Jillian Whiting:

Good morning everyone, and welcome to the launch of Privacy Awareness Week for 2023. My name is Jillian Whiting and I'm really looking forward to hosting this really interesting, really important event today as we're, as we raise awareness within the public sector and also the broader community about the importance of protecting and respecting personal information. I'd like to acknowledge and welcome everyone joining us here via the livestream, including Commissioners and Ombudsmen from Privacy Authorities, Australia. And I'd like to welcome all of you here who have joined us at The Edge here at the State Library. Before we begin, I'd also like to acknowledge the Traditional Owners of the land on which we meet today and pay my respects to Elders past, present and emerging, and also extend that respect to any Aboriginal, Torres Strait Islander or First Nations people who are joining us here today.

Now in March 2023 41.9 million records were compromised by cyber-attacks across the world. According to IT Governments, Governance cloud assets are the biggest target and human error was found to be the primary cause. So the theme of this year's Privacy Week is Privacy 101 Back to Basics, and the essential everyday things that we can do to protect our privacy and the privacy of others. Our keynote speaker is Troy Hunt and his topic Lessons from Billions of Breached Records, and that will be followed by a conversation with an export, expert panel rather, that I'll introduce shortly.

Some housekeeping. For the comfort of everybody here, can you please turn your mobile phone and other devices to silent or turn them off. Toilets are located downstairs on level 0 or via the lift and to the right or alternatively past The Edge that way basically on level 1. The Edge is part of the State Library of Queensland and visitors to the space and website are governed by the policies and standards that the State Library of Queensland has put in place. It's now my pleasure to welcome the Queensland Privacy Commissioner Mr Paxton Booth to say a few words.

Paxton Booth:

Good morning. And thank you for joining us to launch Queensland's Privacy Awareness Week for 2023. I'm obviously the Privacy Commissioner, as introduced by Jillian. And I'd like to begin today by acknowledging also the Traditional Custodians of the land on which we meet and pay my respect to Elders past, present, emerging, and extend that welcome also obviously to the Torres Strait and Aboriginal Peoples here in the room with us or joining us online today. ]

I'd also like to welcome our keynote speaker Mr Troy Hunt, who will be speaking shortly. And I am really looking forward to your presentation Troy and hearing more about the threats that we face as Queenslanders in our society today. I'd also like to acknowledge the many members of the community and the Queensland Government agencies and other organisations engaging with us about privacy today. Whether you're in the room or watching the live stream, a warm welcome to you all.

This Privacy Awareness Week, regulators around Australia and across the Asia Pacific are celebrating the theme Privacy 101 Back to Basics. We're calling on the community and organisations to get back to basics, and there are some simple things we can do to protect either your own data or the data of others that we hold as custodians. Our privacy is increasingly important to us as individuals. As Government custodians of the community's personal information, protecting privacy must be a

priority to build and maintain the public's trust. As part of Privacy Awareness Week or PAW as we affectionally refer to it, the Office of the Information Commissioner runs awareness campaigns each year to help educate the community and the public sector, whether it's protecting your data or someone else's.

It's been pretty hard to miss, I think, in the last 12 months, some of the significant breaches that have occurred to people's personal data, particularly in the cyber security area with Optus, Medibank and Latitude being some of the big ones, just to name a few. It's encouraging to see in Queensland the Queensland Government adopting the recommendation too Peter Coaldrake from Let the sunshine in about an introduction of a mandatory data breach scheme for Queensland, which really I think is changing the landscape of privacy for Queenslanders. I'm looking forward to seeing that introduction in the near future.

In preparation for the impending Mandatory Data Breach Notification Scheme, we are encouraging agencies to raise privacy awareness among your staff and the community, and conduct privacy self-awareness tests or evaluations around your compliance with the information privacy principles. We recently also sent out a survey for agencies to complete regarding their breach response plans. I encourage you if you're within the agency and responsible for that to have a look at that survey and complete it and see where you sit in relation to your preparedness for a privacy breach.

In fact, I encourage anyone watching today to visit our website and find out more about Privacy Awareness Week, including some of the resources we have available, which include videos, shareable images, tips and other paraphernalia for protecting people's privacy. Thank you for celebrating Privacy Awareness Week across Australia and beyond. Both those people in the room today and joining us on live. And very shortly we'll introduce Mr Troy Hunt as the keynote speaker today.

Troy is a information security expert, and Troy is well versed on the far-reaching impacts of data breaches. I'm very excited to hear Troy speak about the lessons he has learned after processing more than 12 billion records of breaches. Just think about that number for a minute. 12 billion breaches. Wow. And it's growing. There is no doubt at all that privacy breaches and the impacts they're having among the community is only continuing to grow in Queensland, throughout Australia, and indeed the world. With that, I will throw back to Jillian now to introduce Troy, and I hope you have a wonderful Privacy Awareness Week. Thank you.

Jillian Whiting:

Thank you. The keynote for today is Lessons from Billions of Breached Records by Guest Speaker Mr Troy Hunt, Microsoft regional director and most valuable professional awardee for developer security, blogger at troyhunt.com, international speaker on web security and the author of many top rating security courses for web developers on Pluralsight. He's also the creator of Have I Been Pwned? He's talking about the lessons he's learned after processing more than 12 billion records of breached data. You'll get a glimpse of behind the scenes of what caused some of these devastating incidents and how they continue to wreak havoc today, despite how much more aware the industry is becoming. It's frightening and it's eye-opening and it's a deep look at privacy and data breaches. Can you please put your hands together for Troy Hunt.

Troy Hunt:

Thank you. Good morning. It does sound like a lot, doesn't it? 12 billion. It's kind of worse than that too because 12 billion is just what I've put into this service, which I'm going to talk about today. The reality of it is it's a lot more. There's a lot more stuff I haven't been able to deal with because time. There's also a lot of stuff out there that have never become public. I mean, Optus was mentioned before. Good example. So there is something like 11 million people impacted by Optus. Someone released 10,200 records, and that was it. And then there's the unknown unknowns. So how many data breaches have happened that we don't know about yet, that the organisations that have been breached don't know about yet? Anyway [unintelligible – "(ui)"] does anyone use this? All right, cool. Right. Probably don't need a lot of intro then. But for those who haven't, it's a data breach aggregation service. So when there are data breaches and the data is distributed publicly, often via hacking forums and other social networks where people exchange this information backwards and forwards, I'll aggregate it and I'll let people impacted by it who are subscribers on my service, there's about four and a half million, it's a free service. They get a little email. It says, look, I'm really sorry, but you've been in a data breach. And for everyone else, you can pop your email address in there and it will tell you if you've been found in a data breach somewhere.

So in processing what's now just about to hit 12 and a half billion breached accounts, including about 28 of mine, so I've been pwned 28 times. I'll talk about one of the ones that I was in shortly. In processing that, I do get to see a lot of personal information, a lot of privacy violations, because that's kind of the nature of a data breach, right? And in exposing so much personal information, it makes life hard not just on the individuals but the organisations that are obviously breached, and then other organisations that might be completely unrelated, so other organisations trying to validate identities.

So a few years ago, I got invited to Congress in the US to testify on the impact of data breaches on verifying identities, which is kind of cool because I got invited and it's like, you know, I'm Australian. Like are you really? Yeah, it'll be fun. It'll be fun. And it was. Like it was really, really super interesting. But the premise there was that a lot of the way we verify ourselves, which we've all done before, is by knowledge. So how many times have you, I'll give you a very specific example actually. My father the other day wants to upgrade his phone plan. So he calls up Telstra. He says, I'm Steve Hunt. This is my phone number. And they basically went, well you say you are but we need to prove that you are. What's your date of birth? Like oh Jeez. He has lots of birthday parties. Well, okay every year he has a birthday party. He's been in data breaches. My dad's not the sort of person to post that to social media. But a lot of people have their birth date there.

So when we're using particularly static knowledge based authentication, so things that are immutable that we cannot change, date of birth, mother's maiden name, first car, first school, all this sort of stuff, it gets leaked once and how good is it? It becomes near useless. And here's a really good example of this. So this big cure people is from last year. Optus customers, going to change their driver's licence numbers. So everyone saw the news about Optus. And of course, the other major ones that Paxton mentioned that followed that, everyone has seen this on the news. I mean, cybersecurity is not something that we just see within privacy circles or tech or infosec circles. My mum and dad see this on the news the whole time.

So everyone's going to change their driver's licences because they had to provide their driver's licences when they got, let's say a SIM card. Now, one of the things that we often tell people or advice we give them of privacy, we say don't share any information you don't have to. If you go to a website and they ask for information that you don't need to give them, don't give it to them. Has anyone tried getting a SIM card and then saying you're not going to give them any proof of identity? Because what's going to happen is they'll say, well, you don't get a SIM card. Well think about

Medibank. If you went to get private health insurance and they say, well, we need to know your pre-existing conditions. You're like, I'm not going to tell you because privacy. Well okay you don't get a private health plan.

And this is the problem we have because we need to provide information for legitimate purposes for a lot of these things. But then we run the risk. So how do we choose? How do we balance? I thought it was interesting before Jillian used the stat I've heard before that say, you know, the vast majority of data breaches are related to human error. Can anyone think of a data breach ever that didn't involve human error? It's like I don't know how this happened. Everything went perfectly well. It's like no somebody made a mistake somewhere. They reused a password or we wrote some sloppy code or we misconfigured a database. 100% of our data breaches have a human error component, and very often it's more than just one human. It's more than just one single point of failures. It's multiple things.

So we go around with these driver's licences. And what I find sort of fascinating about this, and I think about Optus as well, it's kind of twofold. So one is that it was terrible that all of this data got exposed, it exposed a lot of personal information. Obviously, that creates all sorts of problems, everything from mild things like spam through to identity theft. But on the other hand, it's crazy that we're so dependent on this to verify identities. You know how many problems they have in the US because of social security numbers? Which is like the big secret that you give to just about everyone that you do any sort of business with because you need to verify your identity.

So our challenge is not just stopping data breaches, but it's being able to do better things with identity verification as well. One of the things I always find a little bit ironic in this day and age is we're walking around with like cryptographic devices in our pockets. I've got one on my wrist. We've got lots of ways of doing strong identity verification. But we're reliant on nine numbers. And it's different State by State too. I think it's Victoria, New South Wales, not only do you need the driver's licence number, you need the card number as well. So now we're dependent on two numbers instead of one.

This is the person who hacked Optus. Representation of the person that hacked Optus. So if everyone remembers back in September when this first happened, we heard that the data was posted online somewhere. Now, it wasn't posted to the dark web. That's one of the things that drives me nuts. Every time I get this question it's from journalists. Is it on the dark web? And I go, no no it's much worse than that. It's on the normal internet. It's on the clear web. This was on a hacking forum. It's called Breach Forums. Subsequently taken down by FBI and Friends, that superseded the one before that Raid Forums, also taken down by the FBI and Friends. You'll see that as a recurring theme today too.

And the person who posted the data said the vulnerability was a regular API customers used to gather their spelling, not mine, own data, but this URL has access control bug. So I don't know if you recall but when the breach first happened, the Optus CEO was out there and the usual response from CEOs of companies who have breaches, oh it's very sophisticated. Maybe the Russians, you know, it's like that sort of thing. And then Claire O'Neil comes out and it's like, no, this was really simple. And she's right. And we have lots of empirical evidence about how this happened. It was literally changing a number in an address bar, which is fascinating because you go, how does someone who is almost certainly either a child or a very young adult, someone inexperienced, unsophisticated, how do they manage to do that much damage to a multibillion dollar organisation? It's a huge amount of leverage usually from kids.

Now the challenge is not just the data that we lose via the likes of websites, we're now losing data from things. And I want to give you a good example. I'm going to give you three different IOT examples. I like examples that I've been personally involved in. I was in Norway a few years ago doing a training course. And one of the things we do in the training course, we'd look at mobile apps and we'd look at the way they communicate to services and we try and figure out how they're put together. And someone in my workshop had one of these. This is a Nissan Leaf. I'm pretty sure we don't get these in Australia. They're an EV because everything in Norway is EVs.

And it has a companion app. And the value proposition of the companion app is without getting into your car, you can turn the heater on because it's so cold in Norway. You can get the status of your battery, you can get your trip history. And what the guy in my workshop was interested in is, he said., this app must somehow know which car to talk to because there's lots of apps and there's lots of cars. And the way we'd normally do this is that you'd enrol into the service and you get some sort of a cryptographic token sent to the app. And then every time the app communicates with the car, it's in the cryptographic token, that's your secret.

Now, Nissan decided that the secret that they would use is the one printed in the windscreen of every car. So this is your VIN number. And it's worse than that as well, because not only is it printed in the windscreen of every car, but it's a numerable. And the reason I've obviously gave the last few digits here is because you could just keep adding one and finding more cars and turning on the climate control.

Another theme you'll see here is I had a lot of trouble getting Nissan to take this seriously. And the way I eventually got them to take it seriously is after a month of backwards and forwards with them saying this is a major, major privacy issue, I said, I'm going to publish a blog post about this. Would you like to make any comments? And they said, yes, please don't publish the blog post. So I published the blog post and after that suddenly it was important. And this is one of the things that sucks about this industry at the moment. Often it takes a lot of encouragement of organisations just to do the right thing.

Here's another one. This is my daughter Elle. Elle was six years old here. This was four years ago now. And she's wearing a smartwatch designed for kids. And the value proposition of this, they call them helicopter parents. They say people are so worried about their kids they want to have a GPS tracker on the wrist so no matter where they go, you can see where they are. And, you know, they haven't been kidnapped or they've been kidnapped and the kidnapper has taken the watch as well. And that's another problem then.

So a friend of mine in the industry said, look, I've been looking at a bunch of these watches. This one's actually marketed in Australia. A company here in Brisbane called TicTocTrack. We think they're going to be terrible. Let's go and have a look. So we got one for Elle and we sent her to tennis camp. And we discovered that every time the mobile app, which tells you where the child is and allows you to call the child, uses an identifier to match the child to you. It's called a family ID. Now my family ID was something like 2317. And you'll never guess what happens if you subtract one from the number. You get another kid. We only subtracted because I was the last person to register.

So is IOT starting to leak data and leak privacy in ways that we never had to deal with before. And on the kid theme, anyone got one of these? No. Good. All right. So these are messages you can hug. They're called cloud pets. And someone a few years ago popped up and said, I've got the cloud pets data for you. Well, first of all, what the hell's a cloud pet? And then I learned. So these are pets that have a speaker and a microphone and a Bluetooth radio and a button in the paw, and they've got

their little love heart here that can flash. And the value proposition is children can record messages into the teddy bear, sends it up into the cloud, and then a parent or grandparent or someone else gets the message and then they can relay it back to the cloud pet.

All of that data, including all the kids' voices and all the kids' messages, went up into the cloud, into a database with no password. And someone found it and downloaded it. And we had the same problem again, couldn't get the organisation to pay any attention. I use journalists a lot because they're very good at getting responses from impacted companies. I just remember this journo I worked with, someone I really trust. I said, look, the CEO of the company has said we did get reports about a data breach, but you don't reply to some random person on the internet. I'm like, well, but that's who submits the data breaches. It's random people on the internet.

So we're sort of running out of options here because we're trying to minimise the data that we provide websites. But then you've got Optus and you've got Medibank and you've got to give them data. So what if we just take it all offline and we just go back to pen and paper? Which brings us to this one. Now, this was our number 1 data breach in Australia up until last year. Was anyone in the Australian Red Cross Blood Service data breach? Only me. Okay. If you have donated blood, so you should be in the Red Cross Blood Service. So I had gone into a blood van which came around to our office years ago. And I remember very clearly going in there, and they gave me a piece of paper and a pencil, and I wrote my data in here before I donated blood. And then somehow that ended up here.

And someone had popped up a few years ago and said, look, I've got this data, and this is what normally happens. It's like someone with a hoodie because they're a hacker. It's usually that way. They pop up and say, look, I've got this data, about 1.3 million Australians they said. Now we later learned it was about half that. But every time you donated blood, you got a new record. And this is what the data looks like. This, for the most part, is very, very generic data insofar as we see it over and over again in databases, including date of birth, which was the problem I spoke about at Congress, static knowledge based authentication. And including blood type. And I don't know how I feel about that because it's medical data, so it's sensitive personal information. And the bit I don't know about how I feel about is what happens if a hacker gets it? I don't know. I honestly don't know what you can do with that.

But maybe that's one of, it's a little bit like at the moment where people go, oh I'd never use one of those DNA testing services because what happens if a hacker steals your DNA? So, okay, first of all, I don't think it's quite that, it's not like you're going to walk out one day and there's another you somewhere because someone's cloned you. I don't know what they'd do with it. And more importantly, I don't know what you could do with it in 10 or 20 or 30 years from now. That's what makes me feel a bit uncomfortable.

So anyway, I was interested in this, so even though he said it doesn't contain passwords, because really, to answer that question, have I been pwned? We don't need a password. You just need to know if some sort of primary key to your life, usually your email address has been breached. So I said, yeah, look I've, I'm interested in that. I could be in there. And he's like, yeah here's all your data. And this is confronting for me. Like 12 and a half billion record or whatever. If I see my data in a breach, I feel this in the pit of my stomach because I'm just like wow. And this was my old hotmail address, my real date of birth, which I redacted because it's still static knowledge-based authentication.

I wasn't happy about that. And what's curious about this guy is he said, look, he was just scanning IP address. This is what a lot of people do, they just cruise around the internet in a very automated way, looking for things that are exposed. And he said, not a bad person. Our belief, our being myself and the Red Cross, because I reported it through to them. I think they did a fantastic job of disclosing it and cleaning it up. Our belief is that that was true. I certainly never seen it appear anywhere else. But what he'd found was just a database backup. It was an IP address. 5th of September 2016 australianredcrossbloodservice.sql. So one of their vendors had taken a backup of the production data to do some testing. And this happens all the time.

So we get this data exposed a lot. And what we've sort of done as an industry is we said, look, we've had so many data breaches of things like email addresses and passwords. We need to move away from just authenticating people on what is effectively like two things that you have in your head. So we need to use two factor authentication. You've probably all had to get an SMS or use a soft token or hopefully a universal two factor security key. So we're getting better and better. And what's curious about this industry is everything that we do to make it better, someone comes along and messes it up for us.

So when you authenticate to a website, username, password, maybe a second factor. And then you keep clicking around. The way you normally stay authenticated and stay logged in is with cookies. So you get a cookie set on your browser and the cookie gets sent over and over again. Intelligent websites also fingerprint your browser so they'll look at it and go, well, this person's running on whatever version of Chrome it is this week and they're on a Windows machine. They might look at other attributes of your browser and they'll create a unique fingerprint. So between the cookies and the fingerprints, no one can take your identity just by having your username and password.

And then these guys came along and messed that up. This was Genesis Market. And Genesis Market made a marketplace out of selling the fingerprints and the cookies, along with the usernames and passwords and all the other data. And you could go online and choose which victim do you want? Now have a closer look at one of these. Take this one here. So this is someone in the UK, their browser fingerprint tells us, along with the cookies that they're currently logged in to Dropbox, Gumtree, Yahoo, Amazon, Facebook, so on and so forth. You can buy their identity for $41.30. It's on sale. It's a good deal at the moment, because it's normally $59. So it's a marketplace. And I think this is one of the things people find fascinating that this, for all intents and purposes, looks like when you go shopping on eBay or somewhere like that.

Now, the thing is, if you're an evildoer and you go and you buy this fingerprint data and the cookie data, what do you then do with it? So what Genesis Market did is they made a browser plugin. They made it really, really easy for everyone. So you'd go and get this browser plugin so that after you bought the identity data, it could set it all in your browser, so it could set the cookies there, it could set fingerprint data, and you'd then go to dropbox.com and you're already logged in as that person. Now because they're so service orientated, they care about your comfort, I always find these descriptions kind of interesting. So how do we get here? But this is what the site did and this is what it looked like until a few weeks ago. And now it looks like this.

Now, this makes me very happy for many, many reasons. One of the reasons it makes me happy is we have so many great law enforcement agencies around the world working together. So we're up here with the AFP. The UK's NCA is there. What have we got? Germany, Italy, the Netherlands, Poland. About 17 different law enforcement agencies worked together to take down Genesis Market. It was only a few weeks ago. It also makes me happy that the FBI then sent me the data for Have I Been Pwned? And I guess what makes me happy about that is there are about 8 million

people whose data is being sold like this. And the FBI said, look, we generally don't go around emailing people saying, hey, we're the FBI, you've been pwned. That's just not our thing. Seems a bit like fishy.

So it's not the first time they've done it. We've done it with other incidents as well. But they sent me the data, we put it in Have I Been Pwned? And those 8 million people can now come and see whether they've been exposed. I feel like the FBI has become a combination of sort of very progressive because they've let a lot of stuff like this, incidentally in conjunction with the AFP, these organisations work really, really closely together. I also feel the FBI has become increasingly, increasingly fun because I love this imagery. Right. It's like an FBI agent with a hoodie hacking away on the screen with the hacker looking back at them. And they called it Operation Cookie Monster, as you can see, because it was the operation where they took down the people that were selling the cookies.

And just to mess with them even further, the FBI, whoever did this, put a munched cookie next to them, which I think is lovely. I think it's a really nice touch. So one of the themes that I've had coming through here is it's very, very difficult to get organisations to take data breaches seriously. So time and time again we go through this. And it's, I wrote something years ago about basically the, it's like the mourning process of data breach. You know, like the five stages of grief, the Kubler-Ross kind of cycle, it's like that where they come out originally and they're like, no, no, no, there's nothing to say here. Everything is fine. And I can be sitting there with millions of their records. I remember one in particular caused me to write that blog post where there's all these credit card numbers and they're like, no credit card numbers have been impacted by this. Well, what's this?

So getting them to take it seriously is very, very hard. And this is going to sound kind of crazy, but even being able to get in touch with an organisation to say you've had a data breach is ridiculously difficult. Now I'll give you an example of this, and I'm not sure whether this is the case or not, but it's feasible and it relates back to Optus again. So again, this was the person responsible for Optus. They created this account on the now deceased Breach Forum's website. And one of the things they said here in this announcement is, if you're reading this, again their spelling not mine, we would have reported exploit if you had method to contact. No security mail, no bug bounties, no way to message. Now, to be absolutely clear, none of this justifies them going and dumping a huge amount of personal data, nor taking it in the first place.

However, in fact, we were just having this discussion about this very gradual decline in many people, it could have been very easy that they found a vulnerability and tried to find a security contact, couldn't find one. Maybe even sent emails, couldn't get a response. And then perhaps they said the only way I'm going to be able to get them to take this seriously is to do something like this. Now, why they then asked for a $1,000,000 ransom. Okay that's a different issue. I think it's probably pretty obvious why they did. They're a combination of greedy and stupid.

But this is a major problem. Being able to disclose not just data breaches, but security vulnerabilities. And what's kind of crazy about it is that we have a mechanism to do this in the industry, and it's really, really, really simple. It looks like this. Google.com/.well-known/security.txt. So there is a spec for a security.txt file. Now, you can read this as a human. It's not particularly technical. There's a contact link here. There's an email address there. There's a public key for if you want to encrypt your message. And this security.txt spec, it is free. It's a text file that you put on a website. And then people find you by this. Every single Google asset has one. Many large organisations do. BBC has got one like this. Australia's largest website that has one is realestate.com.au. Looks like that. Have I Been Pwned definitely has one. You know who still doesn't have one? Optus.

So what ends up happening is people go and find data security vulnerabilities, something exposed. They get in touch with me and then I end up on Twitter posting messages like this after I have exhausted every possible avenue trying to get in touch with the organisation. And I typically go through, I look for the security txt. Never, ever found one for a data breach. Probably because they're not that focused on security to begin with. I go through the contact pages. I go through social media. I go through LinkedIn. Can I find the CEO or a CTO or God forbid CSO, someone whose sole role is information security. And I send messages like this.

And time and time again I get nothing back. And I give it enough time. And then I'm like, well, I'm sitting on usually millions of records of personal data. I've got subscribers in here. People need to know about it. And it shouldn't be my job either. You know it's not that I begrudge it, but it shouldn't be my job to tell people that an organisation has lost their data just because they won't respond or we can't get in touch with them.

So I thought I'd leave you something a little bit more light-hearted, which sort of illustrates precisely the problem we're having in this industry in ways that I think will be relatable to everyone. There's a YouTube channel called the Lock Picking Lawyer. And he's this guy who just goes around doing like physical penetration tests to padlocks. So what he will do is he'll get some awesome looking padlock and then he'll have like a toothpick and some floss or something. And five seconds later, he's opened the padlock. And because he's a responsible guy, he always reports any findings like this to the organisation before he publishes it publicly.

So a little while ago, he's testing this padlock, which is a biometric padlock. And of course, the value proposition is you don't need a key, you don't need a pin, you put your finger on it. The padlock unlocks. Anyway he notices a screw. And what you're all now thinking happens did happen. He takes out his screwdriver and he undoes the lock with a screwdriver. Like that's it. No key. No secret. So because he's responsible he reports it and he sends them an email and he says, look I've got one of your padlocks. I got my screwdriver out. I undid the screw. The lock came apart. And the organisation responded in a way that perfectly illustrates the problem we have online as well. They said the padlock is invincible to people who do not have a screwdriver. On that note, thank you very much. Cheers.

Jillian Whiting:

Thanks so much Troy. Can I close this down? Is that all right? Okay. Before we continue, I'd like to welcome Aunty Kathy to the stage. So Aunty Kathy is an Aboriginal Elder who was born and grew up on the Cherbourg Aboriginal Reserve. She now lives in Brisbane, where she's linked to the Turrbal people through kinship ties. So she has a very strong spiritual connection to her people and traditions and so she is here today on behalf of Turrbal Elder, Songwoman, Maroochy. So can you please welcome Aunty Kathy to the stage.

Kathy Mills

Thank you. That's very interesting, wasn't it? No privacy in this world. I could say a few other words about people who hack. (ui). Yeah, I'm good. But thank you everyone. My name's Catherine Georgetown Fisher. I was born on an Aboriginal Mission called Cherbourg, which is in South Burnett, about three hours away from here. Cherbourg was made up of about 48-50 different language

groups. And the majority of those languages came from Queensland, north, south, east and west of Queensland.

And it was part of that assimilation project where they brought in people to bust up our laws and tradition. I'll give you an example. My father's mother was stolen as a child from the Georgetown District in Far North Queensland, along with their little brother and another little sister, and they were taken away from their parents, their mother and brought all the way down here to a foreign country, what we call our lands, country yeah. And so she wasn't able to speak our language because there was no one else to speak it with.

And the majority of the children that was growing up, they could only, they were told only to learn English. And the same with, happened with the Turrbal Nation here in Brisbane and the surrounds. The five clan areas, both north and south of the Brisbane River was part of the Turrbal Nation. Those that weren't slaughtered, they did slaughter the majority of the Turrbal People. Those that weren't slaughtered were taken from here and taken north, and they ended up on Cherbourg as well. That left it open for the other tribes to come in and claim country in here.

But, you know, through all the atrocities and the degradation our parents and our grandparents went through, one thing I'll give them is they came through. They held their eye and they came through with, they held their dignity. And they never passed on any anger or, to us children. So that was a good thing. That's the dignity that my old people held. That stays with me today.

(Speaker speaks in Aboriginal language).

What I'm saying is you're walking in the footprints of the ancestors of the Turrbal nation. So wherever you travel, whether it's here in this area or through this country, you're walking in the footprints of the people who were here before you. And always feel the land when you're out there. Walk and feel it. Feel the spirit of the land.

(Speaker speaks in Aboriginal language).

Blessings to you all. Blessings to you and your family. It's a good subject if, today. I wish I could stay. But I want to sing a song. Like one of the old men that was taken off his country, that was taken to Cherbourg. When we had white officials come to the Mission to check up on the natives, our, usually our men would have to be, have to paint up and do corroboree for them. Because a lot of times one thing, I'll give my old people that came from all the different areas, they kept their songs and the corroborees.

And this old man used to sit around his own camp fire singing to his family about wanting to go home and sit down in his own country, sit down, go back to his own bora, to his own ceremonial ground. Because they took him off his country. He was a Kabi Kabi man. And I can't see it in his tongue. But I will sing his song for you in memory of him.

(Speaker speaks in Aboriginal language).

Thank you and have a wonderful session. God bless you all.

Jillian Whiting:

Thanks so much Aunty Kathy. I'd now like to welcome our panellists to the stage please to continue the discussion on privacy. So Nicole Stephensen, IAPP member and Knowledge Net Chair, Dr Alistair Ping, Adjunct Professor, QUT Graduate School of Business, our Guest Speaker Troy Hunt, and also

Paxton Booth the Privacy Commissioner. Can you please welcome our expert panel. You've got slide in there. Yes. Yeah so a little bit more detail. There's a lot of, I find there's a lot of information out there about breaches and cybersecurity and things like that. But I found a Thales data threat report on the latest data security threats based on a survey of nearly 3000 IT and security professionals in 18 countries. And as we've mentioned before, nearly half IT professionals believe security threats are increasing in volume, and cloud assets are the biggest cyber target. The increase in cloud exploitation and attacks is directly due to the increase in workloads moving to the cloud. And as we mentioned, simple human error, misconfiguration and other mistakes are the leading cause of cloud data breaches.

Now that has surprised me. Nicole you're a partner of IIS, a privacy program management specialist, a self-described privacy geek. What are your thoughts on that?

Nicole Stephensen:

Yeah. Well a number of people in the room will know that that's very true. Some people like an app. Other people like (ui) privacy. When it comes to data breach I think we focus a lot on the, this stuff, the things that look like hackers in hoodies and, but it's really important to remember that data breach can happen in other ways as well. So in our public sector setting, which is really relevant to a number of people in the room today, a data breach we must remember is about unauthorised access, disclosure or loss of personal information. Now that kind of unauthorised access, disclosure or loss can happen by losing your thumb drive while you're on the bus on the way home from work right or it can be having something sensitive drop out of your bag while it's go through the airport security monitoring station or heaven forbid you know failing to use the BCC function on your emails and having email go to the wrong people. Those can all constitute data breach and in that sense, if we're focusing on things like human error, yes there was a human error. But I'd like to think that more important than focusing on the error is the fact that something has happened that a person really needs to report, particularly say an individual whose maybe error or has had (ui), we need these cultures of reporting within our organisations and (ui) we really need to report to an organisation so that we can get these breaches under control and quickly. If we can't identify them, we can't make up any of these stats that we're reporting today.

Jillian Whiting:

Well, that's what I was going, there's so much personal information goes through a lot of hands every day. Well how do you identify the risks? Anybody?

Nicole Stephensen:

Sorry do you want me to continue with that?

Jillian Whiting:

Yeah, sure.

Nicole Stephensen:

So I guess identifying the risks relates to what type information are we talking in the first place. So when we talk about data, in (ui) context we talk data. And data is (ui) information but it's not necessarily applied to a particular context. When it's information about you and about me and (ui) or it could lead to us being identified, then rings the risk out for us right. How that's where our risk profile sits. So we need to know what data we're actually talking about in the context of a breach or a potential breach event and work from there.

Jillian Whiting:

Troy if you can talk to more about how small breaches can have such a big impact.

Troy Hunt:

I mean, it's interesting because there's so many different ways that we can have data breaches and so many different ways impact individuals. I mean, I mentioned before it could be something as minor as spam. Everyone gets spam. It's not much fun. Everyone probably gets phishing attacks. Probably every day I get what looks like a phishing email. I file it away and I report phishing and that's it. But I guess what we're most worried about is, is the likes of identity theft using personal data, particularly personal data that is immutable?

And it's not just your date of birth or your mother's maiden name. You sort of made a joke before about things like biometrics. Look I don't know what happens. We've already had multiple data breaches where biometric data's been exposed. We had a major one with the Philippines Election Commission a few years ago. So I think we're just sort of on this trajectory where we have so much information that is so robustly collected and stored and archived that of course we're heading in a direction where we have more data breach. And I think the last thing I would end on, before I went to Congress, I put a question out there and said, what does everyone reckon I should say? Like give me something insightful.

And someone said, we need organisations to stop always looking at data as an asset and also start to understand it's a liability. And I think this is the problem we have. When we look at those two major breaches last year, how much data was retained that became a liability and it just didn't need to be there?

Jillian Whiting:

Alistair to you. Your area of research is why good people do bad things. How easy is it for good people to unintentionally breach others' right to privacy?

Alistair Ping:

Extremely easy. And the example that Troy gave of the hacker saying, look, I'm not a bad person, I didn't mean to get this. That's a good example. I think one of the key things is that we tend to work on the assumption that bad things are done by bad people, and we see these breaches and think, oh

that's terrible, I would never do that. But the simple reality is that really bad breaches don't happen suddenly. They happen gradually. So it's a result, a bad decision gets made a long time ago and then you start slipping down the slippery slope and then bang, suddenly it happens.

So one of the key things is just to be aware, all of us need to be aware of how easy it is to make a simple, dumb decision. And then also the second thing is that when you've made the dumb decision to be willing to go, far out, I've actually done a dumb thing. Help me, rather than thinking, oh it's just this one little thing and I can fix it. So yeah, it's a very interesting, complex area and that we need to be, all need to be very aware of how easy it is to do these things.

Jillian Whiting:

Well how do people justify themselves then?

Alistair Ping:

Yeah. And again, this is the really weird thing. So the first thing is, so the trigger is you kind of feel a feeling that something is unjust and you think, oh I need to do something about this. But then you then, generally what happens is people invoke these flawed justifications. They go, oh I'm just following orders or I'm doing it because I deserve it or because they deserve it or it's a stupid rule. Anybody or everybody else is doing it. And you end up justifying basically an unethical act.

Jillian Whiting:

And the impact, as we've mentioned, can be catastrophic.

Alistair Ping:

Yeah, because then what happens is, as I said, if you justify it using a flawed justification and then you think, oh it's just this one little thing, I can fix it, then like I said, you're sliding down a slippery slope and sometimes that type of behaviour can become normalised. So, you know, years down the track you go, far out how did this actually happen? It happened way back here when the thing started. So yeah, very, very pervasive.

Jillian Whiting:

Paxton we'll bring you in here as the regulator. Is technology outpacing policy?

Paxton Booth:

Look, I think technology always outpaces legislation. It's just the nature of the beast. Technology is changing so quickly, probably at a geometric rate. It's increasing in terms of the things we could do today we couldn't do you know 10-20 years ago. When the Evidence Act was written in 1977 in Queensland, you know, computers just weren't around like they are today.

Jillian Whiting:

So much has changed yeah.

Paxton Booth:

It was written in a world where everything was on paper. So there is no doubt that legislation struggles to keep up with changes in technology. And, you know, whilst the legislative review of our Act in Queensland, it's necessary and it's important, it's not sufficient either. Agencies really need to take a proactive stance in relation to how they apply emerging technology, because ultimately in most cases I think technology is relatively neutral. It's about what you do with it in terms of what you should make of it, in terms of whether it's a good or bad outcome.

So what we really want to see agencies do is develop that privacy by design approach to using new technology and think well actually what might happen if I use this? I mean the example that I think Troy gave before was really interesting where, was it the cloud teddy?

Troy Hunt:

Cloud pets.

Paxton Booth:

Cloud pets. Probably someone had a really altruistic view of what would happen with those toys. Not thinking that it was actually a major vulnerability to put this information up on the cloud in an unencrypted pattern or unencrypted format. So being aware of the risks of using new technology is really important for agencies and individuals as well.

Jillian Whiting:

Nicole, privacy by design, that's something that you, is big for you.

Nicole Stephensen:

Yes it is. Yeah and I think to prove Paxton's point, if we're looking at engaging (ui) who deploy particular types of technologies or rolling them out ourself and building them ourselves, we have to remember we can't really do privacy by design if we're design for something that is intended to protect or respect privacy to begin with. So we typically see this with things like facial recognition technologies right or cameras that are used to surveil a population in order to make decisions about them in relation to whether or not they're going to be able to access services or benefits. It is very hard to design for privacy in that context. Although you can design quite well for data protection, which is, it's you know part and parcel of privacy, the security component. But you really can't, you can't necessarily say that you're designing for privacy in those sorts of circumstances. To Paxton's point though, while we're waiting for the regulation to catch up, we need to be engaged in some good decision-making. This is important in Government and an example that came out of the triple

C's recent Operation Impala, which many in the room might be familiar with, is this a chronic problem with our Government agencies, having individuals with, authorised individuals having unauthorised levels of access to systems or technology or the information within those systems.

And that kind of unauthorised access is a behavioural challenge to Alistair's point. It's, somebody thinks their entitled to have access or they think that they, the information's theirs. So it would be more expedient for them just to access it and use it. But they're creating a situation here, back to the original topic I guess of a data breach or a security incident, that need not necessarily occur.

Jillian Whiting:

So how important you know as an early focus on privacy, particularly for e-Government and technology and innovation initiatives, how important is that and how do we get it to happen?

Nicole Stephensen:

Right. So this is probably my mantra right. It's about ensuring that privacy people have a seat at the table early. So when we're making the decisions in Government or in our organisations, I think privacy shouldn't be seen as a road block or a drag on progress or the office of knowing how many times have I walked into a room and I just see the energy in the room drop.

Jillian Whiting:

Oh she's here.

Nicole Stephensen:

Oh she's here. She's going to tell us to stop our project. Now I wouldn't have to do that, though, if I was engaged early enough at a time where projects are being conceptualised or vendors are being first asked to prepare submissions on supporting Government or our organisations with a particular technology that they have. That's the time to have me in the room to answer some of those questions about not just can we do this activity? But should we do this activity? And what are the limits that we should place around personal information handling?

Jillian Whiting:

To the rest of the panel, what are your thoughts on that? Alistair?

Alistair Ping:

Oh totally agree. That's such a good point. And I mean, the big shift in here is how do we shift from being reactive to being intentional. So the reactive stuff is, you know, Optus and that reacting to a breach. The intentional stuff is thinking about it from the start and thinking about, okay what are we actually trying to create here and what are the values that are going to guide us? And then the

second bit is to be aware of how things like expediency can be used to justify bad decisions. We haven't got time to do the privacy stuff. We need to get this done.

So yeah, it's a critical shift and it's particularly important given the way, you know, society is changing and the way we're being bombarded by so much different information and so much change going on. It can diminish our capacity to think about this intentionally. So we really, really need to be intentional about it.

Jillian Whiting:

Troy any thoughts from your perspective of how we make it happen?

Troy Hunt:

Well, I think part of the challenge is with security and privacy, when you're inside an organisation and they're looking at where to spend money, if they spend on marketing or sales, they get more sales or more products sold or whatever widget it is that they're selling. If we do security and privacy right, nothing happens. Like you get to the end of it, okay how much money did we make out of this? Well, we didn't lose any. You know, like that's the outcome. And it is a hard ask of organisations.

But I think to Nicole's point, there's a lot of stuff we can build in early on, I think particularly the excessive permissions problem. This was one of the things that Medibank said. Look, one of the possible ways in was someone had access via a privileged account. We have these principles, principle is privilege. What's the bare minimum access rights that someone needs in order to do their job? But a lot of organisations aren't culturally adept to that as well. I remember one story where a manager said I want all of the same controls and access rights as my subordinates because I can tell them what to do anyway. It's like, yeah, but you lend your computer to your kid and you know now they're doing something that your software developers could. And that's not a hard problem. We have patents for this, but it requires organisational change too.

Jillian Whiting:

Paxton from a, from your point of view, from the regulator, early focus on privacy, how can that happen?

Paxton Booth:

Look, from my perspective, we had a really important report come out early this year which had a slightly different focus, but some of the points that were made in it were really significant around Peter Coaldrake's Let the sunshine in, around you know the importance of culture within an agency, and obviously the focus there was around culture and integrity, culture, transparency and accountability. And the same goes though for privacy. It is so important to have that strong culture within your agency around the importance of protecting privacy.

And that will lead on, that will kind of you know flow down the chain, so to speak, to your employees. If people are having those conversations in the office about it on a regular basis, raising

the awareness is so important. And I think this kind of goes back to the point that probably we were talking before about, you know, why do people do the wrong thing? And that's what came out of Impala. One of the reasons that we see so many accesses to personal information through an authorised system, we found that in Impala people were accessing confidential information because they were bored, literally, and I honestly think part of the reason is people that sit at a desk at a computer in a monitor and the same screen they access Google through, they actually access company records through. And they're forgetting that when you go through the portal and go through into a company record, the only time you should be doing that is to perform your job. You shouldn't be doing it because you saw your neighbour walk in the other day into the office. Oh I wonder what they were doing, wonder why they're here, and look up their name. That's not what, you know, your access is authorised for.

But I think honestly sometimes people forget. And it's about having that right culture and those conversations with your staff on a regular basis to go back to basics and get the setting and the tone right within your agency to make sure people understand that, you know, the computer in front of them with all that sensitive personal information is there for a single purpose, to do your job.

Jillian Whiting:

On that, privacy rules include that agencies must take reasonable steps to secure personal information. Agencies can assume, this means just technical or systems-based controls. Nicole what does reasonable steps mean in a privacy context and can you give some examples of what these look like on the ground?

Nicole Stephensen:

Yeah. I think that's a really good point. When we talk, particularly information security or issues of data breach, we are in that processes and controls mindset. We're already reacting right, we're being remedial. We're wanting to fix a problem. But reasonable steps are so much more than that and they sort of sit in three camps. So you've got your technical controls, which we've talked about, you've got, and your administrative controls, which are things like the policies and procedures, contract. And then you've got your physical controls. So that's things like locked doors and swipe card access on the ground.

Now, when I think of reasonable steps, if we're talking about say determining whether or not we're going to move to managed service provision to cloud based managed service provision for our data, the reasonable steps that I would be looking for are, has your procurement team been involved in ensuring that there are conditions within the contract with the chosen vendor that indicate that, privacy or binding in the case of Queensland to the rules in this State, that that has actually occurred within the contract.

And then the next step is, is there something also in the contract that requires or allows us to check right that those, that that vendor is doing what they say they will with the data, which probably includes personal information right in some form or other. So that's an administrative step that we can take. Now, that is a preventive and proactive measure as opposed to being reactive and remedial. Another thing that can be done is when we're moving our data from here to the cloud, isn't that a great opportunity to take another administrative step which is training and awareness, letting employees know that this migration is occurring, that there could be some vulnerabilities

relating to the data, and making sure that the culture of reporting, that the lines are open, if anyone sees anything at all that they think is a challenge or a worry, to report that to the correct person and make sure that that gap is plugged. So those are two administrative controls.

And then one of the physical controls would be while this migration is occurring, who's standing guard over the data? You know, if we're actually scanning for example paper files into an electronic environment and then uploading that to the cloud, who's standing guard over those paper files and making sure that when that scanning activity has ceased, that those documents are shredded and disposed of confidentially?

Jillian Whiting:

Would there be people sitting out there listening go, well that, yes but that's time and money really? It's slowing everything down.

Nicole Stephensen:

Oh it is time and money. But it's time and money well spent. The flip side to you know, say you don't want spend your $85,000 right now on making sure that your privacy and security environment is, you know, up to scratch. You will spend so much more money dealing with that data breach down the track. And in Government, there isn't that money to spend. In private sector, you could probably find your funding, pull it from somewhere else in your business if it's big enough. But in Government there isn't that money to spend and you're disappointing the community that you serve by having to spend it at all.

Jillian Whiting:

Is there, for the rest of the panel, anybody else, is that perception out there, time and money? There definitely is?

Troy Hunt:

Yeah definitely.

Jillian Whiting:

Yeah Troy.

Troy Hunt:

Yeah definitely. The irony of it is, is that post data breach, organisations will throw any amount of money at trying to solve the problem. And I know because they contact me and I'm like, I can't put the genie back in the bottle. It's like the time to do the training was yeah six months or six years ago probably. So unfortunately, it's something that you do need to be proactive with.

Jillian Whiting:

And keeping up I guess as we mentioned before, and you did touch on this before Troy, but do we need to collect this much data and how long should it be kept?

Troy Hunt:

I'll give you a really good example. There's a website called catforum.com, and it's exactly what you think it is. And when you sign up to catforum.com, they ask you for your date of birth. It's like what? Why? And it's optional. But I know from the number of data breaches I've processed the number of people that give it away. Like do you get an email or something with a cat photo on your date of birth? Like what's the point of having it? And it sort of comes back to this yeah what is the bare minimum that we need to do our job? Whether that's a principle of least privilege with access controls or whether that's what data do we need.

I think part of the problem too, and if I was to speculate about the likes of Optus, it is cheap to store data. It is cheap to keep it for perpetuity. But we've all probably seen graphs before of, you know, back in the 50s a hard disk needed to be shipped around in a 747. You know and now we've got more storage on your wrist. So storage is so cheap, but processing and purging data, particularly when you have to go back through incremental backups and things, is a harder problem. So organisations do take the easy route, which is really unfortunate.

Jillian Whiting:

So it's important to, it's reducing our tech service, service sorry.

Troy Hunt:

Yeah. There's a saying right and it's so simple, you cannot lose what you do not have.

Jillian Whiting:

Yeah. Alistair when a privacy breach occurs in an organisation, what are the red flags that indicate a serious issue for employers to address in your mind?

Alistair Ping:

The red flags?

Jillian Whiting:

Yeah.

Alistair Ping:

So the red flags are really about, as like leading up from some of the things you've discussed, self-regulation. So anything that's going to diminish your capacity to self-regulate, so if we're time-stressed, health-stressed, financial stress, anything like that, we're going to make quick decisions rather than actually working through the information. Any level of like bad blood that exists in an organisation, so people go.

Jillian Whiting:

Oh that doesn't happen, does it? Not really.

Alistair Ping:

So anything like that where somebody could be triggered to think, well, they deserve it because they did this, those sorts of things. And I was going to say the other thing that's really critical in this is to be able to empower staff with the skills to be able to call out breaches. So one of the key things we've looked at is bystander training. Because the weird thing that happens is that, often what'll happen is, and it's (ui) in research, is that the more people are actually watching something go on, the less likely somebody is going to do something about it. Okay.

So with data breaches, you know little things can get normalised. Everybody goes, oh yeah that's just the way things are done around here or it's not my responsibility. Somebody else should be doing it, blah, blah, blah. And nothing happens. And then down the track a massive thing happens like Optus and somebody turns around and say, oh we knew. We've known about that for years. And why didn't you do something about it? Because they haven't been trained in understanding what the process is. And secondly, that training to be able to call it out is really critical.

Jillian Whiting:

So what about ethics training in organisations? What are your thoughts on that?

Alistair Ping:

Ethics training is really interesting. But again, you've got to think about the context. So the context has shifted. So we're not living in this sort of stable linear society anymore. We're living in this very complex, dynamic, changing environment. And so, you know, you can do your ethics training with people where you say, okay, you know, the standard one, like what would you do in this situation? You know, a trolley is coming down, it's going to kill three people. You pull the lever, it's going to kill another one. What do you do? So you can do that sort of stuff and people go, oh yeah great.

But the reality is we want to train people to be aware of what happens in a dynamic environment. So how the theory breaks down in reality can be very different, and what the intervention points are. So the self-regulatory stuff, the organisational systems stuff, being aware of how easy it is to justify bad behaviour and bad decisions, unethical decisions. And the third thing is creating environments of psychological safety so that people can actually say, oh far out I've made a mistake here.

Jillian Whiting:

Anyone else in the panel have thoughts on ethics training? No.

Nicole Stephensen:

I'm all for training in any way that empowers staff right. Anyone, to empower in an organisation to make better decisions. Sometimes ethic training isn't necessarily the training that we need in these circumstances. Maybe it's training about how applying the privacy rules and security controls can empower that person to make better decisions within their organisational context. Keeping it smaller. Whereas ethics is about am I a good person? Am I making good choices? Where privacy training is am I applying principles that are set out in privacy law to make good decisions about personal information handling. And I think that kind of training is probably more useful in this circumstance.

Alistair Ping:

Yep.

Nicole Stephensen:

It also helps employees very quickly trigger what's my issue here? What, you know at what point have I gone wrong? And that's because the privacy principles that we have certainly in Queensland and Australia, they give us almost like a scaffolding or a type of ladder that you have to actually approach the first rung before you can approach the second rung in terms of decision-making. So to Troy's point about collection limitation right, in the privacy rules, the first principle is around purpose specification. So it's, no what personal information you need to do your job. And then the second one is, limit your collection of personal information only to that.

Jillian Whiting:

To that.

Nicole Stephensen:

And it flows like that. And again to Troy's point, if you don't collect it, you don't have to secure it for its life cycle.

Jillian Whiting:

Let's talk about legislation. And Paxton you mentioned obviously the mandatory data breach notification scheme. Can you talk more about that? Why is it important and what are the challenges that we're currently facing?

Paxton Booth:

Look in Queensland, we currently don't have a mandatory data breach scheme, as everyone I'm sure in the room's aware. We've got a voluntary scheme. People, agencies can report privacy breaches to our office. But we only receive about four a year, which is quite low when you look at it compared to other agencies, particularly the Office of the Australian Information Commissioner, get hundreds a year.

And it's important because when people's personal information is breached, it's critical that they're made aware of it so they can act. I think one of the challenges we spoke earlier in the panel about, you know, how personal information breaches can impact individuals and it's a really individualised thing. How a privacy breach will impact me versus Troy versus the other panel members will vary and people in the audience. You know, if someone found out my address tomorrow, probably (ui) the end of the world, depending what their intentions were. If I'm a victim of crime or a victim of domestic violence and my address gets made public, that's a really big impact on that person. They might have just moved. They might have just settled their kids into a new school, just found a new job, and all of a sudden they're at risk and they don't really know necessarily how big a risk they face. They might have to pick up and move and start again.

So the importance of the mandatory data breaching is about empowering and giving people information to act if their privacy's been breached, so that they're the best placed person to actually make an assessment of the risks to their situation, whether it's their address, their financial information, their medical history. How that will impact on different individuals will vary, and by giving them the information and knowledge that their privacy's been breached, they can take a reasonable response. But I think in that sense, it's also incumbent on the agency to help them when it's been breached, to tell them as much information as they can about the nature of the breach, what's been disclosed and importantly, perhaps even what hasn't been disclosed.

I think often some of the conversation around, particularly when I saw the Optus breach, was people asking questions, you know, was my Medicare number exposed? Was it my passport? Was it my driver's licence? If you're anyone like me, like I was caught up in the Optus breach. Like I joined them 20 years ago. How did I identify myself? Was it my password? Was it my passport? Was it my driver's licence? So telling people what's actually been breached and what hasn't been breached is important too.

Jillian Whiting:

Is it problematic with, you know, that self-reporting that organisations have to decide what serious harm is?

Paxton Booth:

And I think that's a question we're probably going to get a lot when we commence the scheme in Queensland, what is serious harm, and what we really want to see is agencies develop a methodology around that to make that assessment themselves. But you know, importantly, and as I said before, I think it's a relatively low bar in the sense that it's hard to understand how it's going to impact an individual. So if it's someone's personal information that puts them at risk, you kind of need to assume almost that, yeah, there is a risk there for that person and we probably should let

them know to make the decision themselves about what they need to take, what action that they need to take.

Jillian Whiting:

Panel, anyone else have thoughts on what makes an eligible data breach reportable?

Troy Hunt:

Anything. I find it honestly like very frustrating that we have a circumstance here where organisations can self-assess after, on their watch, personal data has been exposed and they get to make the decision. I mean let's say it's a catforum, you know, and you go, I'm running cat forum. I don't think anyone's going to suffer serious harm because their catforum account's been breached. Well, all right, there's your date of birth. (ui) authentication. Also, the usernames and passwords of your 1 million customers are the same that they've used on every other site on the internet.

So you might be talking about cats over here, but someone's doing their banking and suddenly they've lost their Bitcoin right there. Just it feels very out of sync with modern privacy thinking, particularly as compared to other parts of the world.

Jillian Whiting:

Alistair do you have thoughts on that?

Alistair Ping:

I just, I was thinking as you're talking that there's also bias there because, see you have, we have this bias where we think we're more ethical than other people. So again, the organisation, so what was it? Cat?

Troy Hunt:

Catforum

Jillian Whiting:

Catforum

Alistair Ping:

Yeah anyway. They're probably thinking well I would never do anything like that, so I don't need to worry about that. So they have bias where they don't even see the issue in the first place. Sorry perceptual blindness where you don't even see the issue in the first place. And that's part of the problem. And what you're suggesting is, actually make the blanket rule of like every breach is an

issue, like every breach should be discussed, like not actually leaving it up to an organisation to make that decision.

Jillian Whiting:

Is that actually possible, every breach? We would be just reporting constantly, wouldn't we?

Troy Hunt:

I don't think it's quite that bad.

Alistair Ping:

Hope not.

Troy Hunt:

But if we look at the barriers to reporting, so why are organisations not reporting? They're worried about things like reputational damage. But if you do look at an organisation like, the Australian Red Cross Blood Service has been put up as the poster child of data breach disclosure, because they did such a wonderful job of it. But there's so many organisations where they have a data breach which becomes public either by their own free reporting or because it gets out, one way or the other, by someone's website. And you get the masses turn around and go, I'm going to sue you because you lost my username and password.

I had someone contact me the other days, he's getting legal letters from a German law firm. This is someone based in the EU. Because they had a data breach. They reported it. They were public about it. And it was things like email addresses and passwords. And someone says, now he gets all these phishing emails. Can I have money please? So I understand the reticence of organisations when it's so easy, particularly with class actions, there's so many class actions that happen after data breaches where it's near impossible to trace back any harm to the original source being that breach, because everyone's in so many data breaches now, that I guess I'm just a bit sympathetic to organisations worrying about protecting their customers and their shareholders as well.

Jillian Whiting:

When news of the Optus breach and the Medibank breach and that was, my background is news, so the, watching the news coverage is, oh what's, this is the end of the world. But I feel, you tell me you're the experts, is, are we going to, is that going to be just, oh another breach, here we go again kind of thing? Or are we going to see more and is the public going to be, I don't know, expect it more and not panic as much? And should they be? Nicole?

Nicole Stephensen:

I think we can expect a bit of breach complacency at some point. It has, it, it's tiresome in the news cycle as well as you know a dinner table conversation to be talking about you know all of the problems with the world and all of the risks to ourselves just by engaging in society. So if that's the case, we need to think about a new way dealing with the, you know data breach preparedness, for example, within our organisations. And also communicating risk with the community that we serve so that they are more empowered in their day-to-day decision-making. So often in my work I get asked about you know services and platforms that are being proposed, whether it's by Government or by organisations. And I ask them always to reflect on the community that they serve and what is the risk profile of this community? And how are we building that into whatever the service or platform or solution is that we (ui)?

Because we can actually create a culture, not just within, the building of the technology, but we can also create a culture around that technology that is intended to service the community. So do we need to put out communications or supporting material on our website about, this is our new service offering. This is the information we're going to ask for from you. And these are the risks to you. So use this information as part of making your decision about whether or not to engage with us. Now from a money-making perspective, this is a different way of thinking for our organisations. But for Government, I would say that we almost have an obligation to do it this way. We have a positive duty to ensure that whatever it is that we do, whatever we build, whatever we deploy, is done with the community that we serve in mind.

Jillian Whiting:

This is a bit leftfield, but my daughter's at school. She's made a representative team. And, you know, you get all the forms to fill out. I was like, honestly, how many forms I've got to fill out? And the last one was with privacy. Some of this information you've filled in will be kept on servers in another country. So you know the risks of the information you've provided. Now, I'm thinking I shouldn't have signed it. I don't know if I made a mistake. I've not seen that level before. But obviously, is that what we're talking about? More transparency about what's being done with my information.

Nicole Stephensen:

I think transparency, you've got to remember though, transparency's different from consent.

Jillian Whiting:

Yes.

Nicole Stephensen:

And often times what we see with this forms-based culture or clicking yes to terms and conditions is we're being told that that's an agreement between us and the service provider. But it's not actually an agreement. It's a term of entry. I don't have a choice. I need to provide my information in order to receive what it is I want to receive. That's not made clear enough. People are treated as though

they are agreeing to something. So then when the privacy problems start or there's a data breach, you hear all this communication and rhetoric to the community that, oh it's actually your fault. You knew the risks. Now our job as organisations and as Governments is to remove as much of that risk as possible to the community before we ask them for their information, and then take the steps, take the controls as we go to make sure it that stays that way.

Jillian Whiting:

Alistair have you got anything to add on that?

Alistair Ping:

Yeah, I think that's a really good point. And the other thing there is, and coming back to your point, was how do you measure it? Like how do we know? Because, again, it's one of these things where it can't be a set and forget type of solution. It needs to be something that dynamically changes and shifts according to societal expectations, obviously, in technology type changes and things like that. And yeah, and the bad thing about it is often those little clauses that you talked about, they're in the tiny little fine print at the bottom.

Jillian Whiting:

It was a full page.

Alistair Ping:

Oh full page.

Jillian Whiting:

It freaked me out completely. Yeah.

Alistair Ping:

Yeah right. But you signed it because see expediency. I haven't got time to do this, so I'll just sign it.

Jillian Whiting:

Yeah.

Alistair Ping:

And.

Nicole Stephensen:

(ui) consent.

Jillian Whiting:

Well yeah that was it yeah.

Nicole Stephensen:

(ui) your child can, yeah in your enrolment pack for school, no your child can't attend sports, go to sporting events, go to the cafeteria at lunch time, play in the playground or attend an (ui) unless you sign saying that you're happy for your child's image to be included in our social media feeds. And I think that that's atrocious. You know from a policy perspective, it's atrocious.

Jillian Whiting:

I'm glad you said that because that was my thoughts.

Nicole Stephensen:

Yeah. There are many ways of getting around this. But we see it's constantly in the media. And privacy professionals are constantly being asked, is this okay? Is this (ui)? The way schools are going about it, no it's not because they're using consent as the vehicle to tell you what (ui) is.

Alistair Ping:

And the justification would be, everybody else is doing it. What's your problem?

Nicole Stephensen:

Yeah that's right.

Alistair Ping:

It doesn't make it right.

Jillian Whiting:

Troy do you have any thoughts on that?

Troy Hunt:

I think the, to your point about the country thing is sort of interesting. And I guess in times gone by where things existed in physical form in a location, it was probably a different situation to now when, okay which country is it in? But it's in the cloud. And who is managing the cloud? And also, if it's a data breach, it really doesn't matter where you are because a lot of this stuff is externally facing. So whether, let's say it's in Microsoft's infrastructure here in Brisbane or if it's in Microsoft's infrastructure in Seattle or pick any other part of the world, the administration, the access to it, the security vulnerabilities, there are no borders. And I think it's very interesting that we sort of keep coming back to the necessity of local laws and regulations. But every time we talk about people violating them, it is spread out without borders. So for me, I'm probably less worried about where my data sits. I'm more worried about how it's managed.

Jillian Whiting:

So with that form, it was a third, an unnamed country, which again thought, well, maybe this country is not as good with data that Australia is. And on that point Paxton how is Australia going, generally speaking, not putting you under any pressure at all?

Paxton Booth:

Oh look we're evolving. And I think that's the thing with privacy is that it's constantly evolving because the way we interact with technology, the type of technology that's coming out, it's changing all the time. So as we've said so many times on the panel already, nothing's static, it's always dynamic. So yeah I think what's generally regarded as kind of the gold plate standard is you know coming from the EU, GDPRs. But I think they've come from a very different background in terms of their social development and the history to us in Australia in terms of how we've sort of seen and grown with privacy and breaches of privacy in Australia.

So I think we're starting to see the importance of maintaining our privacy a little bit more in Australia and we're growing with our, I suppose, sensitivities to people collecting our information when they don't necessarily need to. So we're improving. There's always room for growth and improvements. I'd like to see us continue to grow along that path.

Jillian Whiting:

Okay. I'd just like to move to final thoughts from everyone in the panel, on the panel. Given the theme back to basics, what's your key message? Starting with you Nicole. Organisations, Government, whoever it may be, what are your thoughts on privacy?

Nicole Stephensen:

So I think it's really important. A number of you have (ui) for a long, long time. So I appreciate you listening again. I think it's really important not to conflate privacy and security when we're talking about the appropriate management of personal information through its life cycle. So information security broadly is the fence that we put around that which we wish to protect. Privacy is personal

information management in accordance with privacy principles. And the personal information, if we're thinking of a security context is one of the things within that fenced area. Right. It's not the only thing. So we need to remember the protection of personal information has a particular security function or a particular security imperative. But we can't see privacy and security as the same.

So when we talk data breach and we're talking about unauthorised access, disclosure or loss of personal information, we cannot just focus on the security controls or the remediations that are security related to address that problem. We need to be focusing on, why in our organisational context we had all that information in the first place? Did we collect only what we need for our purpose? Do we have adequate data retention and destruction processes in place? Are our staff well trained? Do we have a good culture of reporting? All of those things have nothing to do with information security.

So I think it's just really important that we keep our focus where it needs to be, which is on taking care of the stuff about you and about me, and remembering that it's part of a good decision-making process. It's not just a suite of controls.

Jillian Whiting:

Alistair final thoughts from you.

Alistair Ping:

Yeah I think that's a good point. And I think I would want to link, I think that's right, disconnect privacy with security, because obviously that's the corporate view. But to link privacy with respect for others…

Nicole Stephensen:

Yes.

Alistair Ping:

… that's the individual bit. And that's where we get back to the values and about whether or not, you know, we can justify the decisions using those sorts of values rather than those flawed justifications mentioned before. And I suppose the other thing there is just to be really aware of how easy it is for all of us to make these little dumb decisions that end up being major breaches and just to slow everything down and as I said, be much more intentional about what we're trying to do and think about, as I said, the intention about respecting and caring for others in our community.

Jillian Whiting:

Have that thought, do I need this?

Alistair Ping:

Yeah.

Jillian Whiting:

What's going to happen if I proceed with this?

Alistair Ping:

Yeah.

Jillian Whiting:

Troy some final thoughts from you, back to basics.

Troy Hunt:

Yeah. Well I think as Alistair said in terms of being very easy to make the dumb little decisions, it's also very easy for us to make good privacy-centric design decisions from the outset. Deciding not to collect certain classes of data is a really good thing. Designing retention policies is a good thing. Most of the incidents we see here, like I sort of joked at the beginning, they're all due to human error somewhere. And a lot of this we can really reduce the impact of either as organisations or even as individuals when we do go to that you know catforum or whatever it may be, and there's a sea of information they ask you for thinking about what is actually necessary.

And I guess to round that out with some balance, again, unfortunately we're in a situation where if you want a phone plan, you're going to need to identify yourself. If you want health care, you've got to give your sort of medical history. So there's a limit to what we can do. But I feel like we're well beneath there as a broader society.

Jillian Whiting:

And final words to you Paxton as the Commissioner, your thoughts on what's been raised on the panel today, the theme of back to basics and Privacy Awareness Week in general.

Paxton Booth:

Look what I'd love to see people do following this panel discussion today is go back to your offices or if you're sitting online, block out 15 or 20 minutes in your diary in Outlook or whatever you use in your calendar and spend it just to have a look at, what are your privacy settings? What passwords are you using? Have I got strong passwords against all the sites that I'm using or pass phrases? Are there places where I can use multi-factor authentication to improve my privacy resilience? Have I had a conversation with my staff recently about the importance of privacy? If people can just block out, you know, 15 minutes today and maybe in a few months' time again, go back to basics and think

about what are my privacy settings? We've said so many times in the panel today, we rush through life. We see that, you know, the tick a box, come up. You know, you accept the privacy conditions and you click yes before you read it. Go back and just have a little bit of time spent today to reflect on your privacy settings and where you can kind of minimise the information you're sharing and have a conversation with the staff and the people you work with about the importance of privacy, and how you can save your agency literally millions of dollars by not clicking on that phishing email.

Jillian Whiting:

And what else have you got this week? What can we expect Privacy Awareness Week to deliver for us?

Paxton Booth:

Lots on this week if you're interested in more presentations. There are lots on. I'm on two other panels tomorrow down in Sydney. One of them's being broadcasted, one being run by the Office of the Victorian Information Commissioner as well. You can see that online. And there are other events as well being run by other agencies. Have a look Privacy Awareness Week in Google. And one of the other things that collects (ui) data. But yeah, have a look and join in some of the other discussions and forums. But take some time today if you can to think about privacy and how it impacts you.

Jillian Whiting:

Thank you so much. If you could please put your hands together for our panel, Paxton Booth, Troy Hunt, Dr Alastair Ping and Ms Nicole Stephenson. Thank you so much. Thank you to everyone on the livestream who stayed with us. Thank you to all of you who have made the effort to come in today. I hope you've got something out of that. I'm sure you have. I clearly have. It's a fascinating issue. So enjoy Privacy Awareness Week. All the best. And thanks for being here.