**PRIVACY AWARENESS WEEK 2017 LAUNCH**

**COMMISSIONER RACHAEL RANGIHAEATA:** Okay. We might make a start, thank you. Good morning, I'm Rachael Rangihaeata, I'm the Queensland Information Commissioner, and it's my pleasure to welcome you to the official launch of Privacy Awareness Week in 2017 in Queensland.

Firstly, I would like to acknowledge the traditional owners of this land on which we gather and pay respects to their ancestors who came before them and to their elders, past, present and future.

Before we start today's event, I have some quick housekeeping to take care of. For the comfort of other guests, please, we request that you turn your mobile phones and other communication devices to silent. Toilets are located downstairs on Level 0, or via the lift and to the right, or alternatively past The Edge Coffee Shop on Level 1. The Edge is part of the State Library of Queensland and visitors to the space are governed by the policies and standards that the State Library of Queensland has put in place.

At the outset, I would like to acknowledge a few special guests joining us here today: Alan MacSporran, Chairperson, Crime & Corruption Commission; Peter Martin, Deputy Commissioner, Queensland Police Service; Kevin Cox AM, Commissioner, Antidiscrimination Commission; Walter van der Merwe, Electoral Commissioner, Queensland Electoral Commission; Phil Clarke, Ombudsman, Queensland Ombudsman; and Andrew Mills, Queensland Government Chief Information Officer.

I would like to also welcome everyone watching the live stream and encourage you to participate in the conversation on Twitter using the hash tag PAW 2017.

Privacy Awareness Week, or PAW, is held annually in May and was established by the Asia Pacific Privacy Authorities in 2006, of which OIC Queensland is a member. Public and private sector organisations from across the Asia Pacific Region host a variety of programs and initiatives during this time to promote awareness of privacy rights and responsibilities. PAW

provides an opportunity to promote a culture that protects and respects the privacy of individuals personal information and to raise awareness within the community more generally.

In Queensland, the practice of and potential to share information across government and with stakeholders is growing at a rapid pace. Understanding the Information Privacy Act's role in this practice can be challenging for many Queensland Government departments, councils, Ministers, universities, statutory bodies, as well as their bound contract service providers. It is also important for the community to be aware of their privacy rights when sharing their personal information online, including with government.

Information sharing, including personal information, provides an opportunity for public and private sector agencies to make better decisions which can result in better community services. Raising public sector and community awareness of privacy rights and responsibilities regarding information sharing and the protection of personal information will contribute to better outcomes for all Queenslanders.

This year's Privacy Awareness Week theme of "Care When You Share" is designed to encourage individuals to care enough about their own privacy to better inform themselves of what will happen to their personal information before they share it. It also reminds public servants to take care and understand their responsibilities before sharing information and to inform the community about how personal information will be shared.

Today's event brings together international, national and local speakers to share with you their experiences and challenges. I am sure you will find their presentations insightful and thought provoking. To get things underway, and to officially launch Privacy Awareness Week for 2017, I would like to welcome the Honourable Yvette D'Ath, Attorney-General and Minister for Justice and Minister for Training and Skills. Please welcome the Attorney-General.

**(Applause)**

**HON YVETTE D'ATH MP:** Good morning, everybody, and can I start by acknowledging the traditional owners and custodians of the land in which we hold this important event this morning and pay my respects to the elders, past, present and emerging.

I would like to acknowledge the speakers at today's event. If I can acknowledge Ms Rachael Rangihaeata, Information Commissioner, Mr Philip Green, Privacy Commissioner, Ms Elizabeth Denham, United Kingdom Information Commissioner and keynote speaker, who I believe is joining us by video link today, Ms Roslyn Bell, Assistant Information Commissioner, Australian Productivity Commission, Mr Corey Moynihan, Senior Director, Digital Architecture and Information eHealth, Queensland, to all of the other distinguished guests, ladies and gentlemen.

I'm certainly pleased to be here today to join you to officially launch Privacy Awareness Week in Queensland in 2017. Privacy Awareness Week has been held annually since 2006 to promote the awareness of issues and the importance of protecting personal information.

As I sat here last year listening to the keynote address from Shara Evans, a Futurist, I was enlightened by what she had to say, but I was also extremely frightened by the intrusion into privacy through digital technology. I can't help but sit there and listen to an address like that and not just sit there as a Member of Parliament, as an Attorney-General or Minister for Justice responsible for many of these areas, but also as a parent and as a citizen and think what does this mean for our individual privacy rights?

After a decade in politics I can assure you that there is no concept that is quite so rare, elusive and precious as privacy, especially in this fast-pace digital environment. It is also a topic that reflects the diverse nature of my portfolio. Questions of privacy policy range from information management, consumer affairs, the work of the courts and the justice system.

This week's theme "Care When You Share" reminds us of our duties as policymakers. Advances in technology have significantly impacted on the ease with which personal information can be collected, used, shared and combined, introducing new challenges for its protection.

We have a duty of care about and for the information that we gather and use, but for these broader schemes of work we need to help people protect and value their privacy at the individual level. As individuals, we need to take care when disclosing our personal information to others. Our privacy is valuable and we need to understand the importance of protecting it. We also have to be careful about protecting and valuing people's privacy.

I know that last year I had the pleasure of standing here and saying as a parent of two teenagers I had managed to hold back the tide and had neither of them on social media. Unfortunately, in 2017, I stand here as a mother of a 17-year-old and almost a 15-year-old and say that tide is shifting. But it is a fear of all parents, not just about what we do ourselves and the information we provide, but also how we better educate our young people, our teenagers, those in their 20s, and how to protect their privacy in an environment where there is less concern about the privacy of the individual at that age than ever before.

So, while the challenge for governments is we still have people in our community fearing what government does with their data, those same individuals are often sharing more personal information than ever before through social media and they're not seeing the link between the two. They're not seeing that the sort of information that they share every day with government agencies that they're so concerned about being passed on or used for other purposes, they are themselves putting out there on a daily basis.

I know much of what you are discussing today and hearing from the speakers is very much around personal data and the issue of how government agencies protect that data, but, as I say, privacy goes much further than just how government deal with particular data, it's about your personal information and circumstances. So, the theme of Privacy Awareness Week this year being "Care When You Share" and encouraging individuals to care about their privacy and better information themselves of what will or might happen to their personal information before they share it, should be viewed extremely broadly when we have that discussion.

So, when we ask people to care when they share, they need to think about other information that they are sharing about their children, about their friends. As I say, in my role - and my husband's a police officer, my kids haven't got much hope when it comes to having us not

looking over their shoulder when it comes to social media - but I am astounded every day at the amount of information that adults put about their own families, the photos of their children, their names, their ages, where they go to school.

It is not that long ago when our private photos of children enjoying themselves at the beach, in the swimming pool, in their pyjamas, mucking around with their siblings, those were photos you would find in a personal photo album only shared with your closest of friends, but now they're there for complete strangers to view.

So, I do believe that this year's theme when we talk about "Care When You Share" isn't just about government agencies and what they do with that data, it's not just about organisations and what they do with sharing information, but it's also about every single individual in our community actually becoming more aware and educated about what that actually means and what that means for the future.

From a government perspective, we can focus on building public and customer focus in the way we deal with personal information, maintaining strong security and information handling practices within agencies. It is critical that government at all levels strikes the right balance between public safety, service delivery, information management and privacy.

Information sharing can increase the efficiency and effectiveness of government services, improve service delivery and foster innovation, but we need to get the balance right, and I know that Elizabeth Denham will be addressing this very important issue shortly in her keynote address and giving us some suggestions about how we do get that right.

Privacy and security of personal information is essential in creating and maintaining the community's trust in government. The lack of information sharing on the grounds of privacy have led to a less efficient service to the community, that I have no doubt of, and not just across government agencies but across levels of government as well. Often privacy has been used as an excuse or justification for not being able to share information, but we are realising more and more that for us to truly service the community and to get the best outcomes we must share that information. If we are going to have intensive case management of individuals

and families across Health and Mental Health and Housing and Education and Child Protection and Justice, we need to have that information sharing.

I know better than most when it comes to my portfolios in Youth Justice, that the only way I'm going to assist young people who have found themselves in the criminal justice system is to actually look at the underlying cause and start addressing those causes. We can't do that if we're not sharing information, if I'm not talking about that young person having substance abuse and mental health issues and looking at housing problems and whether they're disengaged in education and whether they're also known to the Child Safety system. So we do need to share information, but we've got to get that balance right as to how we share that information and still protect that privacy.

Part of this is having sound privacy practices in place from the outset by adopting a privacy by design approach, but in building privacy by design we must be open by nature. The rapid pace of technological advancement means that privacy is an area of increasing complexity and challenge for future years. I'm keenly aware that a particular challenge is for our government policies, procedures and legislation to keep up with these developments. The spirit in which information is collected must reflect the spirit of its usage, serving the public interest, advancing the State and its people's interests and respecting the fundamental rights of all Queenslanders.

This is the ethos of the Public Service as an institution. The same ethos should inform our use of public information and our considerations of privacy. In considering how we care before we share, we should also consider the use of government holistically. Our government takes a wide view of the information over which we have stewardship. We believe in building transparency, integrity and accountability into new institutions and reforming existing ones to better meet these achievements.

And I personally, as the Attorney-General and Minister for Justice, and the government understands the challenges in releasing information that is in the public interest and ensuring compliance with legislation, including the privacy of people's safety, and I'm certainly well aware of that and I'm sure everyone in this room of recent debates around Youth Justice and the privacy and the balance between what the public should know and must know and the

rights of individuals, and especially young people in our system, and it's balancing all of those legislative responsibilities along with the safety and security of our services and ensuring that the public have confidence in what we are doing. It's not an easy balancing act, but it's one that we have to strive to achieve every day. That's why we have important processes and institutions like the Office of the Information Commissioner to assist government agencies in how they handle personal and State information.

I thank the Information Commissioner, the Privacy Commissioner and the staff of the Office of the Information Commissioner for their efforts in this regard.

In December 2016, I released a consultation paper as part of the review to seek further feedback on key issues raised by those Acts. Over 70 submissions were received in response to the consultation paper from government agencies, community organisations, individuals, corporations and media representatives highlighting the importance of public debate and consultation in relation to right to information and information privacy related issues. The submissions are currently under consideration in relation to future improvements to the legislation when it comes to privacy and also the right to information.

Clearly the issue of privacy will remain an important issue for our society and our State and one that I believe will only become more complex as technology drives change that is no doubt welcomed in many areas of our society and in many ways, but in insuring privacy becomes an increasing challenge.

I commend all of you here today for taking an interest and making your contribution to this forum. On that note, it is wonderful to have Ms Elizabeth Denham, United Kingdom Information Commissioner, to present the keynote address today. Privacy presents a number of challenges and opportunities internationally and it is important that we continue to build a culture of privacy where private rights are being respected and protected in Queensland and other jurisdictions. It is with great pleasure that I launch Privacy Awareness Week for 2017. Thank you.

**(Applause)**

**COMMISSIONER RACHAEL RANGIHAEATA:** Thank you, Attorney, we appreciate your ongoing support of PAW to launch our event today.

United Kingdom Information Commissioner, Elizabeth Denham's pre-recorded keynote presentation on the topic of privacy and information sharing from an international perspective will now be shared with us today.

Elizabeth was appointed UK Information Commissioner in July 2016, having previously held the position of Information and Privacy Commissioner for British Colombia, Canada. She was honoured as a UBC distinguished Alumni for her pioneering work in archives and leadership in the field of access and privacy in 2011.

In 2013, Elizabeth received the Queen Elizabeth II Diamond Jubilee Medal for her service as an Officer of the Legislature of British Colombia, Canada.

Elizabeth's presentation today details three key developments in privacy and data protection in the UK and Europe, being general data protection regulation, updates to information sharing rules for the public sector and the UK Information Commissioner's Office New International Strategy.

We are most grateful to Elizabeth for providing the following presentation for our PAW Week launch today. Thank you.

**KEYNOTE PRESENTATION PLAYED -**

**COMMISSIONER ELIZABETH DENHAM:** Hello from the United Kingdom. I'm sorry I wasn't able to be with you in person today, but I'm very pleased to join you via video link to celebrate Privacy Awareness Week.

Let me start by congratulating everyone in the audience for coming out to participate in this event. If we want citizens to know privacy rights and exercise them with confidence, public education is key, and if we want organisations to be aware of their privacy obligations and better equipped to meet them, privacy awareness is a great way to make that happen.

It's events like the one that you're having today that gets the conversation going, bringing together practitioners, regulators and civil society groups, everyone concerned with privacy and data protection.

I understand that many of you work in the public sector and many citizens don't have a choice but to hand over their data in exchange for the services that you provide. So their privacy is in your hands and the care that you take with their data that you hold is the key to public trust and public confidence.

By taking part in Privacy Awareness Week you're walking the talk and you're showing us that privacy matters and that it's important to get it right. As you heard in my introduction, I'm a Canadian expat living far away from home, and I moved from a tiny island on the far-west coast of Canada to a much bigger island across the Atlantic. After 12 years as a privacy regulator in three Canadian jurisdictions, I'm now working as a national regulator in both information and privacy rights for the United Kingdom.

The ICO is one of the biggest information rights regulators in the world and it's a privilege to work here. We have an amazing team with a passion for access and privacy. It's been about nine months since I took up my role, and while the institutions of governments between Canada and the UK are similar, I didn't realise quite how much of a change it would be.

The UK is going through a major political, social and economic shift, one that brings opportunities to shape the future of data protection. But it's not just the UK, changes are afoot in privacy around the world. Like many of you, I've worked in the sector for a very long time and you'll remember that privacy was once kind of a quiet area of policy work and now it's at the heart of many public debates.

What used to be a backroom function is now central to how governments and businesses operate. The forces that shape our lives from Facebook news feeds to the algorithms powering the data, they are increasingly opaque, yet citizen demands for transparency, for accountability, are stronger than they have ever been.

We live in a world where nearly everything is possible. Technologies can identify us, they can track us, they can learn our shopping habits and our political leanings. No matter where you are in the world, it's an exciting time and it's a critical time to be working in privacy. And while our cultures may vary, at the end of the day know that the actions that you take on privacy here ripple around the world. I know, for instance, that the Australian Court's recent decision on metadata is being reviewed and scrutinised by privacy experts around the world.

Let me turn now to a few issues that the ICO is working on, things that are on our desk, the actions that our office is taking as we cope with the winds of change. So I'm going to speak to you about three key developments in the United Kingdom: the new data protection regulation, updates to information sharing rules for the public sector and my office's new international strategy.

The most important work before us is changes to the privacy laws in Europe. The General Data Protection Regulation, or GDPR, is the first comprehensive update of European data protection laws since 1995. And let's think back to a moment to 1995, those clunky computers, the crunchy sound of a modem connecting to the internet and those brick-sized mobile phones. So this update to the law is a long time in coming and the GDPR applies to any organisation, public or private, that handles or processes or controls the personal information of European citizens. So, if you offer goods and services to the EU or if you're monitoring or analysing using tools to analyse or track consumer behaviours, that activity includes the EU, then you may want to pay attention to the GDPR and it could very well apply to your business.

One of our major changes forthcoming in the GDPR is that citizens and consumers will have more control. For example, they'll have stronger rights to be informed about how organisations are using their personal data. They will also have the right to request that personal data be deleted or removed if there's no compelling reason for the organisation to continue processing

it. And they will have a brand-new right to data portability, to obtain and to port their personal data for their own uses with different service providers.

The GDPR also contains new obligations for data processors and data controllers. There is a new data breach reporting requirement. Where data breaches pose a risk to individuals, the organisations must notify the Data Protection Authority and in some cases the individuals affected. If data processors want to do business outside of their borders, they have a responsibility to make sure the personal information flowing outward does not get lesser privacy protection than was provided for within the European framework.

But the biggest change for data controllers in the GDPR is towards accountability. Accountability moves away from seeing privacy obligations as a box ticking exercise towards building a culture of privacy that underpins the entire organisation and they must stand ready to demonstrate to regulators, to consumers, that a comprehensive privacy management program is in place.

The GDPR mandates data controllers to put comprehensive but proportionate government measures in place, like privacy impact assessments, privacy by design, and these tools used to be best practice but now they're legally required in the GDPR. If you do business with the UK or other member states in the European Union, or you aspire to in the future, adopting an accountability approach will stand you in very good stead. I know that the Australian Privacy Commissioner's Office has issued step by step guidance that can help you get there.

The GDPR comes into effect in May 2018 and everyone in the UK is busy getting ready. Organisations are engaged, they're getting ready for full compliance hopefully from day one.

Despite Britain's exit from the EU in two or more years' time, the UK will implement the GDPR. At the ICO, we're putting together - we have a lot of focus on helping public bodies and private sector organisations prepare to meet the requirements ahead of implementation and we have plain language guidance to help everyone get ahead of the curve. So that's our really big project right now.

The second thing that I wanted to talk to you about is information sharing, and I think it's fair to say that 10 or 20 years ago most of us understood how our data was being used by governments and businesses. We knew what our bank was doing with our information, we knew what government departments were doing with our information, but today data processing can be opaque and business models aren't always widely understood. With chains of companies and partners involved in data processing and data sharing, it's difficult for the public to know what or who to complain about.

You might know that the UK was an early adopter of information sharing, or "joined-up" government as it is called here. Ten years ago, we first learned of Parliament's intent to allow government departments to facilitate and share information more freely. Their vision was to find efficiencies to address complex policy issues, to give better service to citizens. Laudable goals. But there is broad public concern about what information sharing would mean to the privacy rights of individuals. The ICO has played a role in ensuring safeguards are in place. We introduced a Code of Practice, which is a set of principles that organisations need to follow when deciding whether or not to engage in information sharing schemes.

Ten years on, the frequency of data sharing and the ability to combine and analyse data is greater than ever. There's an ever-increasing pressure on businesses and governments to use and combine data to innovate, to improve services and to find new solutions.

I know that many of you in this space feel that pressure every day and I believe the pressures are most acutely felt in the public sector where there's often large depositories of data available and where increasingly governments are looking to establish data analytics capacities to take advantage of their data.

And privacy officers are on the frontlines. You're being put in a situation where you are often holding the keys to the castle. Sometimes it's not clear how the law allows information sharing and without clear guidance on how to make it happen, it can very quickly feel like that you as the privacy officer is the department of no, which can create all sorts of problems from workarounds to misconceptions that privacy is a roadblock to innovation or a roadblock to change.

But there is a way. Privacy regulators around the world have been showing that it can be done by issuing clear guidance that explains how information sharing should work within privacy and data protection laws, working with government to ensure that information sharing goes forward and is done in a responsible, legal, transparent and ethical way. If information sharing is to be successful, it should be clear and transparent for the public. It must be matched with strong safeguards and it must be monitored with robust and independent oversight.

The final thing that I want to mention today is our office's new international strategy. The ICO has always been a global player, but we feel that now is a time to step up our game. We want to make sure that we are globally connected, not just for the future of data protection in the UK but we also want to make sure that we play our part for global privacy rights and protection worldwide.

Think about how much easier your job can be when you can connect with like-minded people and think about all the work that you'd have to do if you couldn't benefit from the research or the lessons of your peers, many of whom are facing the very same challenges. What if the person next to you had already thought about those battles, had already fought the battles or wanted to fight them with you, and that's the power of collaboration. And it's one of the lessons that I learned early on as a regulator in Canada that there's power in numbers, and working with other regulators, with industry, with government and civil society, we can address the challenges ahead and the solutions we come up with are better for it.

The ICO continues to invest in our relationships in Europe and we will continue to do so with the transition out of the European Union. But we're also building relationships with privacy and data protection regulators around the world and this includes colleagues in the Asia Pacific. The UK has been an observer at the Asia Pacific Privacy Authorities of which Queensland is a member and we're pursuing deeper lengths with the Commonwealth through what is called the Common Thread Network. We're involved in global privacy enforcement networks where we engage in joint enforcement actions with other agencies. We're also working with international organisations to develop global standards around privacy.

But we can't do it all. We need to be selective in order to be effective. And I've established a new department at the ICO responsible for international strategy and intelligence who will lead this work and we'll be investing in our time and effort to forums and in relationships that best support strong data protection for UK citizens and consumers, while enhancing our global reach.

In closing, I would say that the challenges are big but the world is small. We must work together for the common issues we face, defending the principles of privacy and data protection for citizens. That means understanding global trends, but also we need to understand what's happening in our own backyards. I think what we all want, the regulators, industry leads, governments, privacy officers on the frontline, is to find solutions that work in the public interest and if we want to find those solutions we have to engage, we have to understand each other and we have to have conversations, sometimes tough conversations about where do we go from here?

So, congratulations to the conference organisers, you're doing your part to get that conversation started, and thank you for letting me to be part of your conference and have a wonderful day. Thank you.

**(Applause)**

**COMMISSIONER RACHAEL RANGIHAEATA:** We thank Elizabeth for her presentation.

I would now like to welcome Ms Roslyn Bell, Assistant Commissioner at the Australian Productivity Commission, to the stage to discuss the Commission's recent report on data availability and use. Please welcome Roslyn Bell.

**(Applause)**

**ASSISTANT COMMISSIONER ROSLYN BELL:** Thank you for the invitation to talk to you today at the start of Queensland's Privacy Awareness Week. It's a real privilege to be here with you.

I'm mostly going to talk this morning about the Australian Government Productivity Commission's recently released report on data. The report was released just last Monday and was a culmination of a 12 months public inquiry for the Australian Government into the frameworks that govern Australia's public and private sector data availability and use.

But, firstly, before I get on to that report, I want you to think a moment about your car. It might not be a very sophisticated model but these days it's most likely got a computer in it. That computer might record technical details about the vehicle, battery status, temperature, oil gauge, for example, possibly even details about how and where the car is driven, average speed, fuel usage, et cetera. If it's pretty sophisticated, you might collect information about how many people are travelling in the car, the weight of the luggage in the boot and how you drive it. It possibly has Bluetooth connectivity to your mobile devices.

Experts suggest that as cars increasing include sensors and cameras and become more automated and connected, each vehicle could potentially generate up to one gigabyte of data per second. One gigabyte of data per car per second.

Your car might be talking to its manufacturer, to your devices, to other vehicles, to the road infrastructure, to your insurer. Sound futuristic? Well the Tesla model S, already on the road in Australia, communicates in realtime with Tesla Headquarters in Palo Alto. Telstra last year announced successful trials of vehicle to infrastructure technology in South Australia.

Who currently has the rights to this data? It's really not that clear. So, in the absence of that clarity, someone will step in and take control and claim that data, and it's probably not the individual whose data it mostly is about.

Imagine the possible risks to individual privacy, security and personal safety that can arise from such data. Imagine too what can be done with that data to improve road networks, road safety, public infrastructure, vehicle maintenance, emergency preparation and management.

It's a balance. It's one that must be talked about and weighed up. It's no longer realistic to think that such data can be locked up. It's an asset, it's not going to be locked up and it's not at the moment, and nor is that really desirable either for the individual or for the community. But we do need workable safeguards and a framework that builds community confidence in data use.

In light of such examples, it's perhaps not surprising that global estimates have the amount of data rising expedientially into the future. So, how are Australians dealing with such massive data generation collection and use? On a worldwide scale, we're big adopters of new gadgets and technologies. As consumers, we provide a lot of data about ourselves. We have the second highest uptake of smart phones in the world behind South Korea as a proportion of the population and the most popular apps in Australia on those smart phones tend to be the apps that deal with maps and navigation. The ones that generally require you to know or reveal your location.

So, Australia's information gate is wide open for better or for worse. Seven in 10 Australians use social media. Eight in 10 have a customer loyalty card and most have more than one. But only five in 10 Australians are fully aware of what data is actually collected about them and how it's collected. The same proportion try to provide false information to obtain online services and we're told that that's really a failure in the big scheme of things. Four in 10 read online privacy policies, and I'm quite surprised it's that high. But only one in 10 avoid social media due to privacy or security concerns.

Overall, the Productivity Commission Inquiry found that there's a general lack of understanding of who has what data and what's being done with it. Typically, some key businesses are finding commercial opportunities from the data that they hold. Woolworths, for example, overlays data that they collect from their car insurance crash database with their rewards database to refine their insurance product offerings. I'm not sure many customers of Woolworths are aware of that.

And there's a presumption that government agencies are doing a lot more with their data than what's currently being done. There are some great examples. The Tax Office, for example, prefills individual's tax returns and the ATO has estimated that this actually saves households about 535 million dollars per year.

But equally there's some quite annoying gaps and they're often caused not by privacy legislation but by highly restrictive provisions in other legislation and a general culture of uncertainty about what's actually possible and what's allowed. In the private sector, for example, the movement of patient data within the health system, even between floors on the same hospital, is archaic in many instances. There are countless examples of data that's collected in one part of government that's not available in another part. The Commonwealth Government holds Australian Business Register data, Child Care Assistance data, and I know the States and Territories sometimes have trouble getting hold of that to make use of it for the better of consumers and households. Similarly, the States and Territories hold data that's not shared with the Commonwealth or with other States and Territories.

Australia compares very poorly on an international scale with its public sector data, especially data on program spending and legislation that's actually machine readable, health data that reveals the performance of specific services. Other countries have released that data but we typically don't. They can release that data because they've already had the discussion about the safeguards that are needed around it and they have in place frameworks that people trust and understand.

While we rank relatively okay on the implementation of open data policies, we have our websites where data's put up regularly, it tends to be updated infrequently and it's not really in formats that are very useable. So our data's having low impact. Maybe we want that, but we probably don't.

So, turning again to the Productivity Commission Inquiry report that was released last week. The productivity Commission's recommended that it's time for a total rethink about the frameworks that govern how Australia's data is handled. As the previous chart showed, the public sector has slipped behind the rest of the world in its data usability and yet we still burden

households and businesses with collecting this data and then waste the value that's inherent in it.

Consumers are treated as a data source but they're given few rights or controls over data that they've provided or that's been generated about them. And incremental changes to date have failed to deliver a culture in which data sharing and release is possible and people are assured that the necessary safeguards will be maintained.

There's two facets to the Commission's recommended approach. The first is a comprehensive right for consumers to data about themselves. The second is a scalable risk based approach to the sharing and release of other data held by governments, by publicly funded research bodies and private sector entities that collect data under taxpayer funding or regulatory licence. Private health insurance companies come to mind here.

The scope to provide consumers with a greater say on the handling of data that's sourced from them is considerable. The Productivity Commission recommended that Australia's consumers, both individuals and small businesses, be given a new comprehensive right to their digital data. It's for businesses, small businesses, as well as individuals, because the 95 per cent of Australia's businesses that are SMEs are also consumers themselves.

Back to the car example that I mentioned at the start, just because a vehicle is owned by Bell Start-up Pty, rather than by Miss Bell, should not diminish the right to joint control of the data that's generated by that vehicle; for example, for car maintenance or insurance purposes.

Consumers would no longer be just a source of data, they would rank equally with data collectors, businesses and governments, in being able to trade and use their data. This right would reinvigorate competition in markets and give consumers and citizens power and confidence in data use. They'd be able to exercise real choice.

So what does the right include? In addition to being able to request edits to their data, consumers would be able to direct that a copy of their data be provided to a third party, maybe

a competitor or maybe the provider of a complimentary product. In some ways, it's similar to some of the things that were mentioned about the EU.

What data would be included in that right? What could get transferred to another business? A lot of the submissions from the public provided to the inquiry focused on the question of what data should a consumer be able to transfer? The Productivity Commission considered that the scope of digital data available to be accessed and transferred under this right would best be developed and agreed by participants in each industry. What's relevant in the health sector is, of course, going to be different to what's relevant in banking. But the ACCC was recommended to approve the agreed scope and if agreement could not be reached within an industry, then a broad default definition would apply.

Inquiry participants argued about whether imputed data should be included; that is, data that's been created by a business data holder that can't really be linked directly to an individual consumer. That too could potentially be subject to industry negotiation.

Now turning to the mass of data that's currently held in the public and private sector, apart from the consumer data. A substantive element of the recommended reforms is a structure that provides legal and institutional capability to share and release data by dialling up and down the access controls to manage risks, recognising that different types of data carry different risks to different people at different points in time depending on how the data is to be used and the environment in which it's used. Existing privacy provisions would remain in force.

This framework, it was recommended, would be created at a Commonwealth level but be national in operation. Some of the new structures, for example, the central accredited release authorities that were recommended, might actually be existing State and Territory bodies. Certainly, the recommended trusted user arrangements were intended by the Productivity Commission to put State and Territory data users on a more equal footing in their access to Commonwealth data.

And the contribution of State and Territories to the recommended new national interest data sets was intended to be on an opt-in basis. States and Territories should be able to choose

to be involved or not. With Commonwealth funds used to maintain some national interest data sets, improved capacity to link these to other data, simpler legislative arrangements for access, the Productivity Commission considered that States and Territories, some of them at least, might find participation to be an attractive option.

We anticipated that the recommended approach would require within governments strong and consistent leadership, leadership that remains steady in the face of missteps. States and Territories are a very important part of the recommended approach, not only can you be beneficiaries of wider data accessibility, but you also hold much of the country's skills and expertise in some nationally relevant central data.

So, we recommended an ambitious timeframe for reform implementation. Some early action would allow State-based linkage units to link with Commonwealth data. Industry negotiations for the consumers' comprehensive right should be started as soon as possible and the bulk of reforms would ideally be in place within the next two to three years.

Other developed countries have been making the long-term commitments necessary to give their communities confidence in safeguards on data handling. It's time now for us to rethink how we want the mass of data that's out there to be handled. Events such as Queensland's Privacy Awareness Week are crucial to promoting such a rethink. Thank you.

**(Applause)**

**COMMISSIONER RACHAEL RANGIHAEATA:** Thank you, Roslyn, we greatly appreciate you travelling interstate to join us today. It's a very interesting report and it's available on the Productivity Commission website. I think it will be interesting to see the developments from hereon and the implementation and the involvement of all of the stakeholders involved.

Our next speaker is Senior Director of Digital Architecture and Information Management, Mr Corey Moynihan from eHealth Queensland, who will talk about the use of personal information and delivering health outcomes. Please make Corey welcome.

**(Applause)**

**MR COREY MOYNIHAN:** Good morning. It always gets tougher the more speakers that are going on because quite often you start to watch the glazy eyes. So if you do feel you need to stand up please do so. I will, however, try and make this topic as entertaining as I can.

I'd probably like to start first by sort of saying I guess there are a few of people in this room that might have had a busy weekend for those of you in the information management business. I certainly know that eHealth Queensland did and if Andrew's still in the room he probably did too. But rest assured it is well and truly under control.

Before I start the presentation, I'll just pose a little bit of a statement to you and I think it goes to a lot of the things the speaker's already said. Most of you, in fact I would suggest nearly all of you in this room, expect the best possible care you can get from your healthcare providers, whether it be public or private. That delivery of care requires a sharing of information.

Gone are the days - well, we've still got a few hospitals but we're progressively reducing them - where the paper chart was handed around and we had lots of people running around trying to find your chart, read the chart, see if they could read the chart, because if anybody's dealt with a pharmacist trying to read a doctor's prescription you'll know what I mean, analyse it and then take appropriate steps to make sure you get the care you need. If they then need to consult an expert, of course, they then used to have to go and take the chart to that expert, consult with that expert, the expert would read the chart and then maybe you would get cared for some time that day.

Now days we've got digital hospitals, or are progressively improving them, including probably the first very large quaternary style full digital hospital in Australia over at PA. That hospital at the moment is doing three million medical records a day, 250,000 scripts a day all electronically, which is just huge.

I'd also like to say as we start to move towards genome medicine it will only get bigger when you look at it because the average genome's about a petabyte to actually manage. So it is getting bigger and bigger and bigger.

So you're demanding that we provide quality of care by sharing. Absolutely. We get it. The second point though is share with care. You would expect us to share it with your nominated GP, but potentially not somebody else who's got a passing interest that just happens to dial up that doctor and they might just want to look at it because they've seen you in the headlines. So, therefore, we take steps to also manage the sharing of that data, and that really gets to the point, I think, around informed consent, capacity to make informed consent, quality of data when we do share it in the first place, particularly when it comes to health data, we can't get it wrong. It does kill people. One of the leading causes of death in hospital is the wrong medications and that's generally an information problem. And, of course, confidentiality.

So that's really why I'm up here today and talk to you about this sort of stuff, it's to put some - I guess some tangible lessons on there and also talk to you a bit about what we're doing to try and get that balance right. And it is a real balance right. I'm sure we'll make mistakes as we go along, we're human, but we are certainly progressing a very strong digital agenda.

The government last year recently introduced an investment strategy. It's worth about 1.2 billion. Some discussions with government about how long that's to be executed on, but that is pushing us very clearly into a digital direction to do all of the things that I just spoke to you about.

Okay. Because I work for Queensland Health a bit of brochure - oops, sorry, that's not - I'm not Philip. Hello. And my presentation's not coming up. Okay. Not a problem. What I might do is I might just talk to you briefly about eHealth Queensland and Queensland Health more broadly.

So, the first thing we need to know if we don't do anything to do with data and we don't manage our way of delivery models of care in new and innovative ways, then by 2045 we'll have spent the entire State's GDP just on health.

When I look at the prevalence of cardiac disease, it's increasing at 8 to 9 per cent per annum. We obviously don't have the cardiac staff that would be able to support that without doing something differently. We have an increased incidence in cancer. Most of them, by the way, having better results. Unfortunately, lung cancer is increasing. Less than 20 per cent are alive after five years with lung cancer. To me that's alarming. We also have a huge increase in obviously chronic disease and other things. So that means to me that we still need to have more work to do, not to mention the differences in life expectancy between us and those that live in more rural and remote communities.

So, I want to put that in around four key planks for health. The first one is we obviously have the patient at the centre of everything we do and to that patient we want to promote wellbeing to the greatest extent possible. So, what do we do to provide data to that patient? Well funny enough we don't have to do anything. Who here's got a Fitbit? Yeah, quite a few. All of you have got phones, little apps with health things on them. A lot of people are already using some of those types of things to monitor their data, their heart rate. If you're a gym junky, if you ride a bike, you know how many ks you burnt; in fact, you tell everybody about it. Yes, my wife's one of those.

Okay. Great. So how can we actually provide you a better experience closer to the coalface, and I'll talk to you in a second about an innovation that we've got to trial some of that sort of stuff, to actually take that data and add it into your normal health record.

Obviously in delivering healthcare itself, so we've gone digital, so what, we certainly don't want the doctors and nurses to spend a lot of time treating the computer and not you. So how do we make that data so that they can have a consult with the Registrar for Cardiac when they're in the Emergency Department in realtime? We have that today. If you go into the Emergency Department, not that you want to but if you have to and you are presenting with a cardiopulmonary resuscitation issue, then don't worry because they'll be speaking to the cardiac experts in the cardiac wards in realtime looking at your records, making notes, making orders, issuing medicines and so on. So that's progressively happening across the State.

Equally though we want to connect healthcare and so in connecting healthcare it's not enough for us to just provide you the best possible care within a facility. What happens when you leave that facility? What happens before you present at that facility?

One of the biggest causes of Emergency Department block is actually from respite care - and Friday and Saturday nights - but mainly respite care outside of those times. So how can we make it so that those people who need care can get it as close to their place as possible? So if you've got an elderly parent, grandparent, and they are in respite care, how can we have a realtime consult with those people in their bed? That makes them feel a lot more comfortable. I don't know if you know a lot, but a lot of people when they get older and come to an Emergency Department, they think maybe this is it and, in fact, quite often that can then cause huge amounts of stress on that individual. Also, it's very expensive because generally it involves an ambulance visit. They have to come to Emergency. Emergency is not cheap, they are expensive places, but for a very good reason, they are lifesaving.

So, what if we could sort of provide a Telehealth consult augmenting their normal GP call-in service whereby that GP could provide that service, not even at the bedside necessarily but with a registered nurse taking the required measurements, you know, zooming in, having a look at their skin, those types of things. Because in a lot of times it may just be a urinary tract infection or some sort of other thing that could be treated with fluids or antibiotics. So that's much better for the individual and much cheaper for the State.

So it's those types of electronic database transactions we need to have.

Probably one other point I'd like to make. I was speaking with a Cardiothoracic Surgeon the other day and he said, "Corey, I don't know why you make us type in all this text in clinic." So he's already gone beyond the paper chart, he's out there. He says, "I video everything. I don't write notes anymore, it's all video." Think about that challenge in terms of the data points we just spoke about before as progressively the source of truth and evidence is actually video. He uses that so he can show his patients what he's doing, for those that are interested, he uses that for research, he uses that to train his registrars and he uses that when he gets sued.

So I look at that and say, "Wow." But he's sort of saying, "No, no, you haven't seen anything yet," because, of course, robotics is here.

I think I'm back online. I think I've spoken about those.

I just want to touch briefly on the health service direction and I think I've already spoken about most of them. Pursuing innovation's probably the one I haven't spoken about so I'm just going to get to this quickly. I can assume you can all read. In fact, I know you can all read. So if there's anything there of interest, please come and see me after the break, but it is really important for us.

Sensors are very, very interesting. Trip and falls, a really major cause of healthcare concerns in facilities again. But we're getting to the point now with RFID tagging and other things like that, when we can know where that patient is. Now that's nothing to be scared about, it's actually a really good thing if you're in hospital, and so if there's a trip risk in your record we'll monitor you. So there's no more of somebody falling over in a shower and nobody coming to get them because they can't reach the emergency call button. Things like that. That's using data for good.

I've spoken about Telehealth before and I've spoken about the digital records.

A fun thing. Patient master data. All right. A lot of us, we're into data. My information managers think I'm into data, although they laugh at me when I try and describe it. Patient registration, patient identification is key. Now remembering we're a public health system. We'll treat you. I don't care who you are, we'll treat you. Therefore, how do I identify who you are? Also people are human, so if you enter data into a record, fine, but what if I have to enter it into two systems, three systems, four systems? What's the risk of me getting your date wrong? What's the risk of me getting your name wrong? Rosemary, one word or two? And all of a sudden two digital records. So digital records are - in fact, record management is more important in a digital age than it's ever been in a paper chart because now that error will not just be in that hospital, it will be all over the State. And, in fact, we're the biggest contributors to the My EHR, or the My Electronic Health Record, that's a national endeavour. We provide more discharge summaries than any other State. In fact, we're the biggest contributor outside, I think, Medicare itself in terms of raw data. So if we get that wrong you've got two records.

So, again, data quality is key. A lot of that is individuals, a lot of that is health literacy.

Electronic Care Plans and images, two very key things. We want to desperately share images anywhere. It's a key recommendation from our clinical senate. But, again, what we don't want to have to do is have clinicians take photos using their camera and then send it to somebody else via Google Mail and say, "Hey, what do you think of this?" Wounds quite often happen that way. So how we can take a photo securely of somebody's wound, send it to a wound specialist and get that information in their chart and get it diagnosed, treated.

Pursuing innovation. I think it was mentioned earlier by a previous speaker about our data sets. I agree, we don't really - we have a number of data collections. The Cancer Registry is probably the most well-known one. We have a whole bunch of them. Are they updated as often as I'd like? No, I'd like realtime, particularly when, again, we get into genomics. I want to be able to provide the best population health data source I possibly can because that will allow our clinicians to provide the best possible results to everyone in this room and their families. So that's where we're at.

How can we do it though managing confidentiality? De-identifying. Should we de-identify? When do I we de-identify? Now we have processes and regulations and rules around all this, so don't panic, but that's really important.

We do have a Clinical Data Repository. It contains everything we know about everybody in one spot. Guess how secure that thing is. Pretty secure. In fact, so secure I can't even get stuff out of it. That's maybe a problem.

I always like - we put the patient, or whatever, at the centre of everything we do. Really quickly, just a couple of key points here. I think the main one for me is actually from our customer. I was speaking to one of the Health Consumers Network representatives for our children's organisation and she said, "I'm sick and tired of being my child's Chief Information Officer. Can you just not keep all the records, share them with my GPs, share them with my physiotherapists? Ask me before you do and I'll let you know, but please do when I say yes." And that requires in an electronic age the ability to send and receive securely. There is a way

to go but we are certainly moving towards it. We are already doing a lot of work with the Mater, for example, Mater Children's and LCCH, to share information around neonates. That's already having great results in terms of not needing to prick a baby two or three times when they move between intensive care and theatre for blood. These are the sort of things that make, again, a real difference, but we're sharing it securely. It's only between us and Mater. Not only are there agreements in place, we monitor everything we do, so we know who's entered what data when. We audit it. We require pretty much very good log-in and authentication and we don't just throw it out there.

So this to me is a little pause for a second slide. I'm a firm believer, particularly given - you would have seen the earlier point from my boss, my Director-General, Michael Walsh, about "information and technology and the third person in the room", that information in a digital world, it's always been the lifeblood, I mean this is how we know about you and what we know about you, the metadata if you will, but our staff really are the heart of our organisation. They make or break the health system. But they can't do it without good information. So it is the lifeblood of Queensland Health and, in fact, I'd say it's the lifeblood of the health system. What we need to do is make it pump better, faster, more efficiently and not leave it on Warfarin.

I think you know about this. There are huge amounts. I mentioned before about the issue around genomics and video outstripping text for recording. It's big. It's going to get bigger and bigger and bigger. Again, in a lot of cases it's a no-brainer. In a lot of cases it's actually hard to manage. How do we get that video off that phone, that device into a picture archiving system, associate it with a patient and make it available. Say, for example, if that patient comes from Thargomindah, how do we make it available to their clinician in Thargomindah from a tertiary care facility here when every time it rains maybe the internet drops out? So these are the types of things we need to deal with. We have a funding plan for Thargomindah if anybody actually lives there or has family there.

A couple of slides. Just to mention that we do collaborate widely. Interestingly for me you'll find a lot of them are actually other government organisations, which I think is fantastic. We're going to do more and more that. We're doing some stuff around Black Lung, we're doing some stuff around wayward children, and so on, but more and more collaboration is required, particularly with our research intuitions. But with the prevalence of disease being what it is, we can't keep up so we need to rely on each other.

Just to give you an idea - and, no, that's not that virus we were talking about before, that Ransomware - this is from our cyber security folks. So just to give you an idea of how often we share, it is a global business of healthcare and we do provide data to people and from people all around the world.

A quick word on opportunity. This is happening right now. West Moreton, which is based out of - its main facility is out of Ipswich, it's already with the consent of its patients taking some of that personal data, we talked about preventative health, this is actually from once they've left hospital. Effectively the top 5 per cent of patients consuming that HHS's budget are what we call - they readmit. They are our sickest. So what we're trying to do is have realtime monitoring with them and an ability for them to dial-in, have conversations on video conferences, take monitoring devices and actually say to them, "Hey, look, we're noticing your insulin's sort of spiking a little bit here, we're noticing your heart rate's a bit irregular, why don't you come in, or we'll send a nurse out to see you," rather than them waiting and going to arrest, then be in emergency, then into a ward, and of course their heart muscle's also dying. So this is a way we make people feel better, live longer and also keep the cost down.

This is the healthcare of the future in my book and we've already seen in the first three months of this trial a reduction on $50,000 per patient on average. So sizeable cost reduction, but more importantly less readmissions of those people. So that's good for them. We've actually had a lot of them actually lose weight, for example, if they were presenting with cardiac positions because they know people are watching. It's a bit like when you have your physical trainer, you're always a little bit more diligent if you know you've got to go back and justify it to your physical trainer after a workout. Same in this case.

This is really exciting for me. Implanted devices and genomics. For those of you who are big readers of the British Medical Journal, I am, I'm a bit sad that way, but implantable devices and the use of genomics for me are the way of the future. They will allow us to be very, very targeted in terms of delivery. You might have also seen, you know - who here uses Dr Google by the way? Is there any? Do you want to admit to that? Right. You've all got cancers, you're all going to die. That's generally what I do when I use Dr Google, everything leads to cancer. But there are a lot of products out there in terms of artificial intelligence now that are getting better and better. They're actually helping clinicians diagnose. Now the clinicians make the

diagnosis, it's around those systems helping them make the diagnosis, again, given the prevalence of disease.

Who here has got children? Yeah. Okay. Phenergan. Mmm. Can be a friend of parents. Who here has the opposite reaction, their children have the opposite reaction to Phenergan? Anybody? Yes. Yes, a few. Well, guess what, with precision medicine, not just for Phenergan, but for anything else, we'll know that before you actually give the child Phenergan and then sit on an aeroplane next to me for the next five hours.

So these are the types of things that I think make a real difference, because a lot of medication has no benefit or worst the bouncy child on the right. So let's be very tailored in delivery of care. I say that particularly true for those with cancer. Cancer drugs are up to $100,000 a dose. If we can use DNA therapy and better target chemotherapy drugs, we can give you the right drug so you don't feel crook, you don't lose your hair, or if you do it's going to have a real benefit for you.

So these are the way of the future for us, but that's all data. Now not only do we know where you live but we know what your genes are. So if that's not very scary in terms of insurance companies and other things, you're not as afraid of it as I am. So, again, when we start doing that sort of stuff, in terms of the risk quotient that was shown before, that's incredibly high risk so we'll wrap that up in gold, don't expect to see that in a data set any time soon.

Timely. With all those opportunities I spoke about before, a little warning, this is from our security folks, and I'll probably talk about the malware stuff. You can see there you can build your own Ransomware kit. Don't suggest you do that. But the thing I like about this is it actually tells me that - not wanting to scare anybody - but your medical records are more important to these people than your credit card details. Generally one follows the other by the way, once they've got one, they'll ask you for the other, or they'll try and reuse bitcoin. But anyway.

So we are very conscious of the need to secure in an appropriate way medical records of every single one of our patients and their associated demographics. And, indeed, that ME

Care example I was talking about before, we encrypt in transit and at rest and we also split the data into two different areas. We also host with vendors that are much better at them than we are and they can actually stop State-wide attacks and comply with the highest DSD requirements.

So that's how serious we take patient data. It doesn't say anything's happened, you know, you can still have people that have access to the systems and potentially do the wrong things, but it's a lot harder to do and I guess that's the risk I was talking about before.

So a few key fundamentals and then I'll get out of your way. To me privacy and security is really important that we maintain it. We need to balance it. Consent is all important. You need to not just have implied consent but informed consent. Even if there's statutory obligations that allow you to share, which we certainly have under certain criteria, you are in control of your data, you're the patient, you tell us where it needs to go and how, but at the same time, back to the start of my argument, we want to share it with your other providers, of course you need to let us know who they are, but that way you don't ask the same questions all the same times, get blood tests about seven or eight times from every different facility because they don't have your latest blood test result. Public and private.

Metadata's a big one. I've spoken about that. To me that's sort of really, really key because that's exactly how we manage your data, but it's also how we know about what data to manage and share. That's actually something that I think needs a bit of work.

Okay. We've got a plan. I'm going to rush through this because I'm a little bit behind time. I just wanted to give you an idea. These are things around basically connecting people up. So those people in Thargomindah can actually have connectivity, optimisations about making sure you've got systems at point of care with the appropriate information controls in place, including a lot of significant work around health informatics uplift. We've partnered with Heiser to provide certified health informatics competencies for all of our staff as we go for a digital investment. More and more we need to make sure our people are across it. As I said before, data quality's all important in a digital system.

And the last one is getting to really that sexy stuff I was telling you about, implanted devices and genomes. We are at different stages in different facilities here. So if you're at PA they're already telling me they're transforming, get out of my way. If you're at some of the more rural and remotes they're still on paper. So we've got to get them off paper. We've got to provide them with a system at point of care and remove some of the feelings of isolation that some of those clinicians have.

I'm just going to skip through the next slides. I will encourage you after this just to have a little bit of a look if you're interested, but I am running a little bit overtime, so I apologise for that.

GP Access I think's really important. I will spend just a second there. We are talking about providing information to your general practitioner. Most people expert that's already happened but it doesn't. It will come through in paper. We are the biggest provider of discharge summaries again everywhere, but we need to know who your GP is. And the legislation recently changed that made it a prescribed system so we can now actually provide it to GPs and the project to make sure that's done properly, securely, safely, with your consent, is actually just finalising now and we're hoping to have it in place in the next few months. So that will be quite exciting in terms of starting to do that full longitudinal patient record.

Don't worry, we will do privacy impact assessments and security and other things about that. We do that all the time.

I think I've spoken a lot about digital therapies and analytics already, so I won't spend too much time on that, except it's bigger and bigger and bigger, particularly with the prevalence of disease, we want to get on top of it and I actually think this is the real ways we can make a change to your personal health.

So takeaways. The first thing, I think, is we can really - we're all data managers, so the data revolution is here. It is our lifeblood for health and so you'll find our health information managers in the hospitals, no longer are they running around playing with charts, they're now actually have conversations with clinicians about the data, they're dealing with things like patient identity, provider identity, those sort of things. So a significant uplift and value-add

from those folks. It won't be easy. There's a 1.2-billion-dollar investment for a reason. It is complicated. Again share, not share, when to share.

The last point I'm going to focus on out of all of that is that it's not ICT. I think most of you know that but a lot of people outside this room don't. A number of clinicians who come to us and sort of say, "I just went to a conference, there's this really great app, can you put it in for me?" And then we say, "Sure, but don't you want it to connect to stuff? How do you want it data entered and so and so? Have you trained your other doctors and nurses on how to use it? Does it meet their requirements as you shift from one specialty to another, say from emergency to an inpatient ward? Does it work in surgery? Can it send a discharge summary to a GP? Can it accept an electronic referral to a specialist?" Those types of things. So it's 80 per cent business change in information management. All of those information management business driven requirements are key. The technology's the easy bit. Relatively.

So, as I leave you, I just want to leave you with one little thing. If you want to know more about any of that, including the bits I had to whiz past, we've got a lot more detail, it's available online, it's just on old school, so I brought a hard glossy with me. Please have a look at our new digital vision. It does describe what we do. It aligns very nicely to the 2026 Queensland Health Vision, which funny enough aligns to the whole of government one. Take a chance to read it. We know it's not easy to manage data, we will manage data better, we will share it and thank you very much for your time.

**(Applause)**

**COMMISSIONER PHILIP GREEN:** I finally get to talk. I think we've launched. Welcome. I'm really happy that we've had such a good show up and we've had a fantastic line-up. Thank you, Corey, that's innovation in motion, I think. Queensland Health, you're doing some amazing things. You know, there are challenges and risk to be managed and you guys are on top of them.

I know your CEO and it's something - I had a big smile on my face a couple of times today. "Privacy by design" I think got mentioned twice by preceding speakers, but we can see privacy by design and that design led thinking, I think, coming into your health services delivery. You've had a bad rap over some ICT projects in the past, but, you know, frankly I've got a bit of trust and confidence seeing what I've seen of your organisation. You know, our team gets in there and does audits on some of the health services. There's some leading examples of information management and data being put to good use. So really thank you for that presentation.

We've had an amazing line up. It's hard to even begin to start to summarise some of the things we've heard today. Elizabeth really led off with some amazing connectivity and international connectivity stuff and GDPR and then we saw Productivity Commission recommending data portability. So interesting connections there and challenges no doubt, but I think that is incredibly important for us to be looking beyond our borders. Data has no borders. That's the key take-home message I think we need to be mindful of today. I'm going to be preaching that on ABC radio later on and I think the Productivity Commission report is excellent timing for us to add to the debate. The ASX Cyber Security report showed that corporations, the top 100 corporations in Australia aren't managing data and cyber security very well. We can all learn from each other.

One of the things I've tried to do since, you know, my stump speech last year, I really didn't have my feet under the desk for PAW very long before we launched the event, but I would like to really emphasise that we need to work together, we need to learn from the research community, and I'm glad to see some of you are here today, the privacy practitioners and professionals, the legal profession, the ICT people, you know, the Productivity Commissions, the economists, to be able to understand the value of data and to put it to use and to have the public debate about where we draw the lines.

It was great to hear the Attorney-General's being very mindful about these things and, you know, very confronted, I think, with the Youth Justice problems that we've had and criminal justice problems. So, the wicked policy problems that governments are trying to work on out there every day, use that data and use that data connectivity to better advantage where consumers and the public expect it, and, you know, that movement we've all heard "joined-up" government and "one-stop shop" in Queensland for longer probably than the UK even,

doing that right in a privacy, respectful way is difficult, it takes a great deal of judgment and debate and collaboration.

I'm not going to speak for the full 15 minutes, I'm going to let you go and get out there and practice and get into it. I'd really like to thank my team, the TSR team that have put together the event today. Fantastic work. Steve came back from holidays today just to be here. But, Emma, you've done an amazing job and I know - in Steve's absence while he's been on leave, but great job.

Thank you to my privacy team. You know, lots of great input. We're hoping to do some cool things for the rest of the week and if I can get you to all get out there and keep the message going for the week, but not just for the week, we've got to think about privacy every day and data security, you know, the breach over the weekend that went worldwide for the Ransomware attack just shows how connected we are, how susceptible we are and that everybody needs to think about privacy and data security.

It's not just, you know, an ICT shop or a privacy officer's job, it's CEOs, boards and management, and you'll see those ASX boards out there right now brushing up, I think, post ASX Cyber Security report.

The My Health Project, and some of those other projects nationally, I think, are great ways for States and Territories to collaborate in this area.

Just this last year we worked a very, very long time trying to get NAPLAN across the line for launch. There was going to be a trial of online NAPLAN in the country in a number of the States and Territories. We worked very hard with that to try and get that across the line. Ultimately the system didn't get up to speed. But that was a national project with State and Territory involvement and it goes to show how important it is for us to network with the States and colleagues and Territories.

Timothy Pilgrim is launching the Australian week as we speak, I believe. He's going to be releasing a data set on community attitudes to privacy. I think that'll be a really good, important

piece of work that we can all use in our daily work to highlight how important privacy is to the public.

One thing, it's still forefront, you know, the youth of the day do manage privacy settings in their electronic world. I'm seeing that firsthand. I've got a grade fiver who's got an iPhone and an iPad and a laptop, scarily enough, but I'm seeing even amongst his friends an awareness of privacy and, you know, concern not so much of his parents monitoring him yet because, you know, that's part of the ground rules of which those devices get put out, but it's and upon which the schools put out their device as well. But I do believe our, you know, future is in good hands.

I'd like you to all take a minute, "pause for privacy", "care when you share". I do believe we're doing important work and it's going to become more important in our daily lives to consider and engage on this as a consumer, as well as in our work as an employee.

One other thing I'd like to urge you to do, the Attorney's going to be out there, I believe - and she didn't mention this today - but there's a commitment from the Queensland Government to enact a Charter of Rights. I believe if there is a Charter of Rights that privacy will get a mention, as well as other human rights. I do believe privacy underpins a lot of those other fundamental things, for employment, for housing, for, you know, your criminal history, or whatever, and for your health records. You know, the data that makes us individuals and upon which we engage in the community I believe is incredibly important. So engage in that process as consumers and public.

And the legislation review as well. Elizabeth mentioned the UK Act, or EU law was based on '95 legislation, or legislation dating back to then when we had brick phones. Our 2009 Act is basically built on those same foundations of the '95 law. You know, Commonwealth legislation goes back to '88 but has had several resets along the way. There's a great chance for us in Queensland to be information leaders. I do believe we lead the way on RTI in transparency and there will be some interesting debate, I suspect, with the Attorney out there under pressure to release in the Youth Justice system more data and, you know, more information. That tension's always going to exist, drawing the lines and drawing the balance correctly. I believe there is great benefit in the community discussing them and consulting more broadly on them

and that's playing out in the Local Government arena as we speak. Some of you may have seen my little tiff with the Moreton Shire Council on audio recording. That's still playing out, so I won't speak too much about that, but I do believe that those issues need to be aired publicly. Transparency and accountability and ethics, and all of our rules, particularly as public servants, but the community does need to be involved. We need to have good public debate on those things to see where we draw the lines and what is important in terms of getting the balance right for the data that we sit on.

I've always said government probably is about 10 years behind the private sector in terms of use of data and valuing it. Malcolm Compton has actually put out a model for how we should value data, that we make it more important for companies and for governments to take it more seriously. I do believe the awareness has risen to the extent where people are taking it seriously now and it's great to be here speaking about it and to have such a great line-up.

So, thank you again for coming. Thank you, Commissioners, as well and thanks for the support. And thank you, Rachael, for stepping in. I know you've been unwell but thanks for chairing and emceeing. And thanks again to the team and for the RTI team too who did the front desk so the privacy team could attend. So, have a great morning and maintain the rage on privacy.

**(Applause)**