PRIVACY AWARENESS WEEK 2018

TRANSCRIPT OF LAUNCH EVENT
14 MAY 2018

Speakers:

Mr Philip Green, Privacy Commissioner Queensland.
Hon. Yvette D'Ath MP, Attorney General and Minister for Justice.
Professor David Lacey, University of the Sunshine Coast and IDCARE.
Mr Paul McCarney, Chief Executive Officer of Data Republic.

MR PHILIP GREEN:

We'll make a start, good morning everyone welcome to PAW 2018! It's great to have you all here to 1 William Street, it's a fantastic facility. Firstly I would like to respectfully acknowledge the Traditional Owners of the land upon which we are meeting today and holding this event, and pay respect to the elders past, present and emerging.

I'd like to take a moment to acknowledge some special guests today of course we're delighted to have the Attorney-General and Minister for Justice the Honourable Yvette D'Ath with us again, third year in a row and it's really fantastic you support our event like this, it really shows the importance that you place on good information and practices in government and its fantastic to have you here again, thank you. The Information Commissioner, sitting right next to you Rachael Rangihaeata, great to have you here again, usually you're up here doing the first introduction and welcome. Deputy Commissioner Steve Gollschewski, representing Ian Stewart and the Chief Information Officer Alan Mills is here too so showing some of the security and technology side and how we work together in the information management space and great to have so many practitioners here, I know there's some fantastic private sector and public practitioners in the area of privacy, really fantastic to see you here and hopefully we'll see some of you at the community event on Wednesday, which is on digital defence run by CryptoAustralia and I think that's aimed at the community but there's a lot of tricks that a lot of us could learn from those people.

Excuse me, I have a bit of a scratchy throat, so bear with me. Privacy Awareness Week this year, the theme is value your personal data - it's worth protecting. I think it's a good timely reminder, on the theme there is a few themes running across the world in the Asia-Pacific realm from compliance to culture is another one of the sub themes, the Federal Government is running with that and also from principles to practice, some good things to remember. As we mature in our information management and our privacy awareness the importance, the critical importance, to get beyond just compliance culture and a tick box culture, we'll see that I believe with the introduction of GDPR, it's been quite the year in privacy in Australia nationally, and even internationally. The introduction of Mandatory Data Breach which has had repercussions rippling across all jurisdictions, GDPR coming in on May 25th is going to ripple across the world and you will have already seen privacy notices being amended, and many of you with social media accounts and any big interaction with any big international companies these days is going to get you involved in the GDPR in some way and there's

notices – and there's some good and some bad and some ugly, that have come out that I've seen and there's been a few quite exceptional ones to simplify that law and its introduction.

I might not stand in the way of our speakers today, we've got a fantastic line up and I'm going to hand over to the Attorney-General to open the event officially, unfortunately she's got cabinet duties later on, she'll have to leave a little bit early but I'm sure she'll be here in spirit so thank you and I'll hand over to the Attorney to open.

THE HON YVETTE D'ATH MP:

Thank you very much Philip for that introduction and can I start by acknowledging the traditional owners and custodians of the land on which we hold this event today and pay my respects to the elders past, present and emerging. I'd also like to acknowledge the event speakers today, Professor David Lacey and Mr Paul McCarney, Privacy Commissioner Philip Green, Information Commissioner Rachael Rangihaeata, the Acting Right to Information Commissioner Miss Louisa Lynch and also welcome Deputy Commissioner Steve Gollschewski which I'm sure I pronounced that wrong Steve, I apologise from the Queensland Police Service. I'd like to also thank the Privacy Commissioner and the Information Commissioner for the opportunity to attend and speak at this year's Privacy Awareness Week Launch and to officially launch it for 2018.

It is timely given the recent Facebook Cambridge Analytica Data Scandal that the theme of this year's Privacy Awareness Week is value personal data, it's worth protecting. Just as companies and governments need to be transparent and accountable and collecting and handling people's personal information, individuals need to be aware of their privacy rights and obligations. People should feel comfortable asking companies and government agencies why do you need my personal information and why do you need so much of my personal information. Individuals should take an interest in knowing just what they are consenting to when they tick the box agreeing to a company or an agency's terms and conditions including whether they might be consenting to that company or agency sharing their personal information with third parties. The truth is that most of us transact with companies or government agencies on a daily basis and most of us do not usually read the organisation's privacy policy or fine print.

I encourage people to read privacy policies and become aware of what privacy legislation provides and to know how it protects our personal information. Websites for the Australian Information Privacy Commissioner and Queensland's Information Commissioner are a great

starting point for this. So what do we mean by the term personal information? We know the Information Privacy Act 2009 applies to Queensland government agencies and defines personal information as information or an opinion including information forming part of a database whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. A similar broad definition is included in the Commonwealth Privacy Act 1988 which applies to Commonwealth government agencies and companies with an annual turnover of $3 million or more and some other organisations. Queensland's office of the Information Commissioner provides a useful guideline in which information is personal information for the Right to Information Act or the Information Privacy Act. Examples are a person's name, address, phone number or email address. A person's photograph, CCTV footage recording a person, a person's medical details and a person's fingerprints. Most of us would like to think that our personal information including our web search history, information in our social media accounts and information about our exercise and sleep patterns whether or not we choose to measure these with a health or fitness device or app, is information about private matters to be protected from others and the world at large.

Clearly there are businesses inside and outside of Australia that are motivated to gain access to this kind of information. Some commentators have asked whether privacy continues to be relevant in the digital age and those who have heard me speak before say there is a real challenge in better educating the community that while they talk about breaches of privacy and their concerns about release of private information they themselves will release an extraordinary amount of personal information in their social media accounts every single day without realising it. Not just of themselves but of their children and where they go to school and their children's names and their ages and details of their dates of birth.

I'd like to say that not only is privacy relevant in the digital age but it is even more relevant now than it was in the past. I'd ask governments, organisations and individuals to value privacy and people's personal information instead of merely viewing it as a commodity. Importantly organisations and governments must ensure that personal information is collected and handled transparently, securely and fairly in accordance with established privacy principles.

It is clear from the Office of the Australian Information Commissioners, Australian Community Attitudes to Privacy Survey in 2017 that privacy is important to Australians. The survey shows that Australians are increasingly concerned about their privacy and the privacy risks posed by new technology. The 2017 survey showed that 69% of Australians are more

concerned about their online privacy than they were five years ago. Australians will avoid dealing with organisations if they are concerned about their privacy. With 60% of respondents saying they would avoid dealing with a company out of privacy concerns. Even before the Facebook Cambridge Analytica Data scandal, social media was causing privacy concerns for Australians. The survey showed that a portion of people who regretted putting information on social networking sites increased from 17% in 2013 to 25% in 2017. This is likely to be associated with an increase in people viewing social networking as a public activity and a decrease in people viewing it as a private activity. The survey shows Australians believe that the biggest privacy risks facing the community are online services including social media sites, followed by ID fraud security breaches then data security breaches and risks to financial data. The results indicate that Australians are increasingly concerned with dealing with organisations online and that they have low levels of trust in social media organisations. Unfortunately our concerns don't necessarily translate to us taking reasonable steps to protect our own personal information.

The survey showed that over three in five Australians do not regularly read the online privacy policies. About half of us do not regularly shred documents, half of us do not clear our browsing histories and nearly half of us do not regularly adjust the privacy settings on our social media accounts. Interestingly around a quarter of Australians have rarely or never asked an organisation why they need our personal information. And nearly 60% of Australians don't know that we can request access to the personal information a business or government agency holds about us. I do not take these statistics to mean that Australians take their privacy for granted or that their privacy is redundant in the modern era. I see this as an opportunity for Australians and Queenslanders in particular to be made aware of their privacy rights. As Queensland's Attorney General I couldn't help but take particular note of the sobering survey results relating to government agencies. Only 60% of people say that State and Commonwealth governments are either trustworthy or somewhat trustworthy in how they protect or use their personal information. One in six people will not deal with a government agency out of privacy concerns. Less than half of Australians are comfortable with a government agency using their personal information for research or policy-making purposes and 40% are not comfortable with these uses. Only one third are comfortable with the government sharing their personal information with other government agencies and can I say how critical this actually is. This is one of the major barriers for good reform across a range of sectors in this state whether it's youth justice, whether it's child safety, mental health, homelessness. If you cannot share information across agencies and bring agencies together to look at these issues you cannot address them. For too long we have heard

organisations and stakeholders and individuals complaining about government agencies working in silos and not sharing information.

So if the Police and Youth Justice and Child Safety and Mental Health and Housing cannot talk to each other how on earth do we think we're actually going to make a real difference. How are we going to have whole of government reforms, domestic and family violence is another key area. So how do we have that information sharing at the same time as ensuring that we are protecting the privacy of that data but importantly giving the public the confidence to allow us to share that information and to have confidence in that sharing. As Queensland Attorney General I hope that this Privacy Awareness Week gives people in the Queensland community an opportunity to better understand their privacy rights.

I know many of you all know this but I would like to just briefly touch on the privacy framework in Australia and in Queensland. The Privacy Act 1988 applies generally to Commonwealth government agencies and other organisations in Australia including those with an annual turnover of over 3 million. The Australian privacy principles or the APPS regulate how these entities, referred to collectively as the APP entities collect and handle individuals personal information with a higher level of privacy protection for individuals sensitive information including information about health, racial or ethnic origin, religious beliefs and criminal records. The APPS took effect in 2014 and replaced the information privacy principles which applied to Commonwealth government agencies and the National privacy principles which applied to the private sector and health agencies. This followed the recommendations of the Australian Law Reform Commission in its 2008 report, for your information Australian privacy law and practice. The APPS are designed to ensure the open transparent, fair and lawful collection of personal information of individuals by APP entities. The APPS regulate how personal information is used or disclosed and require entities to keep personal information accurate, up-to-date, complete, secure and available on request of the individual. The Commonwealth Privacy Amendment Notifiable Data Breaches Act 2017 took effect on the 22nd of February 2018 introducing a scheme for notification of eligible data breaches. Entities covered by the Privacy Act including APP entities are required to notify the Australian Information Commissioner and affected individuals of data breaches likely to result in serious harm. These new provisions build on the privacy protections set out in the APPS and enhanced transparency on the part of businesses and the Commonwealth public sector and it was only in the past couple of weeks that we heard about that serious breach out of the Banking Royal Commission in relation to millions of individuals information being released, or lost.

The Queensland Information Privacy Act 2009 regulates how Queensland public sector agencies collect and handle personal information. Chapter 3 of the Information Privacy Act provides for an individual's right of access to documents of an agency or minister to the extent they contain the individual's personal information. Chapter 3 also gives an individual right to amend information that is inaccurate, incomplete, out of date or misleading. The Information Privacy Act sets out the National privacy principles which apply to health agencies and the information privacy principles or the IPPS which apply to all other Queensland public sector agencies. The NPPS like the APPS afford a high level of privacy protection to sensitive information and allow an individual to deal with the health agency anonymously or by pseudonym. Similar to the APPS, the IPPS and the NPPS require personal information to be collected in a way which is fair and lawful. Personal information is to be used for the purpose for which the information was collected except with consent to unlimited circumstances. Personal information must be kept secure and is to be made available on request of the individual and may only be disclosed in limited circumstances. An agency is to take reasonable steps to ensure personal information is accurate, relevant, complete, up-to-date and not misleading. In October 2017 I tabled a report on the review of the Right to Information Act 2009 and the Information Privacy Act 2009 which was the result of extensive consultation and policy analysis and I thank those in the room who contributed towards that consultation.

One of the report's recommendations was for the government to carry out a cost benefit analysis of moving to a single set of privacy principles in Queensland based on the APPS and a data breach notification scheme similar to that in the Commonwealth Privacy Act. This analysis will likely be undertaken later in this term of government. As Queensland Attorney General I received correspondence from members of the community who were concerned about the use of surveillance devices in a range of context. This includes employers using surveillance devices to record people's activities at work, and people visually recording their neighbours with CCTV cameras. With the proliferation of smart phones and the increasing availability of drones fitted with cameras, people in the community understand and expect an appropriate response by governments to ensure their privacy is protected.

The current Commonwealth and Queensland regulatory framework may cover some surveillance activities but most are subject to privacy or other laws rather than surveillance legislation. For instance an employer, that is an APP entity must ensure that it collects personal information of an employee or any other person including from a surveillance device in accordance with the APPS. Similarly Queensland public sector agencies must ensure that

they collect, store, use or disclose personal information of an employee or any other person obtained from any surveillance devices in accordance with the Information Privacy Act. Queensland's Invasion of Privacy Act 1971 provides offences relating to the use of listening devices including optical surveillance devices which are capable of recording conversations however the Invasion of Privacy Act includes a number of permissible exceptions to these offences including where the person using the listening device is party to the conversation. There are circumstances where the visual recording of a person without their consent and sharing of a visual recording may amount to a criminal offence under the criminal code. Section 227(a) of the criminal code makes it an offence to observe or visually record a person in circumstances where a reasonable adult would expect to be afforded privacy without their consent, such as the toilet or a change area. Section 227(b) provides an offence for distributing a prohibited visual recording of another person without the other person's consent. And a person aggrieved by the use of a surveillance device such as a neighbour pointing a CCTV camera directly into their property may be able to seek relief through common-law actions in nuisance or trespass. This is likely to be seen as unsatisfactory and expensive legal avenue by most people.

I don't need to remind anyone here how important it is that the law is always kept up-to-date and able to address problematic behaviour, whatever technology is involved. There are two significant areas where this government is making a significant contribution in this space. First is in relation to an authorised sharing of intimate images. The Queensland government takes a zero tolerance approach to all forms of bullying including cyber bullying. The honourable Anastacia Palaszczuk, the Premier, and Minister for Trade has initiated a national conversation on bullying and the Queensland government has committed to a new suite of actions to tackle this serious issue. This work commenced with the stakeholder round table held on the 29th of January this year and includes actions such as establishing a dedicated Queensland anti-bullying task force to inform the development of a new anti-bullying framework for Queensland. A Youth Advisory Council with a focus on issues including cyber bullying and a public awareness campaign. Both the Queensland and Commonwealth criminal code contain a range of offences to combat physical and online bullying while commonly referred to as revenge porn the non-consensual distribution of intimate images is a form of cyber bullying and technology facilitated abuse that extends beyond the breakdown of a relationship. While the sharing of intimate images can affect anyone, this conduct disproportionately affects women and young girls. The distribution of intimate images can be humiliating and distressing those depicted regardless of how an image was created or obtained or the motivation for sharing an image.

Threats to distribute intimate images can cause enormous anxiety and in some instances can be used to control or coerce a threatened person and we're seeing this in the domestic and family violence space. This government is committed to creating new criminal offence that targets the non-consensual sharing of intimate images, importantly the offence will extend to threats to distribute intimate images without consent in circumstances where the material may not exist recognising the distress that such a threat can cause. Work is underway developing amendments to implement this election commitment and introducing these new offences will ensure that people who engage in this harmful conduct are held accountable and will reflect a community's condemnation of such activity. These laws will complement civil remedies that are available in the community as well as education and awareness raising schemes.

You may be aware that the Commonwealth Parliament is currently considering and enhancing Online Safety Non-Consensual Sharing of Internet Images Bill 2017. If passed, this bill will establish a national civil penalty scheme designed to deter and penalise individuals and content hosts who share intimate images without consent and provide extended enforcement powers to the e-Safety Commissioner including the power to issue takedown notices providing for the quick removal of offending content. The second area which may lead to a form is in relation to surveillance legislation. You may be aware that in August last year the government released a consultation paper about Queensland drone strategy. The consultation paper noted the potential privacy concerns and the community arising from the use of drones, stating drones have the capacity to travel relatively unnoticed into private property and record live images and sounds. This poses a privacy risk as drones may be used to monitor, record or disclose individuals private activities without their consent. The drone strategy will provide a whole of government strategic vision about the use of drones with a broad focus on attracting investment, industry development, research and development, service delivery improvement and enhancing the lives of Queenslanders. The drone strategy will recognise the current privacy regime is highly complex and that some of Queensland's laws are outdated. In the Northern Territory and all other states, other than Tasmania, surveillance device legislation regulates optical surveillance devices, listening devices and tracking devices. Some jurisdictions also regulate data surveillance devices. New South Wales, the ACT and Victoria also regulate workplace surveillance. Work on issues arising from the drone strategy consultation paper is ongoing with an announcement coming on what further action will be taken.

I raise these issues because it is important to realise when we talk about privacy it's not just about the data, it's not just about your personal contact details that we are talking about. Privacy can form many many different areas and when we talk about those images, we've had issues with CCTV cameras in public areas that are overseen by councils that the community want, they want these things in the community, that makes them feel safer. But when they find out that those images are also potentially picking up audio and private conversations they start saying but is this needed, why are we doing this. And those questions, and those discussions have to be had and that's why Privacy Awareness Week is so important but we need to be having that discussion year round.

To end I would like to say that privacy is an issue that this government takes very seriously. Privacy Awareness Week is a great opportunity for us to reflect on what we can do as a government and as individuals to ensure it is protected and valued. This is not easy and Rachael and I were discussing this before we started this morning. There is always in the view of the public, in the view of the media this tension between information sharing and privacy but there doesn't have to be that tension. It's about balance. And we have to make those decisions every day and the more we have that public discussion and lift that awareness the better the public, the media understand the importance of that balance and why we need to get it right. So thank you once again for the opportunity to attend and speak at this year's Privacy Awareness Week and it is my absolute pleasure to launch Privacy Awareness Week 2018 and I hope that you get a lot out of the speakers that have been organised for this event that is going beyond a week and turning into almost Privacy Awareness Month now. But thank you once again for all of the organisers who have put this event on, it is an important discussion that we need to be having and I thank everyone who is in this room today and being part of that discussion and helping with awareness in our community. Thank you.

PROFESSOR DAVID LACEY:

Good morning everyone, it's good to be with you on Privacy Awareness Week. As Phil mentioned IDCARE by way of context is a not-for-profit charity. It's based on the Sunshine Coast and we are responsible for providing front-line support to 28 million people. So the population of Australia and New Zealand. So we have a small but very expert and capable team where we've got a bunch of organisations that help keep the lights on and one in particular, the University of the Sunshine Coast, my university has been an absolute supporter and backer of our work on behalf of the community and I thank them for that. Privacy Awareness Week gives us an opportunity to lift the lid on what we're seeing in terms

of impacting the Australian community and so throughout the course of this week each day we'll be releasing reports on each state and territory in terms of what residents are experiencing by way of the compromise of their personal information. What it's meant for them in their journey and maybe some lessons that we can learn about where to from here. So today is all about Queensland. We had over 9000 engagements from across the state last calendar year. The Aftermarth report is available on idcare.org on our homepage and so I'm going to just briefly take you through some of the key findings of that report today.

So our approach at IDCARE for those that aren't familiar with it, we are principally there to provide relief and benevolent support to members of the community for free. We can do that in an anonymous way, we don't need to know who they are or for those that are struggling for example and in their engagement with organisations or with law enforcement we give them the opportunity to maybe tell us a little bit more about who they are so that we can advocate on their behalf. Our staff are counsellors, so they're professionals and we train them up in identity and cyber security as opposed to trained technologists to be behaviourists, not casting any aspersions on the ability of technologists in the room. And the key strategies they employ are principally to listen which for a lot of people in the community that's the first time that that's happened, listen and understand what their needs and concerns are. And those needs and concerns are pretty diverse. And to look at how we can identify what the risks are, the situation they're dealt with and work with them to develop a tailored response plan and where possible advocate or navigate on their behalf because the roads a pretty complex one as you'll see in a moment.

So the Queenslanders that have experienced the compromise of their identity information and at times its misuse, around one in 1000 Queenslanders 15 years and over engaged our service last year so that's a pretty strong representative sample I think of the community. We're often, when we give the community presentations people say well it's the elderly and it's the youth who are most at risk and we don't see that. We see the most common represented age group across the country, not just Queensland are 25 to 44-year-olds. Part of the reason why that's the case is they're the major transactors in the economy so they're the ones who are jumping online and getting involved in transactions and sharing personal information and really engaging in the use and trade at times of their personal information. And our hours of operation we can only afford to be open from 8 am to 5 pm Monday to Friday so most of those cohorts are working. So if we were to extend our business operations we'd probably see that cohort growth further.

It's a big investment that we make, most of our staff volunteer. They're volunteers. And we contribute hours and hours of counselling and not just one, one off counselling but multiple engagements online and over the phone and that's a picture of Chrissy one of our fabulous identity and cyber security counsellors there on the phone working away. And our clients, we use the word clients, we try and avoid using the word victim because victimisation is in the eye of the beholder. But our clients reside in every corner of the state. And in Queensland we see a fairly even representation of those from Metropolitan areas such as this great city but also regional parts of the state. I was talking to a lady just last week from the Atherton Tablelands.

So when we talk about identity compromise we look at it in two ways, we look at what's been compromised and how and what's the risk and has it presented in relation to its on misuse. And so one in, almost one in three Queenslanders last calendar year experienced the compromise of their information through a telephone scam and the reaction I get from most people in the community when we give presentations are arms are folded and heads are shaking going how can you be so silly. So I'm going to explain how that can happen and it's got nothing to do with the person's intelligence, it's got everything to do with their context. So I'll give a little case study on that shortly.

Telephone scams are more than three times more prevalent than email fishing. So it's natural for people to think identity theft, that's email fishing yet we're seeing telephone scams dwarf that. And there's also a fair representation of Queenslanders who have absolutely no idea how the compromise happened. How because they probably had nothing to do with it. It might have been an organisation responsible for their information being breached. It might also be because the criminals are really good at what they're doing. So how that cohorts detecting it is they're seeing then the misuse of their identity so last week in the media there was a fair bit of chat around telephone porting, unauthorised mobile phone porting where your mobile phone signal is lost because a criminal has stolen your number and now they're intercepting your SMS communications. That's not a compromise, that's a misuse. What would have been compromised is possibly a driver's license number before that and a lot of those clients don't know how that happened.

So it's a pretty complex area and you can see why the engagement we have in the community can be over a number of contacts. So when we look at telephone scams given that was the most predominant type impacting not just Queensland but across the country we look at the broad data. We see that almost ¾ of those scams represented one of four brands. So would anyone like to guess what those brands are? Australian Taxation Office,

hello to all of the Australian Taxation Office members listening in today. So tech support scams so Microsoft, Apple, Trend Micro is called one group and that's certainly increasing. Any others? Centrelink. So Department of Human Services and Centrelink. And the lucky last is Telstra. So they're the four ones that criminals like to impersonate the most over the last calendar year. And what criminals, the sweet spot for criminals when it comes to telephone scams is to exploit a situation of plausible deception. So what I mean by that is looking for a cohort in the community that are looking to install antivirus or have just purchased a computer and then engage with them to say can I offer you technical support. So it's plausible that you would fall for that. Or I've just connected with the telephone carrier, it's plausible that you may get engagement from a telco carrier. And they're very smart and sophisticated in how they do that. Some of them using add words, and adds to do this. So they'll look to see what you're browsing is online and the moment you hit your Google search on technical support and you jump on a website that's legitimate you might get an ad that pops up and says you've got antivirus on your computer. So it's plausible deception, it's got nothing to do with someone's intelligence, it absolutely makes sense as to why people are falling for this.

I spoke with a lady in, a regional part of this great state of ours last year and she was at home with her young kids and her young kids were on the gaming machine and up came a little pop-up that says you've got virus and the kid went and got Mum and Mum came into the lounge room and said what have you done. It's quite plausible that the parent would blame the child for what they have done. And the scam is noticed. So they're very very smart in creating that plausible deception opportunity.

One in four of those telephone scams led to the remote access of someone's device through mostly Team Viewer. So that's the scammer convincing someone to say you've got a virus or can I show you how the stock market works and can I get remote access to your device and when that happens really bad things can happen. So they might harvest all of your credential information via your emails. They might then forward all of your emails to their email account and so we find that the response journey for these people are actually really complex which I'll go into in a moment. We also see that telephone calls and those annoying ones you get at dinnertime when you're trying to do 300,000 things with kids and dinner and everything else. It doesn't always happen just with a telephone call, it can happen through other channels as well that then leads to a conversation with a criminal.

So these Queenslanders are actually talking with the transnational crime group and mostly that group aren't based here. They're based offshore. And there's thousands of them

targeting us. Not five or 10 but literally thousands of people in call centres targeting us today. That's how big it is. What are they targeting, mostly they're after your bank funds and your identity is a means to achieve that. Mostly they're wanting to apply for new credit in your name so we see around 14% of those clients experience then future misuse.

Our staff like the fabulous Chrissy ask some great questions of people such as why did you believe it and the majority of Queenslanders and Australians are saying I believed it because they gave me a sense of legitimacy through bureaucracy. So I've got a boss, I'm going to escalate it, I've got an employee ID, I've created a sense of bureaucracy around legitimately of my criminal organisations so that was also important to know.

So what about the misuse, what do we see. So there's the theft of the personal information and this is all about the misuse, what happens next. So telco scams, we see about 14% of the telco scam experience resulting in misuse but on the broad we see around one in four cases that come into IDCARE where personal information is being compromised, there is a subsequent misuse. Already you're on the back foot because two thirds of us are the first ones to detect it. So you think of all the money going into fraud prevention and detection by organisations but at the end of the day two thirds of the people are the ones that detect it. And that disadvantages them because they have to prove to others that they're a victim, they have to prove to big business and big government that they're the ones who actually aren't to blame for that debt that's been accrued in their name. It takes on average Queenslanders 20 days to detect it, across the country that's a lot longer so I don't know whether Queenslanders are just naturally more gifted at detecting these things. But importantly it took crooks on average 9.8 days to misuse so they act quick. So already things are stacked against us.

The value of misuse that was reported into IDCARE last calendar year from Queenslanders was about 14,000 dollars, so that's value, that's not the out of pocket loss. That could be the value of the product or service in which the criminals have acquired. And most of that is bank account, mobile phone services and indeed government services.

So if you're ever unlucky enough to be in this situation what does the response journey look like for you. On average you've got to make 17 contacts with about eight different organisations and it's going to take you about 30.6 non-consecutive hours. That's the rub. So when I talk with clients on the phone I say be prepared, even though the criminals are acting quickly you're going to be at this for months and it's going to be a long bureaucratic journey

for you in unscrambling the eggs. And at times you're going to be lost in the administration which is why we are there to help them through that process.

We also cheekily ask them how would they rate their interactions with organisations before they come to us, what does customer service officers tell them to do, is that advice consistent, how long are they waiting on the phone for. Are the call options clear when you press a button, is information on their website. So we collect a whole lot of information and metrics about how the ecosystem responds and the standard's pretty rubbish. Okay so in the words of one of our identity and cyber security counsellors, if you're not harmed by the crime you most certainly will be by the response. So it is bureaucracy central and it's very variable.

So we're seeing at the moment probably bucking the trend of media reporting, what's coming out of Royal Commissions but for Queenslanders the best performers were financial institutions in terms of response. You might say they're financially incentivised to do that and the worst performers were the telcos. And there's a lot in that group that's in the bottom quartile, including government agencies. So part of my work at IDCARE and at the University is to raise awareness of the performance of the eco-system to try and lift standards and inform policy makers about what works and what doesn't despite good intentions sometimes it actually creates a worse problem for the community.

So some closing remarks from me Phil. Valuing personal information which is a bit of a mantra this week. One of the things that we see is we need to find better ways to deter. At the moment if you're an organised criminal throwing grenades into our living rooms every day there's not a lot of deterrence that they're feeling. We need to recognise the value of personal information and act and respond accordingly so do me a favour tonight, go into your Gmail and Hotmail accounts and work out how many license numbers and passport images and passport numbers you have in there and remove them. So emails are a good place for criminals to look and extract. Prevent, respond and be resilient, that's the responsibility of not government or the police, it's actually the responsibility of all of us. So crooks are succeeding here because they are exploiting a network so our response needs to be an networked one so we need to look at that together, not in isolation. So it sounds like I'm going to get the acoustic guitar out and get the campfire going, but it's true.

There is a corporate social responsibility here that goes well beyond what the privacy legislation says you need to do as an organisation. And that's one of the big early lessons that we're seeing from the notifiable data breach scheme at the Commonwealth. Whether you like it or not the people impacted by data breach will call IDCARE and we'll hear from

them what they think of that experience so before you do what some organisations have already done since mid-Feb and tell 30,000 people to call us, maybe have a conversation before you do that with us around what that might need to look like. There have and there needs to continue to be market shifts or shops around privacy and there's more to come. There's a lot more to come. And so that brings into sharp focus who actually owns this problem and how we're going to manage it because we see from a community perspective that the journey that the residents of Queensland and indeed the rest of the country are on is pretty much an unacceptable one at the moment and there's a lot more work that needs to be done and I encourage you and energise you to have that conversation and debate and I thank Phil and the Commissioners plural, Deputy Commissioner Steve Gollschewski, good to see you. Ladies and gentlemen thank you for your time and congratulations on Privacy Awareness Week.

MR PAUL MCCARNEY, CHIEF EXECUTIVE OFFICER OF DATA REPUBLIC:

So thank you Philip for asking me here today. I think I've been on this journey around privacy and around the concept of balancing as we heard the Attorney General say the ability or the need for innovation with the want of privacy and protection of our rights as consumers. Data Republic, Data Technology started up, we're committed to helping organisations be able to, of all shapes and sizes be able to share data and do it securely and do it sensitively and ethically and sometimes those, both of those things are difficult for some organisations and we've seen lots of breaches over the past several years and I'll talk about some of those today and I'll talk about why, why that's occurred. Data Republic is lucky enough to have several large organisations invest in us, companies like Qantas and National Australia Bank, ANZ, Westpac have put their faith in our organisation to help them understand how they go about managing the tension between the ethical treatment of their consumers and the benefits they can get out of sharing data either intra-department or with other organisations and I think the Attorney General mentioned some of those benefits we can see with homelessness, sharing with police, police sharing with mental health. They're all the cases that we see pretty regularly.

So look if we can think about a time which is arguably today where there is enormous huge benefits that we get out of sharing data. Now if we could share, every day we get on a train we're sharing data, every time we write a business plan we're sharing data, every time we deliver a product to a customer generally we're sharing data. Data sharing is existing all around us but still data is often a four letter word. It's still a word that we shy away from and it's a word that is associated with another four letter word which is risk. And the primary

difference between both of those two things and the reason that we are having this conversation today is because there's a lack of trust and so trust by design is a concept I'm going to talk about and the element, and privacy by design is a subset of that. So we can see that you know there is huge value from data. You know 3 to $5 trillion just from governments opening data up is a lot of money and that's just, and that is an annual productivity improvement so let me give you another example of where value sits inside data. So United Airlines owns 1369 planes. Their return on non-current assets which is the planes and primarily the planes themselves and their access to various airlines is around 16% which is arguably in the business world not too bad as opposed to Facebook which is worth $450 billion and their return on non-current assets is over 50%. The differential there is data. The reason they're valued so highly is because operational leverage they get from data, from our data is huge.

So companies are, and the top five companies in the world now are all arguably data, closed data environments, closed data businesses. I'll give you an example. So Tesla sells about, has sold so far about hundred thousand cars which is not very many. Right so Ford sells, Ford would sell that in a week. So about a year and a half ago Morgan Stanley put a buy increase on Google Alphabet as it's called now and they added another $70 billion to the value of that business. And the reason they did that is because Google bought a company called Ymo. Ymo is their autonomous vehicle data business or driving business and Ymo suddenly got access to data from another vehicle business called Lift, has everyone heard of Lift? Competes with Uber in the States. So Uber had arguably 10 times more data than Facebook, sorry than Google so Lift has a similar number. So just by accessing that additional amount of data Google gets a $70 billion valuation increase because they put, which is a big evaluation by the way than the analyst put on their add words business. So the total addressable market that the market are putting on that data, just that one dataset is more than the whole current advertising business that Google run. And that just gives you a sense when we talk about the value of data which is what we're here today, we should value data and let's talk about well, if we should value it, is it valuable. I'm going to talk about that in a second as well, how is it valued. It's actually not valued by the way, it does not sit on anybody's balance sheet, the gap principles don't allow it, it is not an intangible asset right now. It arguably should be and all of our companies would arguably treat it a bit more carefully if it was on a balance sheet, it's probably a discussion and I have another presentation on that should someone wish to see it.

So data is the new oil. Now it's debated technically whether that's the case but it is fuelling a new revolution and is the basis of we would argue the fourth industrial change. But there are huge risks and we've seen them. There are the risks associated with de-identification, honeypot risk, Equafax having all of the PI sitting in one place for people to go to great lengths to access. The risk of re-identification, the ability to use geospatial data and geo-tags is to be able to determine where a secret Army base was. And lastly the one that we've heard most about more recently which has not been a breach of any of the other types of privacy that we think of, this is primarily a breach, a front door breach, coming in the front door and one organisation not policing the intended use or the consent statements correctly of how someone was permitted to use it. There was no matching up of the intended use when we agreed and ticked that box to use Facebook and with the permitted use of how and what they gave their data for to Cambridge Analytica.

So let's think about all of these risks. Why are these various people going to all this trouble, what's in it for them. And what is really the value of that data to them, how do they think about it. And on the dark web we can see there's considerable rewards. These are actual prices from the dark web for those types of data. So for an individual PayPal account people will pay $247 which is a lot of money. So what happens on the dark web is people will bid on these accounts, I'll talk about how they bid and why they bid certain amounts and this is what they, when they are trading, it's in an eBay style environment. They trade our PI and other, various organisations and people buy it and they leverage it. And this is the same, the same here is coming from online banking data. $160 a record. It's going to be hard the next slide because the backgrounds haven't come out great. So we'll talk about why people pay different amounts and a lot of it's got to do with how fast the bank or the issuing organisation act, the faster they act, the less people will pay. So response rate and technology is becoming increasingly important as a race to not be the last bank. The type of data that's being, the type of information and the half life to that data is also important. And that half life means how fast does the data decay and at the moment there is a significant increase on you know data that's 2 to 6 years old people are still using, people reusing it. That data has increased you'll see in a second. 400% increase on people who are reusing data 2 to 6 years old, data that got stolen not 9.76 days ago, two years ago being reused.

And so what we're seeing is these individuals, you know they are touting and breaking the law. We talk about value of data. This is the real value of data right now and it's valued because you've got supply and demand economics of people supplying the data and bidding on the demand for it, pricing our own records and that's hugely challenging for all of us, and

a lot of the reason that we're here. You know it's the reason that, a lot of the reason I've set this business up is to ensure when people hand, or move data around it's done privately and securely and it's done with the governance levels that you'd expect to happen if it was money. That's the key difference, if it was money. At the moment we don't value it like we should and again that is the core of what we're talking about this week.

So we do see data, we do see that half life declining and we are seeing you know a huge increase in fraud that is deferred and so it's important that we design things now and we get our design right and we design systems, not executions but systems to ensure that when we manage the balance between innovation and privacy that we are getting that correct and that balance is one that allows us to innovate whilst maintaining the applied risk for each individual use case.

So there's also rewards for organisations that aren't breaking the law. They're closed data platforms. These companies have utility propositions that allow us to say I'm happy with the search utility, I'm happy with this social utility, I love these recommendations I'm getting, all of that is using our data for benefit. That benefit is outlined there in that graph. So you'll see that Facebook at the moment around $6.70 per quarter they make out of trading our data. Now we often are happy with that trade, we are trading off our privacy or our data for that utility. And these organisations are also, the first organisations to be compliant with GDPR oddly because they are closed environments. It's much harder for, I think there may be one bank in the UK right now who is going to be compliant on May 25th deadline, maybe two. But it's very difficult when you've got product collection statements as opposed to consumer collection statements. It's very very difficult to be compliant right now.

And so the cost is in the billions, the costs for these guys is very low because they are closed environments and they can say you just don't get to get, you don't use it if you don't comply. Because they have a utility proposition which sits outside of their revenue model and that's very very powerful. We just, I'm putting that up for noting, I don't have an answer to it right now but it's something that other companies around the world aspire to and they are concerned with. So what we often don't talk about is the human cost and Steve spoke about it a bit before. You know 30 hours is a long time and that's the cost that never gets associated with breaches. The mental health costs would also be strong and high and I think you know a lot of, we're seeing that with teenagers now with, we have done some work with Reach Out, with Adless(?) and Depression and the challenges around those individuals who are getting data about them shared, private data about them shared is not insignificant.

Now I spoke about those large organisations before and just bear with me with this odd picture. But horizontal and vertical integration for these, particularly the large five organisations is going to be challenging in the years to come. I sit on other public company boards and we speak a lot about these sorts of organisations being able to easily move from one industry to another. Amazon are about to launch a bank in the States. And for any bank or anyone who has been a banker and understands how important data is for credit and risk models and effective pricing and acquisitions, that would be hugely challenging because they would know more about an individual bank's customers than the bank. And that means for more effective acquisition and it means for a better credit model and better pricing for the customer so arguably the consumer wins, they're the competition. But for industries that are thinking about having to compete generally with traditional competition is one thing but when it comes where you are about to be disrupted because of access to data then that's something that every board member in Australia needs to pay attention to and arguably the world.

Now the balancing act between the need to compete and add value, and I say compete because there's a lot of government services here that add enormous value to citizens and the need to add value needs to be balanced up with the ability to manage risk associated with privacy. There are a lot of factors to consider and this goes for an individual share of data and it goes for a whole government thinking about how it regulates and one of the great things in the Farrell report that Scott wrote was around reciprocity so there is no assets stripping of data out of the banks for open banking and he has given a lot of thought of how, of why it sits under the ACCC and why that is a powerful body to think about managing privacy arguably. And the Singapore government has just done a very similar thing with privacy coming under DIPO which is now thinking about innovation and privacy under the one group. And that balancing act is something that every country and every company, and us even as individuals balance every day. We are often making trades around that are subconscious to right now, we're all making a trade that there's apps on our phone that know we're all in the same room together. We're happy with that, we get utility from our phone and our android operating system as we heard this morning in the news. Those trades, we may be happy, we may not, we can choose not to use the phone or leave it at home. And they're difficult trades to make but they're trades that we make around utility and privacy. And all we need really is a mentor or framework to manage that and a lot of what I'm going to speak about in the next few slides is that framework.

So how do we develop trust by design? How can we think about the ethical treatment of data? The three primary pillars at Data Republic that we think about when we're building our platform. Privacy, security and governance. And often they are interlinked, they're often joined at the hip, particularly governance oversees all of them. And so we need to rethink around how data flows around our economy and evolves the conversation to talk about the right consumer consent first, the ability to match that intent when that data is being collected with what is going to be done with the data itself, what is the permitted use. So data itself isn't bad or good, it isn't expensive or cheap when it's at rest it's a bit like money. If you buy a bomb with money it's bad, if you give it to a charity it's good. The use of money often defines its benefit or its risk and data is the same. It's the use of data that allows us to think about risk or benefit and that's the construct that we need to think about at the very beginning. Before we write any code, before we develop any policies we need to think about the construct of governing the use of data.

So the first risk that we see in privacy is one that gets spoken about a lot, de-identification. Going to give you an example of what that actually means practically and a little bit technically so excuse me for those - but it means around taking the PI out of personal information out of a database and ensuring that you don't have at rest the personal information with the attributes and they're separated with separate encryption elements and I'll talk about how that is and why that's important. And it's primarily important because we saw before that the benefit that these criminals are getting from PayPal data or bank data and they are making a lot of money from it, it's important because that's the data they want. They want to be able to marry up Paul McCarney with my bank account number or my password or my driver's licence. If those two things are sitting separate it's very hard for them to do that. And at the moment that's primarily not done. The other one is there is huge reidentification risk and we've seen the ISE come out with a fantastic paper recently all around how we think about the reidentification and the risk associated with reidentification. Particularly using geo-data and health data and retail transactional data. And lastly it's around the governance of permitted use. And so again I mentioned that Cambridge Analytica wasn't any breach or security or privacy breach, it was a front door attack and it was all about the marrying up of the intended use or the not marrying up of the intended use with the permitted use.

So when I talk about deidentification there are lots of mechanisms that we can use. Most organisations don't do anything. They keep their data in a CRM and they have, my interactions with that company sits in that CRM and my email address sits in there and the

fact that I bought a glass of water or a beer or a glass of wine or I transacted or I was somewhere, they're all in the one database. There are other methods that you can use where you can encrypt the personal information or you can hash it which is a one-way encryption algorithm. You can store that centrally for, with attachment of tokens to be able to access that and trade on the tokens or move the tokens around. Or, which is something we are working on or have finished completing actually and launched in a month and a half, a decentralised token network which is a federated system, federated hashing, federated identity, there is no honeypot. There is no risk associated with where the PI sits because it doesn't sit anywhere. It sits in a network. So you're able to match arguably which is why everyone has PI, be able to have match attributes between Department of Human Services and the Tax Department or Police, at the moment that's the most challenging element and that's where most of the risk sits. But having that federated is something that I haven't seen done before and is something that we are quite excited about talking about very shortly.

So how is it done mostly and I just want to give you an example of what it is because lots of people talk about this concept of privacy by design and I just want to talk about one element. So think about the removal of PI from your business, arguably from the economy if you've got it right. So at the moment let's separate PI from attribute data so we decrease the risk of de-identification. What does that actually mean. Here we have an airline flight database and we know that Mr Doe is about to head off from San Francisco. So here we create a separate database in a separate environment and we just have his personal information, it's an identity database. Now let's think about giving that database a token, a random alpha numeric set of characters and we append that to his database record, now we decide that we can remove all of the PI data from that attribute database and encrypt or hash the identity database. So now we have an environment where we have a list of attributes and arguably just an encrypted d hacker Philip and you're about to hack this environment what would you get on either side there, not much. You'd get an encrypted address book with a series of numbers and letters or you'd get some information of just attributes about nobody. And so that's the technical manifestation of privacy by design. But that doesn't happen by itself and it doesn't happen without a whole set of rules and protocols and a legal framework to operate within an those frameworks and protocols need to be built first because expectation management is critical. It is critical that when you go into these discussions to share data and do them securely people understand what is expected, what is going to happen, how is all this going to work. And so the systems and frameworks and technology become more important, not less.

So again I mentioned the ISE paper and I don't know if many of you have read or heard about the New York taxi cab reidentification hack that had Bradley Cooper being outed as a very bad tipper, and but it really just maps to the governance of permitted use. I could go on and on and on about the different types of perturbation and synthesisation and algorithms where you are looking at risky data but at the end of the day there is lots of data that is open, that is not nefarious, that people can use and get benefit from but of the 105,000 data sets that the New South Wales government has very few of those are that type of data. Most of them need to be shared. And the difference between open and shared is governance. And so you need to manage the risk and the governance associated with what people are going to do with that and if they're going to do something that might be determined to be risky, then you need to de-identify it. You need to make sure that the reidentification can't happen, the data may need to be synthesised if you need to get the outcome, it happens a lot in health data.

And lastly around the permitted use of governance, in the middle is our legal framework, it's the one that we built before we wrote one line of code. We spent a lot of money on building a legal framework to ensure that the protocols and the permissionings were developed so that we have the ability to manage and map the intended use that the consumer had signed off on with the permitted use of the organisations that wanted to share that data. And that's helping us balance that need for innovation on one side with the absolute requirement to manage consent and privacy on the other.

I'm not going to spend too much time on this topic, it is a very broad and deep one. Suffice to say that the cloud has increased security drastically and people will say contrary to that. Amazon and Google, or AWS, Google and Azure have thousands of people working on security, thousands. Everybody who works on our platform needs to be accredited, authorisation is critical, tokenised data only is also critical. Any data that's held anywhere should be encrypted at rest. They're the key principles. Having a framework for security is also important, again that's ours on the right.

So the last and arguably the most important element of privacy by design or trust by design is defining the contextual relevance or elements of data, collaborating on it, being able to talk about it and that's also challenging to be done in a secure environment. So collaboration, you know it's important to understand how the data behaved and what you want to do with it to really understand what is going to be allowed or permitted. Again equally who can have access to it, how do you provide access. How are there different permission levels to who has access. Is it just me or Philip or Philip needs to sign off on it finally on any particular

exchange and so the permissioning levels, like we do in any enterprise data warehouse are critical to good governance. And then lastly I'm not going to go, this is, we're sort of winding up now but this gets again quite technical but the difference between open data and never shared data is a huge gap and it could be the difference, and is often the difference between life and death. We see this no doubt in police every day, if we had more liquidity in data it would be much easier for a lot of us to do our jobs. In New South Wales we've seen legislation to enact the sharing of data between departments and no doubt that will, and that is also finding its way into Singapore and into Canada as well.

So when I think about the factors that we can dial up and down to help us manage governance based on a permitted use I think about these things called the six safes or five safes that you may have heard about them. So how much legal recourse is needed, how can you use legal recourse to determine whether data should be shared or data should be valued or what value should be applied on it. How can I authenticate who the person is, is the person of good stature, has the person committed a crime before. Is the project ethical, is it reasonably expected by the consumer that that should go ahead. Are there breaches around insider trading or anti-competitive behaviour, what level of security is required, should I lock them in a room, should I video them using and working on that. Often coefficients can be found in data science that you may not want them to look at. And what degree of perturbation or synthesisation of the data should you apply and lastly how does the output comply with what the permitted use was. So all of those sit on a scale and not every valuation or share of data are the same. We need to dial these things up and down to ensure that for each permitted use we manage it appropriately, whether it's completely open or constrained and shared. So I'll wrap up by saying that we do have a view that data's changing the world. I'm definitely not a cynic, I don't believe privacy is dead and I think that we stand in an incredible moment in time where as individuals and governance of businesses we need to stop and take stock of the real value and the role our personal data plays in our own future and in the future of our technology that we use every day.

Data needs to be able to move around our digital world increasingly. Insights are critical for us to work and operate in an effective society. But it is possible to manage the balance of daily liquidity and privacy if we set parameters up front, if we think about privacy by design and ultimately we engender trust and if we can do that I think we can have a fantastic outcome. Data Republic is trying to manage that for governance not only here, and companies around the world. So I'm very grateful that I've been asked up here to privacy week and I believe this is a real problem to be solved and I will finish by telling my only

privacy joke that I know. So there were two lawyers in Europe and they were talking to each other and they said have you got the name of a good GDPR consultant and one of them said yes, the other one said can you send it to me and the other one said no. So thank you for having me and happy privacy week.

Hard act to follow. I think he's drunk the Kool-Aid to with everyone here there seems to be a bit of optimism about privacy and getting the right balance and the good and ethical use, and socially responsible use of private and personal information and protecting it and preserving in the right circumstances and the challenges as well that we face. Frankly the Attorney's got a hard list of legislation ahead in terms of getting that balance right and some of the laws that actually help underpin our privacy besides the Information Privacy Act. I'd really like to thank David and Paul again, fantastic presentation, really rounded out some of the challenges and particularly the difficulties we can face when our privacy's comprised so thank you very much again.