad policy process is one that oversimplifies the complexity of the problem. And so getting out the complexities and getting them out into the public consciousness is also to me really clear. Policies which try to aim for too much big change, rather than incrementally taking people along a journey, and there's a lot ofidate off on this -- of data on this, they tend to fail. Incremental shifts can happen quite but you still have to take people along on the journey. If you don't, then again you may not get the outcome that you want. I think it was raised at the very beginning and being clear about what the outcome is you want. Even if there's outcomes and multiple questions, that is also fundamental because you can't have good consultation unless those things are also in place.

>> LIZZIE O'SHEA: If you don't mind if I jump in? I would just add, though, the co-design processes we have at the moment in e safety involves development of codes by industry that are looked at and sent to the regulator and looked at again by civil society and others and if not approved, a whole other process. What I would say there is no-one from civil society involved in the process. We are not funded to any meaningful way to do it but we do it because we think it's important and there's very few people for human rights. It can be useful and a default industry process. There's that it best resource to do it. It can be a default regulated design process. And I'm speaking loosely. I'm making assumptions or grandiose statements about it but I want people to be aware there are power dynamics in how these processes of policy development take place. Civil society is on the back foot. It's not as though we're attending and participating meaningfully in all these things. Both industry and regulators would agree that's a problem. I don't think anybody wants that. It's not easy to make good policy outcomes, create good policy if you don't have all the stakeholders participating to the degree they should. And Australia is miles behind, colleagues in the US or Europe that we look to are implementing similar policies and have a much larger sector. I think sometimes people think this is a process that is kind of everybody is participating on an even footing. And it's not. Civil society in these phases is often four people, two of whom are volunteers. We do need a meaningful discussion about those, some of the resourcing questions if we're going to talk about good policymaking. Otherwise it's a theoretical discussion.

>> SANDRA DAVEY: Can I build on that and I wouldn't mind Zoe or Pyrate or Jenny if you have some thoughts. The classic process I've just heard, and it feels like I've heard it for 30 years, someone puts out a paper. A bunch of people respond to it. You may or may not hear back from them and it's done kind of in isolation. Here is my question. If you could change one thing about the policy design process, just one thing each of you, to make it cheaper, easier, faster, more pragmatic, more inclusive, what would one thing be to that, what many of us in this room know a very stock standard policy process?

>> LIZZIE O'SHEA: I have one suggestion if it's helpful. Sorry to dominate, I'll be very quick. My friends sometimes collaborated, looking at gene technology development. And a friend talks about how there's a civil society kind of panel that's involved. And rather than it's a single process and the development of a single policy, you have established an ongoing panel that's funded to do this work that involves members of the community, and listens to them. Civil society might represent those people but there's a commitment that's in the structure of the policy development process that platforms people other than those who have a particular interest, vested interest in otherwise in the outcome of it. I think that's one change which looks to be more expensive or slower than I think in the long run is a far better policy outcomes which is ultimately more efficient and better for Australian society.

>> SANDRA DAVEY: Jenny, what about you?

>> JENNIFER DUXBURY: I did have a radical suggestion and it does not come from industry perspective. But from my perspective as someone who's done research in political science and teaches on an MBA program about institutions of government and law. I genuinely think it's time for us to consider whether we should be reducing the voting age in Australia. So I would like to see at least where there are issues of real concern to young people like this one, that we would allow them a postal vote for example. So more participatory decision-making model. For this particular issue it would be really interesting to go out to young people perhaps from Year 10 to 12, and ask them what's your view on this? Give them a vote that has to be considered by parliament. But, yeah, more broadly, I kind of think that there are so many big issues that face young people now, like climate change. Where it kind of makes us, it makes sense for us to consider whether they actually should be given the rights that other citizens have to have a say on these kinds of issues.

>> I love both those suggestions. Make it more in-ncluse or potentially faster. I don't think faster is the answer. There's constant sense of urgency and I think that's important. These are timely and pressing issues but my observation would be that these are also complicated issues and I think sometimes the speed of consultation does a disservice to the quality of work that could be out there. These consultations usually last four weeks. They realise when it's 10 days in and there's a practicality to this that genuinely and Lizzie eluded to t some of these people are volunteers. How do we set up a scenario and not only is that group funded for their participation but I think what I'm saying is given a bit more time, I have witnessed the Christmas specials that happen. I participated in the Christmas specials. It's not conducive to wilful policymaking. I want to add a comment to this. The power and importance of researchers and also journalism generally to cover a lot of the implications of these issues is very important. But I do think there's a role for media to consider how they cover some of these issues and talking about vested interests, I think it is also an interesting dynamic that some of the political pressure that politicians respond to is not just coming from voters, it is drummed up by journalists and how they cover these big tech regulation issues. And that's important and an important role to play and we can't forget that there is somewhat of a business contention between media and big tech companies that does play into the politicisation of these issues. Being apair of that is important.

>> SANDRA DAVEY: It goes too fast. I was hoping to take a couple of questions but I've lost that opportunity. Jenny, we'll go to you and then to Lizzie, to Zoe and then to Pyrate. If you want the audience to take away one thing you've been sharing with today, what's the one thing you'd like everyone to take away and perhaps reflect on overnight? Let's kick off with you, Jenny?

>> JENNIFER DUXBURY: What I would want everyone to reflect on is the fact that this is not a silver bullet for any problem. Zoe, you also mentioned that. But it isn't a silver bullet for any of the problems that potentially could be laid at the door of social media. Or indeed a range of digital services which are in scope. So this is a complex issue and that because of that it's really important for us all to be able to take the time to think about exactly what the implications are and to not move too quickly to pall -- policy solutions which may have unintended consequences and we haven't had the opportunity to fully explore all of the issues it will raise.

>> LIZZIE O'SHEA: When I heard this proposal or read that it was under way, my heart dropped a bit. But I've been pretty encouraged by the way in which various civil society organisations that represent young people have come to the table and made very sensible remarks. And I think the political mileage that comes out of such proposals has not been as evident in this discussion. And we are having a much more nuanced discussion than I think most people anticipated or perhaps I anticipated when this was first proposed and I find it quite encouraging. I think the basic foundations are there for people to have proper discussions of how we protect young people and give them the chance to flourish and thrive online and also hold companies to account for doing the wrong thing. I think it's there we need to start putting it into place and escalating it, but we shouldn't just assume the Australian public doesn't understand this or young peep don't understand the complexity of these kinds of discussions. And we shouldn't let politicians get away with bulldozing their way through these discussions with fronouncements that may not be valid. We have work to do with people, internet and infrastructure to make those foundations work in service of Pyrate?

>> PYRATE PASSELL: I want all of you to think that if your children, or someone young that you know, would you feel safe that knowing their personal information, such as their visa or their passport, is online? That is my question.

>> SANDRA DAVEY: That's a big one. Zoe, what have you ended up with?

>> ZOE HAWKINS: For me, the thing that I have been thinking about on this particular topic is that online safety is a fascinating policy area because it's highly emotive for a lot of people and it's something everybody feels they have experience in, and I think that makes policy conversations interesting. The trap I'm constantly trying to avoid myself, so I will share for us all, is to try to avoid anecdotal decision-making. I think it's obviously what drives a lot of the political conversation, and so I think it's making sure that we're actually referring to a research evidence base that is beyond just our lived experience. I might say I had a great time with social media as a kid, but I think moving away from anecdotes and sticking with hard research is gonna help us do the work ahead of us. And I think reason for optimism, if we can do that.

>> SANDRA DAVEY: Fantastic. Thank you very much. I took quite a lot away. And I'm gonna have a say as well! I think we need to experiment with a change-up in the policy development process. Lizzie, I really liked your idea, and, Jen, as well. I think it would be not that difficult for the government to try an experiment and to try the policy process a little bit different. Rather than what did you call the Christmas thing?

>> ZOE HAWKINS: The Christmas special. That's a real thing.

>> SANDRA DAVEY: Cannot do the Christmas special.

>> ZOE HAWKINS: A pun on 20th December.

>> SANDRA DAVEY: Exactly. Everybody, I want a round of applause, please, for Jenny, Lizzie, Pyrate and Zoe Hawkins. Thank you very much, everybody. And thank you, online. And the next session will start in about four minutes. Thank you, everybody.

>>

>>

>>

>>

>>

>> ANNE-LOUISE BROWN: Fantastic. Good afternoon. Oh, thank you. It's wonderful to be here this afternoon. I'm Anne-Louise Brown. I'm from the Cyber Security Cooperative Research Centre and it's great to be here today to be able to moderate this panel discussion - the challenges of cybersecurity, of which I think we can probably all agree there are many. Before we begin, I'd like to acknowledge the Traditional Owners of the lands from which we all meet and leaders past and present. I would also like to remind everyone. AuIGF Code of Conduct - respect people, enable participation, stay on topic and keep it safe. Participants that fail to adhere to the Code of Conduct may be removed at the discretion of the organising committee. For those playing at home, I would just like to remind you to log in to Zoom using your first and last names, not your company name or your nickname. Online moderators will remove anyone who can't be identified and they will need to log back in using their real names. We also ask participants to state their name and affiliation when asking questions or making comments. So, this session - challenges of cybersecurity - is sponsored by Identity Digital and will explore the dimensions of cybersecurity in the internet age. It will ask, "How do we prepare ourselves now for the future? Do we need systemic change, individual action, or both?" To unpack these questions, we're joined by a stellar panel: Associate Professor Vanessa Teague, CEO of Thinking Cyber Security, and Australian National University School of Computer Science Associate Professor. Ram Mohan, who is joining us online, and he is Identity Digital's Chief Strategy Officer. And Xavier O'Malley, who's the Assistant Director of cybersecurity Engagement at the National Office for -- National Office of Cyber Security, which we know in Canberra as the NOCS. I will start with you introducing yourself a little bit and your interests in this particular topic. But the thing I would really like to, sort of, unpack in this first question is, how do you define cybersecurity? Because the more that I spend in this space, the more I start to realise that cybersecurity means a lot of different things to different people. And what do you see as the biggest challenges facing cybersecurity now and into the future? Which is just a little question! So, we'll start with Vanessa and then we'll go to Ram and then we'll go to Xavier.

>> VANESSA TEAGUE: OK, just two little questions. So, obviously, both of those things are very hard to define. I think the definition - I think the right way to think about the definition of cybersecurity is to think about the person sitting in front of the device and think about if the device is doing what the person expects it to be doing. A failure of that could include all of the traditional things you think of as cybersecurity failures, like leaking their personal information, or making non-consensual transfers out of their bank account. But it could also include a lot of things that we kind of put up with without exactly criminalising but we don't like. Like exfiltrating the history of their search queries and using it to manipulate them for advertising or political purposes - I would call that a cybersecurity fail, assuming that the person isn't fully aware that that's happening. And what are our main challenges? In Australia, I would say, actually, the main thing we get wrong is we don't emphasise the hard technical education necessary to do a good job of cybersecurity. All of the other stuff is important as well - the policy, the laws, the processes and making nice pamphlets and everything, but actually getting enough people seriously qualified with the hard technical stuff is something we've failed badly at as a nation.

>> ANNE-LOUISE BROWN: Fantastic. Ram, what are your thoughts?

>> RAM MOHAN: Thank you. I'm not going to venture a new definition of cybersecurity - I thought that was a really good explanation for it. And in some ways, defining "cybersecurity" is like getting some blind people to describe an elephant. So, I won't go down that path. But I will say that it's pervasive. The problems that occur, and the consequences of poor hygiene, are visible everywhere. So, really, I think the thing to focus on is how do you increase awareness of the value of hygiene, cyber hygiene? And how do you ensure that the sheer gross inconvenience of being more hygienic is conveyed, the value of it is conveyed, over the sloppy, convenient part of just sending your password over email, or just clicking on that link because it's easy, or just scanning that QR code without validating that it's actually going to a decent spot. Because it's just you need it now and why wait? It's so bothersome to go through these extra steps, right? So, I think that tension that exists between the convenience and the immediacy that you can get through, which is really, what, in many ways what the criminals are exploiting, right? They are really looking at human nature and saying, "This is really - let's go exploit that." So, we need the same thing that, you know, in Australia and much of the world, the same campaign that happened decades ago that convinced drivers that the first thing you do when you get into the car is to put your seatbelt on. That was driving hygiene and it took a tremendous amount of education and awareness. And in that case, lives were lost. In the case of cybersecurity, often it's your money that is lost or, much worse, your identity that is lost. But some level of significant awareness, I think, is probably the largest challenge that we have to solve.

>> ANNE-LOUISE BROWN: Fantastic. And, Xavier?

>> XAVIER O'MALLEY: So, for a bit of context about my role, I work for the National Office of Cyber Security. I'm a Melbourne-based representative of the Cyber Engagement Team. And my team's remit is to really support the work of the NOCS, advocate for the Cyber Strategy, and communicate with state and territory governments, industries, small business networks, and really amplify the initiatives within that strategy. So, I'm conscious that everyone in the room and online is fairly savvy in this space, so I won't deign to describe the elephant, so to speak, about a definition of cyber. But I will share what I communicate to smaller business representatives. Cybersecurity, I think, can boil down to baseline, default settings, both technical and cultural, that enable you to do two things - one, operate online, protected from threats, and to do so - to be able to bounce back quickly if you are exposed to those threats. With the caveat that we should expect exposure to those threats is inevitable. The challenge, I think, is getting just the average Australian to... Because this is a whole-of-economy effort, but the whole economy is made up of individuals that work for all of our organisations, big and small. Getting the average Australian to comprehend that this is not an abstract issue, not an IT many domain-thing to fix, but sort of an emergent national priority, getting to grasp that, I think, is a big issue. But then also the - after raising that awareness, reassuring them that it's not a problem too big to solve, that certain behaviour changes and those, yeah, raising those minimum standards - both technical and cultural - can do a lot to shore up your online risk. So, that's what I'd say.

>> ANNE-LOUISE BROWN: Fantastic. Just drawing, I guess, on what all of you raised then, I'm quite interested in this area of increasing awareness, 'cause we hear about it a lot. There's been many campaigns over many years. But in terms of actually improving that base line, how far have we got? And how do we actually get better? How do we - you know, we talk a lot about stronger passwords and those kinds of things, but how do you, I guess, within the community, effect that behavioural change? It's a big question, but we do hear the same messages over and over again, and we have for many years. Do we need to do something differently to change the way people behave online to make them more cybersecurity, and as a result, the economy more cybersecure? And drawing on what you said, Vanessa, around better tech skills, you know, I think that that's really interesting - there have been lots of conversations around the professionalisation of cybersecurity in Australia. I don't know if we've actually got there yet. You know, we don't have that kind of accredited body that helps mark people out at particular levels, and things like that. So, sort of, drawing on those two things, you know - and, again, a big question - but what are some of the things that we could do differently to help drive that change?

>> VANESSA TEAGUE: Wow! That's two big questions! OK, first of all, it's very unclear to me that we are getting better. There are some aspects getting better, but there are other aspects getting worse. And if you look, for example, at the demonisation of end-to-end encryption, that's a perfect example. We need to decide whether we actually want people's communications to be secure or we need to decide if we're going to bang on about how encryption is only for terrorists or paedophiles. Because at the moment, they're getting totally mixed messages about whether a certain technology is good or bad for their security. And there's a number of other examples like that, although that's probably the worst. So, that's item number one. I find it's kind of astounding how little good-quality education orients around relatively simple things, like ad blockers for kids, or privacy-preserving web browsers like Firefox, or even how many adults know the security implications of different ways of communicating. So, I don't think we... We may be doing a decent job at the corporate level. But I don't know that we're doing a great job at the ordinary Australian-person level. Some things have gone backwards. For example, my bank used to have a proper independent second factor of authentication. They keep trying to persuade me to switch over to SMS. Eventually, I will give up. I'm holding on to my plastic token for now. I can't find an Australian link that doesn't involve SMS. Why is that? That's mad. I'm not sure we are getting better. I'm not sure there are enough people who really understand the technical implications of these ostensibly very similar choices that actually have very different implemencations under the hood, to be making good decisions in this space.

>> ANNE-LOUISE BROWN: Xavier, you're obviously at the forefront of this, driving a lot of this work from a government perspective. You know, are there any things that, I guess, you know, especially through the NOCS and the role that the NOCS plays, given that it's still a relatively new kind of construct, are there any different approaches that are being taken to help drive this uplift in the community and across the economy?

>> XAVIER O'MALLEY: Many, and it's a broad question, so you may have to just cut me off if I meander through too many points. But on the questions of, like, secure technology, I think that's a big part of the strategy, is to ensure that not only are we asking Australians to change their own behaviour, but that we're also doing - we're also assisting by ensuring that they can trust the products that they use. So, one component of the strategy is ensuring that Internet of Things devices, or software that comes into Australia or that's manufactured here meets certain minimum standards, even basic ones that align us with international standards, like ensuring IoT devices have, you know, default - switching out from default passwords, and ensuring that you don't need to switch on security measures, ensuring that these things are built in. So, secure-by-design is a big push from this strategy. In terms of the work that the NOCS does, part of the coordinator Michelle McGuinness's remit is to, well, at a high level, do a number of things. One, bolster the commonwealth's cybersecurity. Because it's a bit cheeky to ask industry to meet certain standards and then not bring the government along with it. So, that's a big body of work. Overseeing the National Cyber Exercise Program. Obviously, you've got smaller businesses and your general punter who is exposed to cybercrime, and they're gonna need to bolster their cyber hygiene and their use of devices, et cetera. But the top end of town, when you've got critical infrastructure, and just larger businesses of scale, practising incident response plans, ensuring you have business continuity capabilities, stress-testing your cyber posture with exercises, advocating for threat sharing across sectors, providing advice for small businesses - there are so many things, but it's a huge collective effort. The government sort of writes the strategy, in co-design with industry, of course, but then it's a case of getting broad buy-in, building relationships across public and private industries, and then maybe later in the session we'll talk about some of the programs available. But certainly, yeah, there's many levers being pulled to try and ensure broad economy uplift Yeah.

>> ANNE-LOUISE BROWN: Fantastic.

>> VANESSA TEAGUE: Am I allowed to answer?

>> ANNE-LOUISE BROWN: Then we'll go to you, Ram.

>> VANESSA TEAGUE: IoT devices standards, that's a great idea. But you have to make sure that the certification has teeth. There are so many examples of things that sound like a great idea that set out a bunch of standards and then the certification ends up being a secret are youu rubber stamp by incompetent people behind closed doors. So, set up that thing and make sure there are incentives to get genuine certification. Like, genuine certification is gonna fail some stuff. That's how you know when it's working, is when it gets refused. So, make sure there's serious public scrutiny on the certification process so that it's real, because that's the only way that your standards are actually gonna be upheld.

>> XAVIER O'MALLEY: Yep.

>> ANNE-LOUISE BROWN: And, Ram, you've mentioned before, you know, the importance of communication campaigns, essentially, and how we can make those more effective. I note that you're joining us from the United States. And I'm not sure what time it is there, but I think that it's quite a different time to what it is here! But in terms of, I guess, what you see in the States, is there anything that is done differently in the States to sort of spread this message that is effective and, I guess, could help - you know, that Australia could learn from?

>> RAM MOHAN: Thank you. It's a good time - it's a good time to come in and participate in this conversation. Look, in the States, the government is doing quite a lot of work in disseminating information about how to be safer, et cetera. But I think, actually, the biggest levers that are being pulled are being done by the big technology giants. They have, I think, done a good job in pulling the level up. I mean, I was reading an article earlier today that said Microsoft users end up getting 60,000 attacks - sorry, 600 million cyberattacks every day. That was an article out, I posted a link to that on the chat here, right? But if you look at, say, what a Microsoft or a Google or an Apple, et cetera, the platforms that have the largest amount of usage, one of the good things that they have been doing, promoting, and also it's being translated to lots of other sites and other services, is they're moving away from, "You must remember your password." They're saying, "We're gonna send you your one-time-use code for you to get in." And that, for example, is a small, little step in the right direction because, as you know, most people end up using either a simple password or, worse, a simple password that they use across every site, or every place that they access. And it's ridiculously simple to reverse-engineer most people's passwords, right? So, kind of moving away from that model, I think there is some progress that I see happening here in the States. The other side of it is that this is a somewhat larger country than yours, and as a result, the issues of awareness and scale are far greater. So, there are so many successful scams and so many successful attacks on compromise of credentials that really work well in the US. And, you know, even at my own firm, there are people who I look at them and I say, "Why are you not using a password manager? Because then you don't have to remember any passwords. You remember one code and then it can generate these wonderfully complex passwords across everywhere you go and autofill, et cetera." And it just doesn't happen, right? But I like that the big technology companies, many of whom are domiciled here in the United States, are moving away from the old method of username/password credentials to one-time password as a way to enter their services. S

>> Almost moving to a security by default met udevery time you're logging in to something. I will ask Vanessa a question now and we touched on this a bit before you mentioned and encryption but lot of your research has been focused on secrecy and its impacts on security. In your view is secrecy good or bad for security and how can a balance be struck between the two?

>> I think there's a mistaken belief by some parts of the Australian Government that things become secure because they're kept seek R. That's a mistake. It doesn't necessarily mean making them public will automatically get them mixed but there's a tendency to use security as an excuse for hiding things when that is not valid. There is the source code for the Senate count and one or two other things of a similar kind. And I think it's almost never justified. On the contrary there have been some good examples, for example, we recently looked at the code for the ACT's paperless electronic voting systems which are not used in any other states. Which were doing shuffling of the votes that had been cast, in a way that was actually not sound. And the code was not available in 2020. It was made available this year. So this year we figured out in 2020 they hadn't been properly shuffled. So the fact the code is made available made it possible to fix it in time. That kind of process is not appreciated enough and more stuff should be open by default.

>> Ram, at Identity Digital, you work with registrars and deliver registry services and provide top level domains. How important is cyber security to your organisation and over the years how have you seen the importance of cyber security evolve in this space?

>> RAM MOHAN: Thank you so much. The main registries were domain registry and worked with registrars worldwide, and we recognised registries are the gateway to a secure and trusted online experience. So we end up in our own chart, we end up conforming to best practices in the cyber security framework, essential aid in Australia, the Centre for Internet Security and there are a set of standards that we work with. And the other part of it is if you look at domain names for example, there is a particular code in Domain names and you need that code if you want to transfer your domain name or perform certain transactions with your domain name. And we end up working with registrars for example to say, hey, in the protocol, that particular code is actually not hashed, it's in clear text. But in your database you ought to think about what you're doing with that data as an example, right." But even at the registrar level, I think the primary job that we're doing is working with them to get basic awareness out to all of their customers. How do you stop your credentials from being compromised, right? And if you look at data that's out there, what is clearly seen is that in the, if you look at the top five ways by which hackers get into companies, the number one way is exploits that are not patched and fixed. The number two way is fishing. The third way is stolen credentials. The fourth is prior compromise. The fifth is website compromise. That's worldwide. But if you look specifically at the Asia-Pacific region, what is the primary way by which cyber attacks happen and the way by which hackers get into companies? It's by prior compromise? So in the Asia-Pacific region we end up working with folks in the industry to say watch for that particular attack vector because it is popular in that area. If you look at Europe, the Middle East and other parts of Asia, you'll find fishing is the top. And in the Americas, both North and South America, the top way of accessing companies and data is via exploits. So there's a variety of techniques that we know are being used to gain illegal access to crucial information and the biggest thing that we do is to work along with them, with the industry, to both disseminate that and have them work with their customer base. We're talking 200 million plus domain names in the world that the registrars are engaged with. You're still talking about tens of millions of small businesses, tens of millions of individual users whose security practices could deal with an upgrade.

>> One of the things that is Shaning through is the role that collaboration has to play in terms of actually achieving cyber security and by that I mean public and partnerships and those kinds of arrangements. In terms of the 2020 Australian cyber security strategy which has been out for nearly a year now - has it been a year yet? And I'm sure a lot of you in this room are quite similar with the cyber security strategy and as I mentioned before, as Xavier mentioned before, it is really tasked with helping implement some of those initiatives in terms of making the community feel more at ease or helping communicate how they can be effectively implemented within the community. Where are we on the journey now, Xavier?

>> XAVIER O'MALLEY: It's coming up to the year and the strategy was designed to have three phases of the work on the path to 2030. We're in Horizon 1. And some of the key achievements, Horizon 1 came with an action plan of 20 items with I think 60 initiatives within them. Home affairs leads the bulk of those. But with partnerships with ASD, DFAT, and various collaborative other agencies pitching in and leading different initiatives. The achievements that have made progress this year. The ransomware playbook that's hosted on the government website and encourage everyone to spend part of their week to look at it. And also the Act Now Stay Secure campaign is trying to really put those basic cyber hygiene measures of past phrases, MFA and software updates into just the environment, so people are sort of soaking them in through media, through your exposure to that campaign which has got funding for three years. It's not going away and those measures will still be the ones that we ram home. As Ram said before, you have very clever people, otherwise very well structured with an online presence, reusing passwords. Having insufficiently long and complex ones. These behaviours do need to be continually rammed home. Cyber awareness month this month added a fourth key measure which is just be cognisants of Fishing, both the scale of it and the increasing sophistication -- fish -- phishing, both the scale of it and the increasing sophistication. Voice ph sh ng and -- phishing and the corresponding amendments to the security of critical infrastructure act. The key ones there being that introduction of a power for the minister to introduce a standard, as Vanessa mentioned before, will need to have some teeth. The idea there is that standard is to be created and it will likely align with at least the first three measures there. The introduction of a limited use obligation on the cyber coordinator and the ASD. The purpose of that being to make industry feel reassured and confident to come forward and report and work with these federal level intelligence and remediation services. Safe in the knowledge that information they share about a cyber incident they've gone through won't then be used against them in a reg regulatory setting. That's part of a broader effort to encourage and incentivise threat sharing across sectors, reporting in general, because we want to be able to create a map or understand the actual scale of threat that we're facing. The ASD cyber threat report which is due any minute now, provides a year on year comparison that maps that picture but can only utilise what's reported. Really encouraging reporting across the economy, encouraging entities that have gone through a cyber incident, particularly when at scale, to engage with the ASD and with the cyber coordinator. That was another part of the cyber bill. And then the introduction or the establishment of a cyber incident review board. Which to date we haven't had a mechanism that can sort of look at with a no-fault, no-liability attitude, what actually happened in this cyber incident, what can we learn from it? What can we disseminate to industry and government so that Quay, rather than finger wagging or looking askance at an entity that's been through a cyber incident, rather acknowledging that this is likely to hit various entities at any time and thinking what can we each altogether learn from it, to build that collective resilience. I told you I'd re-Mander through.

>> The last part is that whole notion of knowledge is power and if organisations know what their issue is and what the problem is or what the vulnerability is they can at least take steps to remediate it and prevent becoming a victim. That's especially the case in relation to ransomware.

>> XAVIER O'MALLEY: Glad you mentioned ransomware. That's the other of the bill.

>> I'm wondering if anybody has questions to ask from the audience? We'd love to hear from you. We have a willing victim.

>> How are you doing? There seems to be an inherent conflict and a spectrum, how do we, where do we set the line between encouraging good cyber hygiene practices for consumers and small business for which they don't do it for a job, they don't have a size 18 and don't have an IT professional potentially running the cash register at the butchery, and making them so scared that they stay offline completely because they're too scared of doing it wrong?

>> XAVIER O'MALLEY: Really good point. That's the challenge to get to use urgency to raise awareness but then to provide solutions that they can utilise. Two of the main ones I'd raise is one has just been announced last a small business cyber resilience service, they won the grant and they'll be commissioned to provide, to be a free 24/7 service to assist with realtime support for small businesses. Eligible small businesses. That is those with an ABN and under 20 staff. Because we encourage reporting to the ASD and really that's a portal to try and catch larger, more significant - and there's regulatory requirements for critical infrastructure to take that avenue. There's a little bit of a gap for small businesses to get that person to person support, advice, remediation assistance possibly. And then another program is trying to encourage smaller businesses and this is where we're talking ma and pa shops, going through online training to get the baseline awareness and maintain membership of that program to become a certified cyber warden. And then hopefully with sufficient uptake of that, inject a cyber culture into the smaller businesses that don't have an IT department for example, cracking the whip. And if we can make that supportive and warm and raise awareness of support like ID Care, Scam Watch, and if we can convey urgency and reassurance in the same message, that would be ideal.

>> Is it reasonable for an individual or someone a small business like that, to actually take the stance of I'm not an IT geek, I expect my service providers and I expect my bank and the Qantas website, I expect all my service providers to get their together and make sure they're unprotected, regardless of what I do and get the systems up to be secure by design so they don't have to remember passwords or a one-time code or figure out how to use a password manager if they're not IT literate?

>> Rank Ram would be able to comment on that, say with things with DNS filtering and some of the great things that do happen and I'm sure Vanessa will have a comment as well or a perspective.

>> RAM MOHAN: DNA filtering happens. And it happens - a few years ago, maybe a decade ago, in the technical community and other places, we would say this is a really bad thing, don't do it. But we have come to realise it's going to happen nevertheless. So therefore now the task is to try and mitigate the harms that come from large-scale DNS filtering. And to especially help educate policy-makers in responsible places around the world that it is actually a very blunt weapon. And should be, it's not that you should never deploy it, the governments will make a call based on what they think is the right thing to do. But it has a significant impact and in many ways it's an irreparable impact because the end user has no control. You remove control from the end user and it's taken by someone else and there's no way really to get around it for the average user, right? So measures like that sound great. They make for terrific sound bytes. And if you come in and you say DNS filtering is the best way to protect national security interests, I can point so many ways by which such DNS filtering measures get thwarted. The question here is what is a proportional response towards a specific threat? And I would say in most cases DNS filtering at large scale is a vastly disproportionate response to what really ought to be a narrow band problem?

>> We might go to the next question. If you could introduce yourself?

>> Representing myself. One of the things that struck me both with a question about small business and about the broader discussion right now was that Australians have not faced, in terms of total numbers of risks that we've faced, the biggest ones in recent times have been mass exfiltration of our own data by companies that retained far too much for far too long

>> So what I'd like to hear is now we're going to discourage organisations to retain any data at all. When they must retain it, how long and how they destroy it as well? It's often that vague area where they're not quite sure how long they retain it. So by default they retain it for longer just uncase they get asked for it. We need to be much better at telling them don't keep this data or don't collect it in the first place which will be perfect and sometimes they have to. That advice can be given to small businesses as well. So that they aren't writing stuff down on paper and typing it into Excel and storing it forever and maybe that's something that doesn't require a lot of technical expertise but it does require a lot of clarity on the way people operate.

>> I completely agree and we're not just not doing the right thing, we're actively not doing the right thing in some circumstances. I'm not a lawyer. It was unclear to me whether Optus had to retain all those ID documents. I'm not sure. But they definitely had to collect them and there are plenty of countries where they don't.

>> Optus publicly said they were not sure. That was disputed and I don't know what the truth of the matter is. In a previous life I dealt with a lot of telcos who put data in the cloud and they all pretty much said the same thing. We don't know so we're keeping it.

>> That's terrible. The other obvious example is the recent regulations on relevant electronic services that the e safety commission just put through, mandate the retention of email addresses of phone numbers. You have to collect one of them and retain it for two years. I don't know how that will fly when the Google Play Store and the Apple Play Store enforce the European rule where you have to delete something when somebody wants to delete their account. We have these regulations that insist on doing the dumping.

>> Adding to the data retention laws in Australia are many and varied. That's where a lot of that confusion comes from as well. And I think it's one of the key problems with older data is the way the data was put into a system to start with, it's hard to start pulling it apart. You don't need to do that bit now because it's linked up to this bit. There's no easy answer to that question but I agree with your sentiment.

>> A lot of laws that you think expect deletion of the data have this little weasel word that sort of says delete or deidentify. So people can go we deleted or deidentified it, when in fact all they did was strip off the specific literal name and address of the person and kept the identifiable boundary instead.

>> We have another question.

>> Hi. I'm from the internet governance team and I have a 2-parter. The first one is to what extent do you see DNS abuse as contributing to significant cyber security problems? And the second part is if you do see it as a contributor, do you think it's better to keep working on DNS abuse as a kind of a collective? Or do you think it's better to break it up in to the bot nets, sort of pieces and work on them from that perspective? Which would be more effective in terms of helping the average Australian?

>> Ram, you'll be very familiar with this topic?

>> RAM MOHAN: I am, unfortunately. Maybe fortunately. DNS abuse is a significant contributor. In many cases, it's the means rather than the medium itself. If you look at how people get compromised and people get attacked, phishing is a huge form of attacks. Delivery depends on stable and functioning DNS. There are many forms of online harms and certainly DNS abuse is a really important topic. Now in the last few years, domain registries and domain registrars have taken specific aim at policies that can address these kinds of harms and the global body that helps oversee the name space has also promulgated good policies in this area. So if you look at registrars and registries now, every single one of them that are accredited with ican must have an abuse of contact. Somebody real, not just a role account. There is also a lot of registrars and registries have implemented multi-factor authentification as another method. The awareness campaign is really where a lot of the work has to be done. One of the things - I'm the chief strategy officer for Identity Digital, but I'm the chair of the Internet's Security and that's at ICANN. We're working with them to actually build what we're calling safer cyber. That's a campaign that starts off trying to demystify these crazy techie words and trying to explain it in ways that our grandmothers would be able to understand. Our grandmothers are accessing the internet and they didn't learn about it when they grew up. They're not digital natives. We're trying to convey those kinds of messages about protecting your credentials. Simple steps, three or four simple steps that can significantly improve your security. Yes, as a result, I think separating these harms and focusing on them one at a time and trying to look at, making some progress, is the right way to do it. Not just take it all in one big bucket.

>> Fantastic. I think we have an online question and then we will go up the back.

>> Thank you. An online question now. Are there better public policy practices to explore more effectively that empower end users, who are not digitally savvy to navigate the online world safely and carefully?

>> Thank you. It would be very rich if you had the silver bullet for that question. I'll hand over to Xavier.

>> XAVIER O'MALLEY: You would indeed. I perhaps want to reiterate my previous comment that the introduction of programs like the Small Business Cyber Resilience Service and awareness campaigns that can help folks realise because embedded in the question is an expectation you would need IT support or IT literacy to defend yourself. We should do away with that. Cyber security is a culture problem. Everyone should be leaning in to be able to fort nigh their own devices at the very least. And we can't just expect each, when we consider the elderly for example, you can't just expect everything to have people in their lives that could provide that support. Having resources that they can reach out to to help, like the Small Business Resilience Serve, cyber wardens, or for places that are harder to reach or don't have access to translated materials or even cyber advice in Braille, in one of the components that we've tried to do, accessibility for CALD communities and literally just hard to reach regional places that aren't sort of absorbing biosmosis cyber security messaging in cities. One of the things we've tried to do under shield one of the strategy which is supporting small business and citizens is to fund community awareness grants for groups, install and medium and large across the country that can help - I like to use the phrase throw the ball, so it can be caught. Deliver the message that will land with a particular audience and so that includes outreach programs for elderly, translated materials for new arrivals. People who are not necessarily digitally literate, it would be great if we could then partner up some of those programs with the really strong nitty-gritty advice that you can find on the eSafety Commissioner's website. Some of these things that are on that website but are not necessarily, there's an irony in having a page on a website and a video that teaches you how to use a website is on the website. But we can help that

>> Counterintourative.

>> XAVIER O'MALLEY: We can help people to reach those things. We can start off and make software updates automatic and install MFA. Some people need to be told how to turn their phone on. Trying to catch the whole range of support services there and then up that, you get all the way up to critical infrastructure where you need to bolster more regulatory and complex secure environments and essential 8s and stuff. Short essential 8s and stuff. Short answer, there's lots that can be done, but there's plenty we're trying to do.

>> ANNE-LOUISE BROWN: Sorry, I interrupted then, but the continuity is a really important thing too. And we do tend to work in, sort of, three policy cycles that align with elections. Things like that. But I think one of the good things about the cybersecurity strategy is that it's a 7-year strategy, as opposed to a 1-year or 2-year strategy. So, it is something that can build upon itself, potentially. And I think we have one final question.

>> Thank you to the panel. I am the acting president of Phoenix Victoria, the Victorian Association. So, my question is for Xavier and probably Vanessa might have some familiarities with the new regulation. In the intersections of small business operations and open-source technologies, what brought this to my mind, a few months ago when the Optus happened, at the same time we had monthly workshops at the small cafe in Essendon in Victoria. One of the members, Brian, had installed a system that's open-source, tailored point of sales, that's supported by EU and Switzerland government. And we see a lot of cases like this, especially in my previous role in Open Source Industry Australia, a lot of French and German government initiatives that really helped with smaller communities when they're trying to apply for grants, they could point at - in those communities, "Hey, this is the funding for this project, we want to use this project," they would get extra funding to implement that. So, my question is, are you aware of - because of your roles or understanding - aware of similar initiatives or acknowledgement of open source technologies to enable smaller tech communities to help out small businesses in their own areas?

>> XAVIER O'MALLEY: Do you mean in terms of procuring, like, recommended technology?

>> At a corporate official level. Linux Victoria, the user group, has been operating since Linux was introduced 30 years. There's a lot of similar groups across Australia that have a very good command on technology, and a lot of them are small business owners or have people in their communities. Implementing very good, stable, resilient technologies doesn't really take much. It could be facilitated through grants. They challenge that we had was there was no reference point in the Australian guidelines or legislation, contrary to the American and European ones, that you could easily approach the decision-makers, because open-source technologies always there's a misconception of not having a reliable vendor and licensing agreement and others, which are -- which our counterparts in Europe and America don't have that issue. My question is are there recent... That understand those engagements?

>> VANESSA TEAGUE: Are you asking will the Australian Government help fund projects or are you asking can you persuade the Australian Government to use open-source software?

>> There are implied, but that would be ideal. But I think what would help is even an acknowledgement. I remember at that time, the Digital Transformation Agency didn't have the words "open source" in their guidelines, so we could not refer to open source in the applications. I wonder if any initiative does have that so that we can point at. Not just us, I'm also extending it to other local players that are technical, want to help in their own local community.

>> XAVIER O'MALLEY: I won't stray into what the Digital Transformation Agency is working on, but it's possible that they're across some of what you might want to know about. One thing that is in our wheelhouse that we're trying to do is recognise the national security risks of certain vendors and be able to make that available to entities operating in Australia, that these are a list of high-risk vendors that we encourage you to consider not utilising. I would shy away from discussing open-source tech just 'cause it's a little bit out of my area of understanding, but we'll chat after.

>> VANESSA TEAGUE: And we think that's the answer, though, actually, is that there isn't anybody in most state or federal governments who understands open source. So, it's not... They do dumb things. Again, they do dumb things, but not because there's any malice or any particular desire to not use transparent technologies. It's just that there's nobody who understands how easy it is... Often, pulling something and compiling it and running it and giving it a go, it might be free, but it still requires a certain level of technical knowledge. Whereas if there's some vendor in a shiny suit knocking on their door and, you know, offering to build it for only a few million dollars of public money, they'll often choose that instead because the person making the decision isn't able to assess, you know, the free thing that they could be using instead, right?! (LAUGHS)

>> ANNE-LOUISE BROWN: Thank you so much for your question. It's a big question, because there are so many conversations going on around open source at the moment as well, in a whole range of...

>> VANESSA TEAGUE: Not enough!

>> ANNE-LOUISE BROWN: Yeah, mmm. Look, we are over time. But just before we finish up, I wanted to thank everybody so much, our panellists. They were fantastic. But also, in one sentence, I want you you - so we can be happy at the end - to tell us what is the biggest opportunity that you see for the community through enhanced cybersecurity? You go first, Xavier.

>> XAVIER O'MALLEY: I think it's an opportunity in itself to be - to get ahead of what is just a continually scaling-up threat. And if we can bolster our cyber workforce so we can get Australians, youth coming up to want to get into cybersecurity and recognise that it's not just an IT job, that there's a range of analyst roles, advocacy roles, yada-yada, but, yeah, there's a real opportunity to live that ambition of the strategy, which is to be a world leader in cyber by 2030, have the workforce here, come through.

>> ANNE-LOUISE BROWN: Awesome. Ram?

>> RAM MOHAN: From cybersecurity to cyberhygiene.

>> ANNE-LOUISE BROWN: Fantastic. And, Vanessa?

>> VANESSA TEAGUE: I don't think you can spin it as an opportunity. It's a threat we need to learn to defend ourselves against, and we just have to get better at the tech, and we have to have better technically informed decisions influencing our policy.

>> ANNE-LOUISE BROWN: Fantastic. Thank you so much. You've been fantastic. (APPLAUSE) thanks, Ram. You can go to bed now!

>>

>>

>>

>>

>>

>>

>> Welcome, everyone. I hope everyone is feeling refreshed after the break. I'm delighted to be moderating the next session on protecting the data in our online lives. We're joined by two fantastic panellists, Holly Raiche and Rachael Faulk. Holly sits on the board of the Australian Privacy Foundation and is a lecturer at the University of Sydney. She's held a raft of other impressive roles, including as the former executive director of the Internet Society Australia, former vice-chair of the Asia-Pacific Regional at Large Organisation and sat on a number of boards. We've also joined by Rachael Faulk. She leads a high level collaboration between government, industry and research institutions. Rachael is one of the nation's leading cyber security policy experts and commentators. She was appointed by the Minister for Home Affairs and cyber security to the 3-person expert advisory board to advise in the development of Australia's 2030 cyber security strategy and she also led the independent review into the Department of Home Affairs. Management of the Optus and Medibank cyber breaches in 2022. She has a background in telecommunications, litigation and commercial law. Welcome, Holly and Rachael. Let's get started. This panel is particularly timely. We've had several major data breaches and a growing movement around privacy reform. My first question is to Holly. Last month Australia introduced a long-awaited privacy law reforms to strengthen Australia's privacy framework. Did you want to talk about the reforms and other tranche 1 forms announced just a few weeks ago? A good start? Not enough or both?

>> HOLLY RAICHE: If I had to talk about the privacy reforms I'd be thrown out for bad language. So I'll talk about one element that I think is a failure and it's been a failure for about four years or probably a lot longer. Personal information, the information that is protected by the privacy act. In terms of information about somebody. That very much narrows the level of protection that you get. It's your name. A few other things that are about you. If you contrast that with the definition that's in the GDPR which is EU privacy law, it is information concerning. If you think about the way that we use communications nowadays, you look at what's the definition of personal information, if it's only about you, there's all sorts of metadata in terms of the phone towers, destination, sort of things that will give a lot of information about you that's meta data but it does tell stuff about you. If you look at our legislation, and you look at the European it is protected. Way back in 2019, the final report of the digital platforms, the ACCC report said, "We need in this digital age to expand the definition." The Government response was, we totally agree in principle." We need a privacy about reform. The privacy act reform said, "We need to redefine the definition of personal information." The Government said, "We totally agree in principle." They have just released the first tranche of the reforms of the privacy act. And they agree in principle still to change the definition.

>> On that note, Rachael, did you want to talk us through as a lawyer some of the implications of the proposed changes as well as the obligations under the existing legislation for companies around data and meta data?

>> RACHAEL FALK: At the moment we have the cyber security bill that's been introduced by government and still working its way through the House and hasn't gone to a second reading yet. The changes, the changes for some of the legislation is to capture potentially an Optus-like situation. So in Optus they had obviously identity data and a whole range of data stolen, as best we know. And that was the security of critical infrastructure act was not applicable and some of you may recall the then minister Clare O'Neil getting pretty frustrated in the media and might have called the legislation bloody useless at the time. And that's because it didn't actually apply to a breach of that nature with a telco. Some of the legislation is the changes are to introduce business systems back into the definition so that if that system was breached again, government could be a role and could have some levers in that. And that's yet to, that's also going through. There's way to go on that. No matter what legislative changes and what legislation we have in this country, it's all subject to interpretation. So if you're looking at a telco, they have an obligation to obtain identity data for all customers. So prepaid, post paid, where a telco must get your identity information and hold thatidate that information and have to be able to. That's for law enforcement purposes. Bruce Tonkin, if he's involved in a crime, we know whether he was there or not and weather his telco services were registered. It's important we look at that and it's important that identity matches. We know that historically it's very problematic because people get burner phones but telcos and meta data are an increderably sit source of primary evidence in a whole range of officers. There's a whole range why telcos have identity information. The challenge is keeping it and retaining it and for what purpose. I won't bore everyone to sleep with the act the legislative requirements but that's just an example of where you have identity documents. There's a document verification service that Optus subscribed to that they could have used to verify identity. While we have legislative requirements not just in telecommunications and financial services, you have to put enpersonal information and it's all retained by the or the credit provider at the time. They have obligations to keep and the law dictates obligations to retain. So it is very challenging for organisations on one level to know, they know what they have to retain but it's deletion of data in a timely fashion. It's the how you retain that is critical and whether it is retained and they might get through the network but it's like having the data in a safe. To me, there's lots of potential legislative reforms that might make Australians and Australians safer and we hope it does. But it's really important that organisations do as legislation states and if there are exemptions to that or they've been granted exemptions or workarounds, that is transparent as well as we move through that. I think it's fair to say if we're talking about legislative changes, boards are grappling with what good looks like and that's a challenge and Holly will correct me if I get it wrong but at the moment there's no case around cyber. We have one judgement and that was consent orders and a judgement. Helping directors ask questions, get information, get comfortable with what good looks like in their organisation and know to be frank when their technical people are leading them or not telling them the right things. And echoing previous panels, this might sound like a technical problem, but it is actually not a technical problem if you ask lots of questions. I always come back to the fact that lots of smart people can understand lots of things. It's how it's explained and is being explained in a way -- whether it's being explained in a way that makes sense. The Australian Government is not there yet. It still has a round of approvals and consultation. At least caches of data are more secure. Once a threat actor is in the system and how it secures. The best legislative framework in the world is what happens once they're in a system.

>> Yeah. I mean, I feel like there are so many threads can I'd go through what you just said. Just to throw it back to Holly, you spoke about the GDPR. How do you propose reforms and compare with other privacy frameworks around the world and what lessons or best practice approaches or what to avoid could we be applying here?

>> HOLLY RAICHE: It is kind of the notch, privacy real should look like, being protected. We're a long way from that. I have already talked about one issue. One of the principles that is honoured in the breach is how much information is collected? Now we have got privacy principles which is a good thing. They're supposed to be followed which is another good thing. But collection of data should be adamant and only what's necessary. So I suppose my next question to everybody is do you fill in all the blanks when you ask to or why do you need my address just to buy a sweater? There are so mane -- many situations where you have to fill in lot of information that probably isn't nes except that you shouldn't be doing it because it's -- necessary except that you shouldn't be doing it because you're in the act. I'll spend my time what's wrong with the act. Another issue aside from the collection of data is some of the exemptions and one of the exemptions that is egregious is small business. Now, I realise it would take an enormous amounts of time and effort for small business and they're under an enormous amounts of financial pressure right now but there are 2.5 million small businesses in this country approximately. Every one of them collects data about us. And they are not bound in anierment for the privacy act. So all of the data that they collect is simply not with the privacy act. So you think about all the data, your favourite coffee shop or small grocer collects about you and it's not protected. It's just not protected. Do you want me to go on?

>> Yeah.

>> HOLLY RAICHE: Off to you, Rachael.

>> RACHAEL FALK: Privacy act?

>> Feel free to take it where you would like? You can talk about what broader measures we could be taking.

>> RACHAEL FALK: Unfortunately the privacy review measures probably in my mind didn't go far enough. The small business exemption is one that surprised me. I run a small business as well. It does cost money to be cyber secure, absolutely. But the flipside of that is if you have a digital presence, you have to be prepared to put money into securing that digital presence. It would be no different from a small business saying, "It's too hard to comply with OH&S laws and I have over 10 staff and will not bother or I'll just only employ nine staff." It's crazy because you derive a profit and a benefit, presumably a benefit from having a digital presence and having your records digitally managed. So I kind of think your obligations as a director mean that you have to take reasonable steps to protect the assets of the company. So, yes, it costs money but if you don't want to spend the money, don't be on the internet, don't use cloud or email, that's fine. But you have to in 2024 spend money on being cyber secure. Does it cost money? Yes. Do you have to do Fort Knox? No. There's lots of small businesses, and if any of you apply for a role in a small business, you're giving your CV to them and they'll keep their CV. They're keeping data and maybe a contract that you might have done work for them and they keep a lot of sensitive material in varying degrees. So we at the cyber security centre do spend unsurprisingly given our name and reputation quite a bit of time and money on focusing on cyber security because it's the right thing to do and that's my view and the board's view. I just want a small thing, if you ever want to be test what you think companies might and might do with your information big and small, go and look at their privacy statements. They have always been a bug bear of mind. They are obligations of companies and have to have a privacy statement. Most large companies and listed companies and they're supposed to tell you what they'll do with their data but they're deliciously vaguely worded. There will be a line in we reserve the right to share your data from time to time with third parties who may assist us or help us undelivery of services to you. That's a beautiful line.

>> You have memorised it.

>> RACHAEL FALK: It means if wore a big company and need to do something for you, we can share some of that data in order to deliver those analytics or whatever. It's very opaque. I think privacy statements are relatively meaningless. There is usually a vague post office box or some number you can call or email and I'd love to know what happens when you email that. But when companies do, since Optus and Medibank and Latitude and they know they can't just pay lip service. The Optus breach happened and Optus realised they couldn't just make statements. They had to look at the public facing statements and not just Optus, around what they were saying and there's many examples I could use but there are many that have in their tag line, security or we keep your data secure. I think it's about, not just about having a tag line or saying security really matters, it's about what you do and you you demonstrate that. I will say the current privacy about is an enormously powerful piece of legislation. It actually allows claimants, so people who do complain, and have investigations, to recover psychological damages. Extraordinary heads of damage in that act that are in no other act or are they recognised in common law. If you have time on your hands, if you look at some of the determinations, they are actually really interesting in that they do compensate individuals for sometimes really egregious breaches and it might not be enough or what those individuals are hoping for but it is actually quite a powerful act as it stands. The APP are quite at the moment good at recognising reasonable steps and watch this space for the Medibank and OAIC civil penalties proceedings because that's what the OAIC based the pleadings on reasonable steps and they allege yet to be determined Medibank didn't take reasonable steps to protect the information. That act is a powerful act. It's just in, and I think the Privacy Commissioner is turning her mind to how she uses that and all power to the commissioner. But it is actually, the act itself is not deficient and has a lot of remedies. You may have a view on that, Holly?

>> HOLLY RAICHE: How many of you care? Good. How many times have you read the privacy policy? All two hours of it? Really? That's one of the criticisms of the act is if you want the vagueness of what you're agreeing to which you've talked about, the length of it. If I go back to my digital platforms and other criticisms, one of the real criticisms and bug bears is consent. If you tick no and you have to go wind your way through two hours of privacy statement to figure out what it is you're agreeing to, somewhere along the line you're going to go down to the bottom and say I agree. And I think you have to question what you've agreed to. And one of the, one of the strong recommendations after a lot of discussion in the digital platforms report, was a real criticism about what you consent to, the need for clarity as to what you consent to, the need for brevity so you're not scrolling forever to consent to something. And making it very clear as to if there's any third party, exchange, what that is. And our own privacy principles limit the extent to which there should be any sharing of information. I won't go through that wording but there is a limitate. Do you care? I was lecturing other people about communication in a past life. And it was the first class in the morning and I watched kids nod off as I talked about privacy. The next morning in comes a bright sparkly little person who was irate because she had emailed a friend of hers to say where can I find a nice small fridgeor our unit? -- fridge for our unit? Anne started flowing in and she said how can it happen? I will give you the privacy lecture you slept through yesterday and you can possibly pay attention to what's being said when you consent or not and what you're consenting to. One of the very strong recommendations out of the digital platforms report about privacy was about clarity. Very brief consent statements. Very clear statements about what will happen to the data. Very clear statements about what you're consenting to, when you're consenting? And also the possibility of withdrawing consent. So that you can stop consenting to things. All these things are supposed to be clearly spelled out, they are with there creasing amendments to the GDPR. Some of that is happening in Australia but in my view not quite enough.

>> RACHAEL FALK: Just on Holly's point, what happens with your data in our company? Everyone who knows me knows I all of a bug bear about loyalty cards and loyalty statements or when you go into a shop and they say something beline like do you want -- benign like do you want us to email that receipt? That's all part of harvesting your data. I think if they were compelled to, and you signed up for their loyalty card, if they say in signing up are you OK with us sharing your data with 47 different organisations, spanning 13 countries across the world? Most people would probably say no. But because I have no obligation to be upfront about that and my best advice to you is try and avoid loyalty cards and programs unless they're really good and benefit you. And there are ones that we all love. For the most part you don't need to share a lot of data to get coffee pods or a shirt. That is all about you becoming the product. But in doing that they also build a book of customers. And undoubtedly some of them do share not necessarily your coffee pod habits but they share data about you and your email, address, phone number and things like that. Truth in data collection is a really good though.

>> MERCEDES PAGE: Fascinating. We've kind of moved into the next question, which was how aware is the general public around their privacy rights and what can be done to improve understanding? And what role can individuals play in protecting their own privacy and security? And, I mean, maybe just to expand upon that last part of the question a little bit more, I mean, aside from not signing up for loyalty programs, what more can individuals realistically do to protect their data and their privacy in this very online world that we find ourselves in?

>> HOLLY RAICHE: Well, I think we might try an experiment. Everybody, the next time you're faced with a "do you agree?" Say no. And see what happens, if you get the service, if you get the product, or whatever. Because until people start saying, "No, I don't consent," and then waiting to see what happens...

>> RACHAEL FALK: Well, you often won't proceed with the purchase. It's often not a yes-no binary. If you don't tick it, you won't be able to proceed to purchase or book, or whatever you do.

>> HOLLY RAICHE: Exactly. What is also coming in, and is coming in, in the European Union, because it's required there, there's a thing called third-party cookies - God help us, I'm not gonna explain that - except to say that every time you purchase anything online or even use Google to find information, all of that is collected. Google has gone from a company that's almost broke to one of the largest corporations in the world, based on our data. And if you think about the data that Facebook collects, it's a hundred categories. It's not just name, address, phone number. It's where you live, the size of the accommodation, is it a house, do you own a car, when did you buy it? A hundred things about you that is collected, and that means the advertising can be targeted to you based on every time you go searching for something. So, in terms of reforms, in terms of things like third-party cookies - and I was talking to Paul earlier about this - gradually, that's been phased out because the European Union is beginning to say that is unknowing collection of personal data that, unless somebody says, "Do you agree to consent of third-party cookies?" You probably go, "What is this about?" In the EU, they explain what it is. Nowhere else do they explain what it is. But it's about the collection of data that is then used to specifically target you. And it's probably about a 3-year process, four years, it's being phased out in Europe. It's less being phased out here. First of all, the question, "Do you agree with having cookies collected or not?" You don't know what the question means. The translation is, "Do you agree to have all of the personal information generated by what you look at saved for us so we can use with you?" That's the next kind of step. And that's the unwilling, unwitting collection of data that is now coming to a slow halt in Europe. It's very... You can see it's starting here. But, again, it's the consent and the way it's asked, the comprehending that goes behind do you know what's being asked? And then back to my question, do you care?

>> RACHAEL FALK: That's right. Maybe people don't care. If you think b if any of you are on Apple and you have apps, there are many apps that we all purchase for a range of reasons that actually will use your data, and they may claim to anonymise it and do all sorts of things, but, again, who looks at the terms and conditions? Because we're trained to shrink wrap, click, I accept. And Apple would know all your way of life. Who friends are, where you go. Because when you get in the car, it says to you, "It's 20 minutes to home," because it maps your home and knows where you live. Back to the "do you care?" I kind of go do I care until I don't care or until I do care? Because then I think I would care if it got creepy. But then I think of all the apps, you know, it would know how healthy I am, it would know who I text and call the most, to the point, internet searches. And it's fine until you think, "What profile is it building?" Or not. It may not be. But I guess we cede a lot in the bid to have a seamless life, where it's easier and I'm all on one device and I'm all Apple-connected, we - THEY, with respect, they are the Big Brother of the world. I'm not necessarily saying it in a malicious way, but if you think of big tech would know you better than some of our own family members, absolutely. And I think that's where we go, "Hmm. Right." And in some ways, it's great, I love the convenience of it. But do I care? Do people care? Maybe people really don't care. And genuinely generations younger than me may not care. It's about care until you... You might not care until you need to care. I don't know. That's an open question. I don't have an answer to that.

>> MERCEDES PAGE: Just to pick up on that, like, you say you might not care until you care, I mean, what is the prompt for you to start caring? When it starts to get creepy or there are security concerns?

>> RACHAEL FALK: In the New York Times several years ago, there was a women who had been diagnosed with a serious chronic illness of some sort, and it wasn't until she got sent medication on a sample basis, because they had worked out through her searches that she had been diagnosed, and obviously that data had been sold, that then that became super creepy.

>> HOLLY RAICHE: A better example, or a similar example. Father looked at daughter's emails and there were ads for pregnant women, so he went to his under-aged daughter and said, "Should we have a chat?" You know? As I've said, Facebook has got this... It's all there. We're all there.

>> RACHAEL FALK: To my mind... I tell this story, I haven't told it for a while, but sort of 10 years ago, I would be online and those ads that come in, the embedded ads, I'd constantly get ads for alcohol rehab in Thailand, and I didn't order online, by the way. I did not search "alcohol". And then "tummy tuck". I was really offended that the algorithm was putting me into some sort of category! But also it's, like, tummy tuck in Thailand - I had never looked that up. Obviously, then if it didn't know much about me, it had put me in a demographic - probably harried mother, frustrated. Clearly, I was in a demographic somewhere, so again that kind of offensive use of the algorithm that had me shaped in some strange way to do something, or to be rushing off to Thailand. But I think, again, it delivers up things based on some searches or some sense of what it thinks you want or need, maybe, yeah.

>> HOLLY RAICHE: I think it's the lesson to learn, I mean, is from the GDPR and some of the really important points that are being talked about, and we know they'll happen in principle somewhere down the track, but they should happen sooner than later. It's about consent, about what you have to be told what consent means, how you should have a right to withdraw consent, and then a good look, after all of the Medibank and everything that's happened, a good look at why you're retaining the material, for what purpose do you need it, when you should get rid of it. Or, if you're saving it, why, and what's the rationale? Because there's so much information collection that we don't think about until we think about it. And the lessons that are learned and, you know, the privacy layers, privacy reform is quite specific about the need for clarity and brevity with the statements as to what's collected, why it's collected, what you're consenting to. And doing away with, by and large, if you don't consent, you still get access - that's now in Europe and it should be here. If you say 'no' to a cookie, you shouldn't be penalised. So, there's plenty of reforms out there, many of which we already know about, but we're waiting for the second tranche of the legislation, I think.

>> RACHAEL FALK: Yes. Of the privacy, or which one?

>> HOLLY RAICHE: Privacy.

>> RACHAEL FALK: Well, yes, hopefully.

>> HOLLY RAICHE: With our optimistic!

>> MERCEDES PAGE: We do have a few more questions for the panellists, but I'm conscious of time and that there might be questions from the audience. So, maybe we could move into Q&A. If you have a question, please line up before the microphone. Just a reminder to please state your name and affiliation, if you have one, before asking a question. We also do have some questions coming in from the online audience as well, and then perhaps if there are no questions, we can go back to the remaining questions. Please.

>> Hello. My name is Anastasia. I'm a science communicator and I have, sort of, online channels where I make videos about digital rights and things. Earlier this year, I know that Meta updated their privacy Policy so that they can feed everything we've posted since 2007 to their AI tools. And at that point, I tried to remove my real face from the internet and only have my drag face up there, so I looked at Meta's Privacy Policy and I thought, "I'm pretty sure that when I delete my account, it will be deleted for them as well." I'm pretty sure, but I can't quite tell, and then I went on to TikTok and tried to delete all of the videos that had my real face in them. But I'm still getting reminders, "On this day, remember one year ago when you posted this?" I'm saying, "You shouldn't have that video. I tried to delete T" I'm just wondering if there's anything in Australian law right now, or might be in Australian law in the future, where I can compel companies to delete my data when I've deleted it for me - I want to delete it for them as well!

>> MERCEDES PAGE: Great question.

>> RACHAEL FALK: The right to be the forgotten, which we don't have enshrined, as best as I know yet. I'm not on expert. I will defer to Holly.

>> HOLLY RAICHE: I wish I had better news. Facebook's policy is, "Look, we'll take it off." And what they means it's not visible but it's not gone. They still have you. I hate to say that. They still have you. If there's gonna be a change, it would be in Europe. And the beauty of something happening in Europe, 27 countries, it means they have to start dealing with a very, very large population and addressing those things. And that's how things, once they've had to think about it, you can see that then gradually other people start to say, "Why don't we have that?" But in principle.

>> Hello. Suzanne Thompson from IAA. Can you speak a little bit about the centralised digital ID and the way that that feeds into our privacy and some of the arguments that are being made for it are that if you have sort of a centralised, say, government-controlled source of this information and people have to go to that to get the information, and whether or not that's a good idea or a bad idea - what are your thoughts?

>> RACHAEL FALK: We already had the document verification system that's managed at a federal level. It's just about allowing an organisation to check with, they don't have to get a copy of the data and that's valuable because you're not then getting data shared. So, I think that's already something that is important. And, yes, further state by states are doing that as well. I think it can only be a good thing to not hold the data yourself as an organisation, and just if you need to verify identity, it's a way of doing it in a safe way for the consumer. And I think there are enhanced obligations being looked at around for the commonwealth as well around what can be done and how that can be extended. I'm all in favour of everything that means that less consumer data is swirling around out there and that it's a safe way of sharing, or just verifying that I am me, and I want to get, say, a telco service or something like that. As for the states, I don't quite know where they're up to on that, but that's certainly the commonwealth position. I know they were also looking at in as part of the cybersecurity strategy consultation.

>> HOLLY RAICHE: I think it was probably a response to things like the Medibank and others, where why is it that all of the cache of data that was there, when if you had a better system, that all that's said is, "This data has been verified." Then when there's a breach...

>> MERCEDES PAGE: Thank you. Next question.

>> Hi. My name is Bruce from auDA. I heard a couple of you, Holly and Rachel, you mentioned the long privacy policies and most of us don't read them. I must confess, I don't read them. But I wonder if there's some analogy that might relate to something like food labelling. Because if you go to the supermarket and you pick up a jar, it doesn't say, "Go to our website and find out what's on here." In three points, it will say has it got salt in it, sugar in it, where was it made? You know, there's a couple of key things. I would think with a privacy policy, you could have a few, like, is it going to go to somewhere else, where is it stored? You know, it should be three or four parameters that you could actually make visible, I would have thought.

>> RACHAEL FALK: I think that was a recommendation of Digital Platforms. Also about material countries it's shared with as well.

>> HOLLY RAICHE: I wholly agree. The only reason they're as long as they are, and as misty as they are, is because they actually don't want to tell you that much information. It's concise and accurate, and "by the way, we share this with everybody that pays us".

>> Hi. I'm Anne-Louise Brown from the Cyber Security Cooperative Research Centre. I guess it may be sort of a challenging question, given that we're discussing Privacy Act and privacy reform, things like that. Obviously, GDPR has been held up as this holy grail of all things privacy, but we're actually seeing a bit of a shift in the European Union by the European Commission at the moment around their thinking in relation to GDPR. So, there was the recent Future of European Competitiveness Report, which is known as the Draghi Report. But it actually called out GDPR as the biggest barrier to European innovation since GDPR came into effect. And EC Commissioner Ursula von der Leyen has shifted her focus from big tech regulation to delivering Europe's digital ambitions - that's a really big shift in language that we're seeing in Europe. Is there something in an Australian context that we should be taking from this? That we should be looking at GDPR, which has been the aim for a long time, for Australia to kind of reach those same levels of privacy protections as GDPR? And actually, I guess, you know, having a look at the European experience and taking that on board and going, "Well, you know, is this actually working in practice?"

>> HOLLY RAICHE: I would be really happy if what we took on board was what our own Digital Platforms Report said in 2019. All of the reforms about what information you collect, and that should be minimal. What consent you ask for - and that should be minimal. You should allow withdrawal of consent without question. I mean, even this stuff that is really, really basic, you don't have to go back to the GDPR, go back to what - you know, I mean, a very lengthy chapter and a very thoughtful chapter, our own ACCC spells, "This is what we should have. This is our version of what it should look like." And that's very different to what exists. So, if you don't like the GDPR - which it was a catalyst for a law - if you don't like that, at least stay in Australia and implement stuff that's been there for five years.

>> ANNE-LOUISE BROWN: But, I guess, taking that into account, there is the government, I guess, the Federal Government is striving for GDPR-level-like protections. That's what the Privacy Act reforms are essentially modelled on in many ways. So, do you think, in a way, that that should be reconsidered at some level?

>> HOLLY RAICHE: The one area that I say I would recognise there are significant barriers, the small business exemption. You know, this is 2.5 million small businesses, and they're really under the pump right now. Putting in a system, you know, revising everything they do, is a big ask. But I would like for someone to say, "Well, at least start. At least have a process so that, in five or 10 years, if you're still around, you've at least reached some benchmark." Because right now it's just - it's seen as too hard, maybe on economic grounds, and maybe there's a reason for saying that. But that would make a huge difference.

>> MERCEDES PAGE: So, we have some questions coming in from online.

>> Yep, just the one here from Sharon in the chat: What are the panel's thoughts on a cashless society with reference to the protection of data?

>> RACHAEL FALK: Sorry, cashless society with reference to...?

>> The protection of data.

>> HOLLY RAICHE: Well, that's one of the reasons I always carry cash. Yes. And then it becomes, what of that data do you collect? How long do you collect it? Where do you store it? And it's like everything that Rachael was talking about in terms of, well, if you're keeping the data, why, how much, how long, and what are you doing to make sure that while you're holding it, it's safe?

>> MERCEDES PAGE: Rachael, did you have anything to add?

>> RACHAEL FALK: No, I think the world post-COVID is pretty well cashless. I think we do have to keep legal tender, which is important. Yeah, it's really easy to track every transaction. But I just think that's the world becoming more online and it becoming streamlined with digital transactions. There may be a day where there's no cash. But, yeah, I've not sort of worried about that. There are other things that keep me up at night, I think, yeah.

>> MERCEDES PAGE: Thank you. Next question?

>> Thanks, Mercedes. My name is Briony, and I'm gonna ask this in my personal capacity. I have been thinking a lot about international data governance for a little while now, and I really took the point you were making around people becoming the product, and data harvesting. And a couple of months ago, some very smart intelligence analysts finally explained to me when 6G is, and I'm sure there are a lot of technical people in the room who actually know what this is, but in a very lay person's term, my understanding, 5G is collecting data, 6G is creating data. And so we're gonna see this exponential creation of data from devices, not just from people, and the interrelation of that. How does the Australian Privacy Act and the privacy framework, how is that going to evolve? Does the GDPR deal with that? And consent solve that or do we need to evolve the policies that we have for 6G?

>> HOLLY RAICHE: We haven't got to 5G yet. How are we doing with 6G?

>> RACHAEL FALK: 6G is about more and more end points, more and more IoT, and more and more connected devices. And it's whether the contemplated changes to the - sorry, the new Cybersecurity Act does talk about a co-IoT and connected devices, but it's the data we want to keep, all sorts of data. Some of it will be dumb data, will not help anyone, is meaningless. And others will be incredibly valuable data in what we do. It's not just the data, it's the collection of data and the cyber risks it presents. Anne-Louise Brown, who just asked the question before - and I have co-authored a paper on the solar ininvestorer risk and the risk to solar investors being hacked and potentially taken down, particularly Chinese-made inverters. That's all about the IoT risk and not securing them in what we do. So, that's just one example of IoT risk. But it's the creation and storage of what kind of data will matter, and understanding what data is collected, that we will care about - both us as individuals and then what's of value to corporations or governments. So, yes, I think it's just fair to say we're moving into a data-rich world. Every year, more devices, more collection, and where we can collect it, we will. But should we keep it, and for what purpose? And there should be data we probably shouldn't keep. It's not an easy question to answer. And it is staggering, when you think of how much more - how much more data will be collected that can be used to do amazing things, but also what's needed. So, there will be a point of reckoning - and I don't think the Privacy Act contemplates that yet - but a point of reckoning about what just isn't there, what do we not need, what will people need to dump? Really, there will be a point where people, organisations, won't afford to store data that's not meaningful for them. But you're right, it's going to be a rich-data world, richer than ever before.

>> HOLLY RAICHE: Do you know, I think part of the question has to be, "Who collects the data?" You know, if you're having a little conversation with your little device, who owns that conversation, what laws are they subject to, who's going to enforce it? Because you're having regular, you know, "Siri, would you do X, X, X, X, X?" And Siri might turn on your fridge for you, or whatever she does. Some of that is obviously trash. But who owns Siri? And who collects data for Siri? And what jurisdiction does the owner come under? And what does that mean for Australian privacy?

>> RACHAEL FALK: But also more - just to sort of take this another step further - it's whether those, like Siri, whether Siri is a sentient being as well. So, will there be a time, if you're deemed to be too rude to Siri, or you're communicating rudely to your interactive devices, will you be chastened for that? Will it disconnect you? Will it refuse to deliver up responses because it deems you to be rude and talk to it in a rude fashion? We laugh at it now, but sentence is a thing of the future. And snapping at Siri and you might just get, like, an Uber rating! And after a while, you're deemed to be a really, you know, a person who's not worthy of interacting with devices. So, it sounds weird but, you know, it's been contemplated now, as we speak.

>> HOLLY RAICHE: That could solve the privacy problem?

>> RACHAEL FALK: What, just be rude?

>> HOLLY RAICHE: And then it stops.

>> RACHAEL FALK: That's right. Be too rude and you just won't be connected to anything!

>> MERCEDES PAGE: I mean, it's kind of like China's social credit score, in a way.

>> RACHAEL FALK: Yeah.

>> MERCEDES PAGE: Yes.

>> RACHAEL FALK: If you have a robot helping you, do you have to be polite to your robot? Do you have to treat it...? Will we see a human rights for robots, connected devices? I know! But, you know, we have spoken about this, and every time we do have a conversation, we do kind of laugh. But will there be a point in time - you know, it used to be funny when your kids asked Siri, "Do you love me?" In the future, having sensible conversations with Siri will be a thing.

>> HOLLY RAICHE: I love it. Privacy policies for Siri.

>> RACHAEL FALK: Siri will have her own, or his, their own privacy policies and their own code of conduct with you as the consumer.

>> HOLLY RAICHE: I like it.

>> MERCEDES PAGE: So, we're coming up to the end of the session. So, I think maybe a good note...

>> RACHAEL FALK: One more question.

>> MERCEDES PAGE: Sorry.

>> Sorry, thanks, guys. Dr Jelina Haines from the chat, a student from the University of Canberra, "May I ask what is your perspective on the importance of digital assurance, transparency and the implementation of robust policies in today's digital landscape? How do you believe these elements contribute to building trust and accountability in various organisations?"

>> HOLLY RAICHE: That's huge.

>> RACHAEL FALK: You can take that one. (LAUGHTER)

>> HOLLY RAICHE: That was asking for an opinion on just about everything we've said, I think. Is there anything in that question that we did not cover?

>> Well, how important are they... Uh, how do you believe these elements contribute to building trust and accountability?

>> HOLLY RAICHE: Well, let me repeat. We have on the cards a government commitment, in principle, to significantly upgrade Australian privacy. Now, we've seen the first tranche and it had some things that were pretty good. But if that's things like updating the definition of "personal information", the requirements about consent, requirements about what you collect... If a range of issues aren't addressed, there will be a significant improvement, but I think that, you know, we absolutely agree with Rachael - there's only so far this Act can go, and if we're looking at a, gosh, 6G, we're gonna have to rethink that one 'cause we're not there yet.

>> MERCEDES PAGE: We've spoken a lot about legislative measures. I mean, what broader changes or general advancements could there be to better protect Australians' privacy and security of data? I mean, aside from law, like, what else?

>> HOLLY RAICHE: I'm gonna use two words and then Rachael is gonna answer it. It should start with Australians actually caring about their own privacy, about what information is held about them, and doing enough to do something about it.

>> RACHAEL FALK: Sure. I think, look, legislation is very powerful because ultimately companies and organisations follow it, more than they do if they don't have to - that's kind of just a standard rule of business. But there are things, as consumers and individuals, we can do maybe as well, is from now on, if you don't want data out there, or you don't want particular things posted about you, or you don't necessarily know if you want that image out there, then not necessarily sharing everything openly on social media. Once you share that valuable data, it is out there, depending on privacy settings. It can be very hard because there are some transactions where you get involved with, where we have no choice but to share. So, it's about where you have choices, exercise those choices where you're best able to. But it is really tough in a world where so much is online and connected to have any sense of a choice around what you may or may not be able to share. But I think being conscious where you don't need to share dates of birth... I recently went to book at a restaurant somewhere and it wanted my date of birth. If you need to put one, then you don't necessarily - if it's for a transaction like a restaurant booking, I would argue maybe you don't have to share that, definitely, it's not necessary, unless you want them to know or give you a birthday greeting if it's your birthday. But it's where you have a choice to not share. I think Vanessa Teague was on the last panel. She mentioned she likes to mess up the algorithms too by having random searches to lots of different things at once, so it gets completely confused about what you like and what demographic you're in, and then that is a way, if you have time - I think that's quite clever - so not only are you having tummy tucks in Thailand, or rehab in Thailand, you're also going into aged care and then you're pregnant! It just gets completely confused about who you are and what you do. But aside from that, it is tough just being cognisant of where you have a choice, exercising the choice you want to make.

>> There used to be a website that you could go to and it would generate random searches for you and I remember a colleague and I were sitting there one day and we were pressing the button and all these random searches were coming through. Interesting stuff. Look, thank you both. I'm conscious that we have barely touched on this topic. And that we could probably talk for another hour very easily. Before we wrap up, did either of you have a final conclusion? Or thought to share?

>> HOLLY RAICHE: Rachael said it all. When you can care, care. When you can exercise choice, not to reveal your data dump.

>> RACHAEL FALK: What she said.

>> Please join me in thanking Rachael and Holly for a great session.

>> JORDAN: I can't quite get in. Great. OK. Good afternoon, everyone. My name is Jordan. I work at the Australian Domain Administration. And it is my joy and privilege to be your moderator at this most excellent session which of course falls immediately before the drinks function. Which is always nigh favourite kind of session -- my favourite kind of session to moderate because I get to annoy everyone for a period of time. Our theme today is connecting across the region. And the reason that the steering committee put this on the agenda is to give a bit of a chance for some of that from local to global work to happen in person. We're lucky enough to have two of the organisers of the Pacific IGF with us here in person today, Sarai Tevita and we have Maureen Hilyard online. We said in the destruction, many of the challenges on the table here are facing Pacific countries. And there are many challenges Pacific countries are facing which we do not face in Australia. But we're part of the region. And sharing and understanding both ways, that's happening by default in an upward trajectory in participation by people in the region. But it's also something that we can join in hearings and insights and messages from us. So thank you, Sarai and Andrew, for joining in person. And Maureen for joining online. I hope it's day time where you are. And we're going to start with an opening round of contributions from the speakers which will take about 25 minutes. And then there will be a chance for some audience questions perhaps to draw out things or other observations you'd like to make. It is a slightly shorter session. We've only got the 40 and we've started a bit late buzz of me arriving -- because of me arriving late. The order of the speakers will be Sarai, Andrew and Maureen. If they go over the mark I'll start throwing things at them! Hopefully that will work. Sara i, over to you.

>> SARAI TEVITA: Thank you for the great opportunity. First, I'd like to acknowledge the people of the land. And the protection and guidance for us while we're here away from home. I'm from Samoa but I'm here representing and we have 519 members in our chapter. And I think we are one of the biggest members in the internet society. I appreciate the opportunity from auDA to invite us here today. Samoa hosted the CHOGM where 56 countries came to Samoa. If you see on the map, just a small island, but we hosted 56 heads of government, around 4,000 people during last week. It was so interesting to be part of the CHOGM. And we saw the dedication from Australia came to Samoa, and your Prime Minister, and we saw that he got a title from Samoa. We have adopted Australia. He has the honour from our country. Pacific island Chapter of Internet. We have internet governance. Andrew will talk more about that. But it's a long time society, internet society, and we have people here in the room as well as online and Maureen, the previous year. So we have that contribution to the internet governance and woe want to see more what they can do for us. The reason I mentioned the CHOGM, all of us are part of the Commonwealth here. And it's interesting to so that they consider internet governance talk. It is good to see that. But the priorities were given to climate change. The second priority is youth and peace. Part of those priorities is internet guvenance. There's a consideration and an emphasis opinternet governance on that level. We talk about it today with the involvement of multilateral and they consider that too maybe this forum as well, we can advocate more, because there is a strong advocate, advocacy of climate change, hence the consideration from the heads of government has given and considered it. And there is a little awareness or little engagement and little discussion, more discussion of internet governance at every level or in every age. I take Samoa as an example with the current CHOGM that we hosted. Every people knows what CHOGM means in Samoa. If you see on the TV from the village, even small kid, even old people, they know that their villages adopted some countries from the 56 countries and they know what the CHOGM is. They know it's for climate change. They know it's for the youth, women. If we have that sort of approach in promoting more and advocating more internet governance because in business forum they supported it as a survival mechanism. Because the reason why the climate change and the high level of recognition is because of survival. Us from the small island states. Because we're prone to climate change and we're prone for internet governance of the digital divide. If we keep on promoting this and the importance to us, as a survival mechanism, I think we need to work together and promote more. The multilateral can consider us in that space I stop here for now.

>> JORDAN: Thank you. That was great to get a direct readout in what happened in Samoa last week. I will hand now to Andrew.

>> ANDREW MOLIVURAE: Thank you. I hope everyone can hear me. First of all, I want to thank Annaliese and her team for the invitation and having us here and the opportunity to talk about the islands. And I'd like to thank Rosemary, for the collaboration that we've had in supporting the Pav IGF last -- Pacific IGF last year and this year. And Internet NZ, we have Rose here. I'd like to say thank you for the support that you have committed last year and this year. APNIC and the team from APNIC have been very supportive! I will take a few minutes to take a few minute about Pacific IGF and why. I think as Sarai have said, we have decided to accommodate the Pacific IGF since 2018. 2017, I think. In Vanuatu. Woe have had this discussion, this dialogue since 2011. Although we've missed some years, so the last few years woe have been consistants in having this -- we have been consistent in having this discussion. It is because of the limitations faced in the Pacific for internet governance and the potential the internet gives for development and secure and trusted business platforms to boost economic growth. And we have had this for quite some time, since 2011. The leadership is within at the moment, the chapter that Sarai has mentioned is a multi-stakeholder group within the Pacific. And the leadership remains at that level with the Pacific IGF. And we have included other members within the community to be part of the multistakeholder group. The whole thing can be done anywhere and the last two years we have hosted it in New Zealand and Australia as well. And we thank Australia for the opportunity. So it's not, it has no regular funding. Same as the Pacific and Pacific IGF was only supported through partnerships that we have. We partnered with APTLD and have it in hybrid mode, where we have quite a number of remodelling locations. Buzz of COVID. We have about seven countries running hubs and that was a very good model we had back then. And we had the first face to face since COVID and the partnerships of auDA and internet NZ, APNIC and a few others and of course ICANN. And we have seen those supports and it has grown and this year been able to get support from UNESCO and also the European Union through partner ship and slowly we have gained more partnerships and more interest to support the Pacific IGF. Woe still have a lot of opportunities and difficulties that we faced because of the issue of continuity but we are resilient in the islands. We can find things to do, find ways to get a bit of support and we run with that. That is how it is at this point in time. And I think we have come so far since the first IGF in New Caledonia in 2011, we were able to get engagement and bring more of the islanders into the discussions and with the support and collaboration we have gone this far and we believe that we can continue to collaborate, especially with our current partners, to continue their dialogue, especially in a time like this when we are at the crossroads, and we don't know whether this can be carried forward as we have discussed in the few sessions ago. It is a very important time for this discussion and dialogue. These discussions with the multistakeholder but we are trying to get more governments into this discussions and we were able to have ministers into the discussions. I believe it is a growing voice and to make the voice louder we would love the support to come in. The discussions that we had in the previous session next door and I went to where it said that Australia is stand in a very well established, internet governance arena. I would say Australia stands between the Pacific and the global internet community. And I think there are opportunities to collaborate and also bring all those probably in the Pacific up to the level so that we can all contribute. Thank you.

>> JORDAN: Thank you very much, Andrew. Our third speaker is Maureen Hilyard. I do know you're on the internet and you're here to help. I'll hand it over to you and if you can keep it half past the hour and maybe a bit longer, thank you. Over to you.

>> MAUREEN HILYARD: Thank you so much. Oh, my God. Please. First of all, I want to thank the Australian IGF for inviting us to participate in your event. And I'm so pleased that Andrew is there. In person. So thank you very much. But what I wanted to sort of, just following on from what I've said, I think that the internet governance, the governance forums that we're actually, for example, being able to be here today, just gives the Pacific sort of like a much, just more of a voice. It's very seldom the Pacific does actually get a voice. It's not just the fact that the opportunities don't come up, but it's just very few people sort of get that opportunity to do so. And I mean there's 22 sort of like islands in the Pacific and they all have their own unique sort of issues and I think that this, we're so lucky that we have got organisations which have a mailing list. If people have issues, they can sort of bring them forth to the board and to be able to, so that they can actually raise those issues in the other sort of forum that they might attend. But I think one of the things that is really, really important about raising their voices is the fact that they actually can sort of work with partners such as auDA for example, and other similar organisations and as Andrew has mentioned, APNIC has been a staunch supporter throughout the whole time that I've ever been involved. And we have got, they're just an amazing organisation. But I think one of the things that is, that we're broadening, we're actually broadening our connections with people from across the region. And I think this is really, really important because more people are sort of getting to understand now just what those issues are. And they're quite, the issues are quite diverse. And one of the things that I wanted to men's about the 2011 and Keith was one of the key coord of that particular Forum, because that was actually run in conjunction with a meeting of the ministers of the region. Who were in charge of ICT transport and communications. So that one of the reasons that it was established at that time was to allow to be part of the minister's meeting but also that a lot of the ministers actually stayed behind and were actually part of the discussions at the Pack IGF. It's something we wanted to continue. But for some reason, COVID probably came a lot later, but there were lots of reasons why we didn't actually organise it again until a lot later. One of the important things and I do stress and support what Sarai and Andrew have said, about the fact Pacific want to get people, people want to get together to discuss their issues. They're a part of a lot of larger organisations and sometimes their concerns are diluted a little bit and they're not really addressed as much as well as they could be. And I think that the managers meeting in Wellington really, I know that the guys really appreciated that session because the focus was on what was important to them. And how could their partners help them address issues that are important to them. So I think one of the things that, if we can support that kind of initiative, it will be really great to sort of like make sure that we, you know, that we're actually addressing what is important to the islands and so they can progress. But I think too that we, I think that we've come a long way and I know it's really great to sort of have strong people like Andrew and Sarai and others from within the Pacific who are now really strengthening that, sort of coming from the Pacific. One person I have to mention of course is Paul Hunter who has come from the Cook Islands and now the Pacific director of the Pacific global forum of expertise for example. And I recently attended a meeting straight after Wellington actually. Where, you know, the Domingo from Kiribati has recently been made the chair of Pac. And just getting in and strengthening what they can actually do for themselves. I think this is what we need to encourage more. I will stop there. Thank you, Jordan!

>> JORDAN CARTER: Thank you, Maureen. That was very disciplined and very interesting. Thank you for sticking to time. Thank you to you all for sticking to time. We've got 15 minutes in the session. I heard a little whisper down the table that you two have got some more to say, perhaps. But I did just want to ask - we've got this opportunity with three people from the Blue Continent here - did anyone have a question for them? And if you did, it would be great if it was actually a question, not the old statement style. You do? Fabulous. Thank you, Jenny.

>> Hi. My name is Jenny. And I was wondering if you could give us an example of regulated internet for everyday use, for the every man or woman in your community? So, just to give you one quick example - if I go to a remote town in Australia, there's one library, it's probably only open two days a week, and you can only use the internet for one hour, even if you bring your own device. So, I'm just wondering if there are the same limitations for access in your communities?

>> SARAI TEVITA: OK, I'll go first, and then Andrew and Maureen next. OK. In the Pacific, they have their own different infrastructure, different regulations, and different legislations of their Indigenous community as well. But I take Samoa, because I have been in the industry for 20 years in the technical side. The coverage of the internet is 99, as per se from the telcos. But if you go out to the remote areas, some, they're still in 2G, some still in 3G, but they're promoting 4G and 5G is available. So, still underserved communities out in the rural areas, and some in the other islands, still no connection. But the availability of the internet is there. But the infrastructure-wise, still there are some problems, you know, in terms of connectivity. So, we're expecting to see Elon Musk doing the CHOGM. That's why that side of the events was in that room, because they wanted to see Elon Musk. Unfortunately, he wasn't there. Only the VIP person was there, but he was good answering our questions. And recently Samoa has accepted the standings. That will help out those remote areas that no internet or limited internet access. But there is no time limit. For that we discussed, there was a telecentres project implemented in Samoa, and fortunate to have that, in those days, the last 20 years. But now with the mobile technologies coming up, with the satellites that are available as well, so those telecentres has slowly faded. Some, there are no more telecentres in the rural areas that they used to. But the good thing is that's the starting point of learning how to use computers, how to use internet, how to send emails in the last 20 years. So, the changes of technology, the technology environment, has changed the perception of people and how they use it. I think that's the other thing, that we need to educate our community as well. Digital literacy is still an issue within our community, so we need to work with that. So, I hope I answer your question.

>> ANDREW MOLIVURAE: If I hear you directly, I think you're talking about restrictions, right? Regulations? By the government? I think most islands do not have any regulations to, sort of, block any certain group at any time. I think we are still struggling with connectivity - that's why we do not have that in place yet. But so I think there's not - we are not in that situation just yet. Thank you.

>> JORDAN CARTER: Thanks, Andrew. Maureen, do you have a response?

>> MAUREEN HILYARD: Nothing much more to add. There's no regulations as far as accessibility. I think that one of the... The key thing for us is just trying to get some of our outer islands to actually have the same quality of connectivity as it is on the main island. I mean, but they still do have, yeah, internet 24/7 - that's not a problem - especially now that they have sort of, like, solar energy, so that there's, you know, electricity for 24/7, whereas it used to be six hours a day. On fuel generation. And that was what was limiting, like, any connectivity. But we've gotten over that and we're just trying to make it a little bit faster and a little bit better for them and the outer islands, yes.

>> JORDAN CARTER: Thank you. Thank you for those. Susan.

>> Thank you for that. That was really, really helpful for getting a picture and understanding of what's happening in the Pacific and Samoa. Where my husband lives, I can't live there because I can't access the internet very well. I have to actually take the phone out and put it up onto a waterway/downpipe, where I can reach and put it, so that it just gets the 4G, and then when I'm talking back to uni or anybody for meetings, I'm, you know, stop and start and freeze. Is that the same level of access that you have? Yeah, OK, thank you.

>> SARAI TEVITA: Yes, we are in the same boat! (LAUGHS)

>> ANDREW MOLIVURAE: Yeah, I think it's common. It's common in the Pacific. As Maureen said, if you're on the main island, then it's OK. Now that Starlink is coming to the islands, in Vanuatu we have approved the licence for Starlink to operate. I think it will make a difference, definitely make a difference in those areas where the mobile network is not reachable. So, I think we're getting there.

>> JORDAN CARTER: Thanks, Andrew. We've got a tension between seven more minutes and Johanna, who wants to ask a question. Go very quickly, and then I'll invite each of the three of you to do one or two minutes of closing wraps. You might want to answer her question, you might not. You might want to come back to Susan's. Up to you.

>> My question is around not so much the resourcing but the capacity. So, I think about Australia, the Australian Government, and how challenging it is actually just to keep on top of how many different internet governance forums and meetings there are annually. So, assuming that there was funding available and the ability to travel and participate in all of the internet governance questions, to me there's still a question about the capacity to engage when a country as big as Australia still struggles to choose and be at the right meetings at the right time. And so my question to you is, what is it that we can do, as a country like Australia, in order to support - not necessarily from a funding perspective but from that building the capacity to get to the right meetings at the right time?

>> JORDAN CARTER: There you go.

>> My point is, even if you have all of the funding, you actually still can't divide yourself and go be at every single meeting, so how can we practically help in those instances?

>> JORDAN CARTER: How could Australia help, if it could help? What would be useful?

>> ANDREW MOLIVURAE: Yeah, um, I'm trying to think about the answer to that question. But I think what we... Being here, for the both of us, is quite something that has a lot of value for us. These discussions in the last day and today, there's a lot of value to us in terms of capacity-building. Because it also not only gives us some new perspectives but it broadens our idea on what to discuss within the Pacific. And we see how far we are from the discussions that the Australian IGF is discussing, especially with things to do with the in the islands. I was telling Sarai here, I said, "When you get back to Samoa, you make sure that Samoa government has a position paper." Because they have a vote at the UN on these things. So, we aim to bring that home. But this is an example of the capacity that we may have lacked in the islands that we need to maybe come to these sort of discussions to be able to understand further - not us, but probably a government representative from the islands can be here so that, you know, implications can be positive and can be done. And, again, yes, funding is also a challenge. But I think, as you say, that is not the only challenge that we have. I think the capacity is. And the other thing probably is to come to us - I was just talking to Yenn recently. I asked him if we can connect with someone in the AI regulation approach because we're having our Regulatory Internet Forum next month, and we have a session on AI, and we could learn from someone here, even presenting remotely, just to give us a perspective on what AI regulations look like. I think these are some of the connections that we need to have so that we can build the capacity there. There's a lot that I can say, and past conversations like we had with Bruce previously, and he came up with the idea of... In terms of ccTLDs, he came up with a shared register... Who are now struggling to get some money out of the ccTLDs. But that sort of discussion, I think we are getting there. We are discussing it. And Australia is now, through auDA, has been discussing a lot of issues positively with us. And I think that this can be expanded to Yenn's theme or any other in Australia who would like to be part of these discussions. Thank you.

>> JORDAN CARTER: Thanks, Andrew. We're really tight on time. Maureen for 90 seconds and then Sarai for 90 seconds. Let's see if we can do it.

>> MAUREEN HILYARD: OK, I'll try. One of the things I think that I wanted to say is that, you know, like, not all the Pacific Islands are equal. There's 14,000 people in our island, and so that when we're actually, sort of, like, have to spread people out to - who have any idea of what it is that they're actually going to be going to when there's an IT conference on or something like that, we're actually really very limited. So, it is - you know, like, I mean, it's as much as we can do. And I think that what happens is that I think what's more important is that we get our governments ... A lot of the meetings, IT does not get that much - gets probably a minute time span within the big discussions. And there's not enough. And I'm talking about my own prime minister, who I always am really disappointed that he doesn't engage himself a little bit more in IT discussions. But that's where the emphasis has to come.

>> JORDAN CARTER: Thank you, Maureen. Sarai?

>> SARAI TEVITA: Thank you, Jordan. I just want to add to what Maureen and Andrew mentioned, and say this engagement between Australia and the Pacific countries, yes, we do not only through funding but also through fellowships. We have the Fellowship from the Newcastle University that they bring some of the Pacific Islands students to the Newcastle University in February on cybersecurity. So, when we have the CHOGM, there's a team from Deloitte, a company here based in Sydney, they were there during the CHOGM, having the security operation centre. And we collected all the people from the Pacific to have that operation because of the CHOGM, you know, for the security, not only for the data, the sea, the land, and everything - everything has to be secure. So, we have that partnership and we are thankful to Australia because they are our close neighbour, and the partner for the Pacific as well for providing the opportunities. So, we do, yes, funding, the resources, and as long as we have these collaborations between governments, as Maureen alluded, it's very important to have that, the government-to-government collaboration, and then for us to push it through and advocate it. So, that has that importance. As I mentioned before, if the climate change has that facility for the Pacific, for us Pacific Islands, can go and seek for funding, why not this space of internet governance? So, as Andrew said, yes, I think 20 years ago, maybe some people already gone in our government, so it's for us that can go back and lobby our governments, since that we are in the government, and also for the Pacific, the PICISOC. Thanks to him here, mention that if we go back, have a virtual, online virtual, like, a webinar. And then invite the experts from Australia here on research so that we can more understand it. Surely, maybe only 10% in the Pacific knows about it. 20 years ago, now we want to review it and revive it. So, something that we need to look at. But thank you very much for the opportunity.

>> JORDAN CARTER: Thank you, Sarai. And thank you. One last from Andrew?

>> ANDREW MOLIVURAE: Yep. I think I just wanted to let you know that the next Pacific IGF will be in Apea, Samoa, from 30 June to 4 July 2025. Thank you. (APPLAUSE)

>> JORDAN CARTER: Thank you for sharing with us some perspectives from the Pacific. It's a bit more of a one-way sharing but I'm glad we fit some questions in. Thank you for taking the time to travel here for this in person, and thank you, Maureen, for joining us online. This concludes Day 1. There is a drinks function outside, about to begin. The sooner you get there, the sooner it will start! Sorry, Annalise? The drinks function is sponsored by Verisign. There might be a very brief remark from them outside. But cheers to a good first day. Thanks, everyone.