Transcript

PRIVACY AWARENESS WEEK 2021 LAUNCH

Queensland Information Commissioner, Rachael Rangihaeata

Good morning everyone and thank you for joining us for the Queensland launch of privacy awareness week 2021. My name is Rachael Rangihaeata and I'm the Queensland Information Commissioner. I would like to begin by acknowledging the traditional custodians of the land on which we meet today and pay my respects to elders past, present and emerging. I extend that respect to Aboriginal and Torres Strait Islander peoples here today and joining us on the live stream. I would like to welcome a keynote speaker, Mr Alan MacSporran and Miss Waveney Yasso performing acknowledgement country with us today. I would also like to acknowledge the many members of the community, Queensland government agencies and other organisations engaging with us about privacy today. Thank you also to Bundaberg Regional Council for hosting a special event today with many other councils and our Principal Privacy Officer joining Council up in Bundaberg today. We know many people are joining us on the live stream from across Queensland, Australia and abroad. A very warm welcome to you all.

This Privacy Awareness Week, privacy regulators around Australia and Asia Pacific have come together to call on the community and organisations to make privacy a priority today and every day. Our privacy is increasingly important to us as individuals as government custodians of the community's personal information, protecting privacy must be a priority to build and maintain trust and confidence. We recognise that personal information has an increasing value and is essential to our economy and the digital environment, the delivery of vital services and in our daily lives. During the pandemic it has also been critical to the Covid 19 response and recovery. We live in an ever expanding digital world of technology at our fingertips 24/7. Understanding how we protect privacy with evolving opportunities and challenges is critical. It is not possible to set and forget.

The human element is always important. A strong culture of privacy awareness and privacy by design can help prevent irreversible and significant harm to the community, including our most vulnerable members. This year's theme is particularly timely given the increased use of technology and devices at home, work and school during 2020, 21.

PAW 2021 reminds us to protect and respect personal information because if you don't, the consequences can be significant and far-reaching. And of course privacy is everyone's responsibility. As individuals, we must take steps to protect our personal information by securing our devices and accounts and being aware of what and where we share our information. Government agencies and other organisations must take the privacy by design approach assessing risks early minimising risk from the outset and building them into an ongoing risk management system.

Agencies also need to use training and technology to help prevent privacy breaches caused by human error. These actions are important, not only during privacy awareness week but every day at work, home and in the community. We have a great event for you today, but before we officially get things underway some housekeeping. Please turn your mobile phones and other communication devices to silent. Toilets are located downstairs on level zero or via the lift and to the right. The Edge is part of the State Library of Queensland and visitors are governed by the State Library of Queensland policies and standards. The State Library is a Covid safe venue with a Covid safe site plan in place, encouraging visitors to maintain a physical distance, 1.5 metres wherever possible, especially when queuing on exit.

Thank you for celebrating Privacy Awareness Week with us across Queensland and beyond, both in person and joining us on the live stream. If you'd like more information about Privacy Awareness Week or privacy rights and responsibilities in Queensland, please visit our website. We have a range of pool resources including tips, sharable images and content. We have also released new agency breach notification resources on our website to help ensure appropriate agency responses to minimise harm. Shortly we will hear a video message from the Attorney General and Minister for Justice, the Honourable Shannon Fentiman MP currently in Longreach for community cabinet.

First were very honoured to have a wonderful and talented artist to perform an Acknowledgement of Country this morning and song form in the language from the Quandamooka Coast. Please welcome Miss Waveney Yasso to the stage.

Acknowledgement of Country

Performer, Miss Waveney Yasso

(sings song 6.28 – 7.01)

This is a song that I co-wrote to pay respect to my ancestors, the elders and the traditional owners of this land. The local tribes of Mianjin, which today is called Brisbane and the Turrbul, Jagera, Malanjali, Yugambeh, Jinibara and Quandamooka people. My mob is from North Queensland on Birri Gubba country, a small town called Bowen on my father's side. I have aboriginal ancestry. We are descendants of the Koolgumbara people, the saltwater Murri's off the coast of Mackay and I also have connections to the Quandamooka people here in the Bay Area. Also have heritage from Tennor Island of the South sea and Vanuatu and on my mother's side I have Scottish ancestry, which basically just means I'm a bit confused. It means that I've got freckles and curly hair, but it also means that wherever I go acknowledge the traditional owners. I thank them for their stories, for connecting us to song lines. I thank them for their knowledge and for keeping this country beautiful.

We're really lucky today in the physical sense. If you're here in the physical sense to be right on the, the beautiful Brisbane River, which is known as the Muntagurie, the beautiful creator spirit, the rainbow serpents, it's always lovely to see. In this song I sing language from the island of Minjerribah. Minjerribah is known today as North Stradbroke Island. The language of the Quandamooka people is Jandai and I've had some words translated by a beautiful song and dance man from over there. The words that I sing are (ui/indigenous language spoken) which means mother earth she sings and dances, mother earth is alive and mother earth plays a really integral role in a lot of First Nations cultures all across the world. I'd like to extend my acknowledgement to any First Nations people who might be amongst us. We have thrived. We have survived. We come in all different colours, different shapes and sizes and with different voices and I hope today that wherever you are all the good spirit.

(sings song)

Attorney General, The Honourable Shannon Fentiman MP

Good morning and I'm sorry that I can't be with you in person today. Queensland's theme for Privacy Awareness Week this year is make privacy a priority and that is exactly what Queenslanders expect and it's what our government believes in and what we're

committed to delivering on. This includes a right to privacy and reputation in our Human Rights Act. I strongly encourage everyone to value and respect personal information to build good privacy practices into routines and to actively manage privacy risks in the workplace and in our personal lives. A recent survey found that privacy is a major concern for 70 percent of us. It also found that almost 60 percent of us have experienced problems with how our personal information was handled in the past 12 months. Most of these concerns related to unwanted marketing communications or having personal information collected when it wasn't required. Community confidence in how we manage information is critical. If we don't have public trust, Queenslanders will be reluctant in sharing the personal information when it's really needed. During Covid the need to be able to conduct rapid contact tracing meant Queenslanders were required to share their personal information more than ever before. When going to a café or restaurant or even a sporting event.

But privacy concerns and a lack of public trust can easily undermine the success and uptake of new initiatives. As Queensland's Attorney General I have administrative responsibility for over 200 Acts, including Right to Information Act and the Information Privacy Act. These Acts touch on not only information privacy, but privacy, communications, territorial privacy and surveillance. You may know that our law reform commission are looking at civil surveillance and the protection of privacy was tabled in June last year. The civil surveillance report recommended that invasion of privacy be repealed and replaced with a draft surveillance devices bill. The Queensland Law Reform Commission has also been asked to report on workplace surveillance and the Palaszczuk government will seek to protect the privacy of Queenslanders with tougher, stronger laws to tackle the increasing pitfalls of the surveillance error.

I want to finish by thanking everyone here for their efforts, in particular the staff of the Office of the Information Commissioner in making privacy a priority right across government. I wish you all the best with the event and the rest of the week.

Queensland Information Commissioner, Rachael Rangihaeata

Thank you to the Attorney for her message and also to Miss Waveney Yasso for a moving performance. As you know we have Mr Alan MacSporran, QC, Chairperson of the Crime

and Corruption Commission's here with us today as our PAW 2021 launch keynote speaker. For over 30 years as a barrister and prosecutor Mr MacSporran has been part of important legal, public sector and social reform in Queensland. From the Fitzgerald enquiry in the late 1980's to the floods commission of enquiry in 2011/12, and the 2015 review of the Queensland Greyhound racing industry. As chairperson of the Triple C since 2015, Mr MacSporran has initiated public hearings into the states local government sector and the Queensland prison system, both of which resulted in large-scale legislative and procedural reform. The Triple C's most recent public hearing, Operation Impala examined public sector agencies management of confidential personal information. In February 2020, the Triple C released its report, Operation Impala, a report on misuse of confidential information in the Queensland public sector.

This report examined critical issues about how the Queensland public sector protects the community's personal information and protects individuals from harm, including some of our most vulnerable members. Mr MacSporran will speak to this report today and its recommendations in his keynote address titled "I trusted you with my private information, government powers and practices to prevent misuse of personal information". Please welcome Mr MacSporran to the stage.

Crime and Corruption Commission Chairperson, Mr Alan MacSporran QC

Thanks very much Rachael and I'd also like to commence by acknowledging the custodians of the land on which we meet and to pay my respects to the traditional owners of the past, present and emerging. I thank particularly Rachael for not only her introductory remarks, but for the kind invitation to present this keynote address. This topic as it turns out, has been some years now a particular interest of mine because I think you cannot overemphasise the importance of this topic. A lot of people downplay it by saying look we didn't have authority to access the information but we were very, very curious, it wasn't for a nefarious purpose, we just wanted to satisfy our curiosity. I mean that's the most benign example you can give of unauthorised access to information but even that most benign example shows how fundamentally undermining of public trust it is and that is where it does the most harmful of course.

Our positions as employees in the public sector are built on a foundation of public trust.

For most of us to do our jobs effectively and efficiently we need confidential and often sensitive personal information from members of the public, it's just necessity to do our jobs. In line with growing community expectations the people's personal information should be respected and kept private by any agency authorised to collect, store and use it. Employees within public sector agencies need to ensure that information is handled with a commitment to be responsible with that information, maintaining privacy should always be our priority. Whether you're a nurse collecting information about a patient's medical history, a teacher recording personal information about a student or an administration officer collecting information about a member of the public's address and financial details to access a government service.

Nearly all of us will come into contact with another person's confidential information during our working career.

This information may be sought and exploited by commercial enterprises seeking market advantage or an extended customer base or even stolen or appropriated for use in criminal activity, such as identity fraud and cybercrime, something that is regrettably becoming more common on a day-to-day basis. Data theft and breaches of information privacy are now a global concern for government, legitimate private sector operations and the people whose information is being improperly accessed and/or disclosed. For this reason, an increasing range of legislation and other safeguards, warnings and management requirements are being put around the collection, storage and use of confidential data. To provide our functions and services to the public will rely on the public to provide us accurate information. If the public lose trust that we as the custodians of information will not handle it appropriately then their willingness to disclose information will diminish naturally. The obvious consequence being that the performance of functions becomes less efficient and reliable. And I'd argue ultimately will break down altogether if you can't trust people to respect your privacy and confidentiality.

The public places an enormous amount of trust in us to guard their confidential information and to only use it for appropriate purposes. We must be careful and diligent not to breach that trust. Just a couple of examples you know a police officer for instance who again for the most benign reason of simple curiosity accesses the database which in the police

service is called QPrime, it's a massive database as you'd expect and they accesses it and it's discovered and that becomes a black mark on the disciplinary history, that same police officer he might be a witness in a very serious case, could even be a capital offence of murder, defence counsel will be the first to use that benign example of dishonesty to undermine that officers credibility and that can have as you'd expect devastating impacts upon that serious prosecution.

Likewise doctors, nurses, health workers who might for the best altruistic reasons access the database to follow-up on a patient who's no longer under their care but who they're desperately interested in the welfare of. So the motives are pristine but the purpose is unauthorised. And I'm told that the, the move to have all health records moved to an electronic database which is a very important initiative of public health and safety initiatives, saving lives, if that information is at your fingertips electronically. The greatest obstacle to that happening is the lack of trust in the public to allow their data to be collected and stored that way, and their lack of trust it will be stored confidentially. So you see how again even the most benign examples can fundamentally undermine very important health and safety issues whether it be in the Health Department, the Police Service or even the Education Department, likewise so again you cannot overemphasise the importance of this topic.

The theme of Privacy Awareness Week this year is make privacy a priority, very appropriate for the reasons I've been saying and I unequivocally support that agencies and every employee should commit to this as a matter of significant importance to ensure we uphold public confidence in what we do every day of the week as part of our ordinary daily work. Some data for you. Between July 2014 and December 2020 allegations of misuse of confidential information have been in the top five allegation types of suspected corrupt conduct. During the last six and a half year period allegations of misuse of information equated to approximately 20 percent of all allegation types during that period. Unfortunately, allegations about misuse of confidential information have been steadily rising since 2017 and during 2019 and 2020 it has been the most commonly reported allegation type of suspected corrupt conduct currently. Almost one in three allegations of corrupt conduct are about misuse of confidential information. That has to stop frankly, it can't be allowed to continue.

The Commission noticed this trend emerging in 2019. This was one of the reasons the Commission determined to hold a public hearing in relation to the issue. The hearing was known as you've heard from Rachael Operation Impala and it was borne out of the recognition of the rising number of allegations about misuse of information. The other reasons we determined to hold the hearing were because it's a matter of significant public interest, a guarding against misuse of confidential information has been a strategic priority of the Commission since 2016 and the Commission considered that scrutiny of these issues through a public hearing will promote public confidence in units of public administration's capacity to manage confidential information.

We also thought the use of public hearings would generate discussion and opportunities to understand why these allegations are occurring and the public hearings would generate an opportunity to develop solutions to the issues identified. And for the purpose of the public hearings we selected seven large public sector agencies, namely the Queensland Police Service, Queensland Corrective Services, two Hospital and Health Services namely Mackay and the Gold Coast. The Department of Health, Transport and Main Roads and the Department of Education. These departments weren't chosen to name and shame them by any means. They were simply chosen as the larger agencies where the data we could analyse was largest so they had the best samples for to use to identify trends and to generate discussion about possible solutions. But I can ensure you what we found and what we understand to be the problem is common across the entire public sector, and I suspect from what I've been told across the private sector as well, it's a very widespread insidious problem.

We examined the agency systems and cultures to find out how public servants were able to access people's confidential information without any legitimate reason and why they continue to do so despite the obvious issues it can cause. We also wanted to understand how agencies responded to misuse of confidential information whether by disciplinary action or by referring matters to the police or to us for consideration of criminal charges. During the hearings we heard from a variety witnesses from agencies, subject matter experts and some members of the public who had been the victim of misuse of

information. The aim of Operation Impala was to help all public sector agencies build systems and cultures that will ensure the information the public gives to these agencies is properly stored and protected.

So what we found We found that agencies were at different levels of maturity in this area, their approaches and sensitivity to risk seem to depend on the type of information they collect and how strongly the individual agency emphasises the importance of protecting people's confidential information. It was comforting to see that several agencies had several practical initiatives to protect the confidential information they stored and these included automated internal audits, for example. A system used by Queensland Health known as P2 Sentinel which identified potential improper access to the integrated electronic medical record database, it's a very important initiative. Additional system access controls in relation to people who were identified as vulnerable. Significantly vulnerable people, including domestic and family violence victims and high profile individuals were identified as being a particular risk of having their information misused and when accessing government services.

Transport and Main Roads spoke about customer record suppression service. We found disturbingly that whenever there is a high profile media event such as a police arrest of a high profile individual or a high profile individual getting into some strife or other and you checked the police service database you had a spike in unauthorised access. Be it people just because they could wanting to find out what that was all about, and no doubt being able to go around and tell their mates and family members, and so forth. What that front-page story was all about. You know seriously so it's a serious issue and it just can't be allowed to continue.

So why do employees access confidential information despite the number of initiatives and training already available to staff. There are still a number of staff who access confidential information from improper reasons. The main drivers were identified as a personal interest, curiosity, I've already mentioned. The desire to obtain a material benefit for themselves or another, even if it was only just having information. The existence of relationships that could make some employees more susceptible to misusing confidential information and personal circumstances of an individual at times of high levels of external

stress, particularly in their personal life often led to abhorrent behaviour by employees. They might be reasons but none of them. none of them are an excuse for this behaviour.

Concerningly one of the things that we learned during the hearing was the lack of understanding by some employees in relation to the reasons they could lawfully access information. We heard a number of employees thought that access to the agency's databases was permitted for a whole variety of personal reasons, whether it be checking on their own profile or information holdings themselves to examine those of other family members or people they were entering into a relationship with or simply to satisfy their own curiosity about something they'd seen in the media. In a world where more information than ever is at our fingertips through Google searches looking up people on Facebook, Twitter or Instagram. More and more people are choosing to publish a lot of information about themselves and that's often done without any appreciation of the risks you're placing that data of yours in. It can get challenging for some people to distinguish between what they do and have access to in their personal life compared to how they can and should access confidential information available in their workplace.

For this reason, a strong culture which regularly reinforces the importance of privacy has never been more important. I'll come back shortly to how agencies can embed a culture of privacy later, but for now I urge you to think about when was the last time you spoke to your staff or your peers about the importance of privacy in your workplace. That is one of the keys frankly, to be talking constantly about these things. This is not a case we have a policy where you tick and flick. Where you have an acknowledgement by people they understand have read the policy, that's not enough. It's a cultural thing you need to live it and speak about daily especially as leaders to emphasise the importance of this.

The three most consistent risk areas contributing to employee misuse of information were identified as firstly managing large volumes of information that is vastly diverse in nature. Secondly, ensuring consistent approaches to information security across devolved entities and thirdly maintaining currency with advances in technology that have the potential to impact information security, access control systems and/or database usability.

So what are the affects of the misuse of information? Operation Impala found that the detrimental effects of agencies from a misuse of confidential information, included

financial liability for the actions of those employees as well as adverse community perceptions of the Queensland public sector. The hearings also detail the significant personal consequences on victims of misuse of information. Such misuse was found to have ongoing and long lasting affects including stress, feelings of vulnerability, financial loss and frustration with the difficulty of obtaining redress or adequate compensation. And, of course, fundamentally undermining their personal trust in the public sector's capability to look after their sensitive information, that is the most damaging personal affect that this issue has in this space in my view.

So the recommendations that arose out of the Operation, we published a report which included 18 recommendations for agencies throughout Queensland. It's very important to emphasise that these recommendations were not just intended for seven agencies that gave evidence during Operation Impala. They were directed at all public agencies to ensure that Queensland's confidential information is handled and stored using best practices. The recommendations can be divided into four distinct areas. Firstly, privacy frameworks, a range of recommendations aimed at improving systems and privacy frameworks in Queensland agencies and these included that agencies ensure all computer databases that contain confidential information, have unique user identification log-ons, that they regularly review and monitor user access changes due to staff moving to different areas within the agency or employee separations. That they ensure that additional control measures are implemented for vulnerable people. That they ensure that agencies have simple and consistent ICT policies and procedures that explain when it is appropriate for staff to access and disseminate confidential information and they develop and implement a robust education and awareness package to clearly explain the agency's policies and procedures in relation to reasons and circumstances in which employees may access confidential information. This was considered particularly important as I said because one of the recurring themes identified from the case studies was the fact that employees often stated they were unaware that the reasons for which they accessed information was not permitted.

To reinforce this training the Triple C also recommended that agencies adopt regular information privacy campaigns to keep the issue of privacy in front of mind when staff are undertaking their work. Information Privacy Awareness Week is an obvious time for staff

to be reminded of their obligations about handling confidential information appropriately. But other opportunities throughout the year should also be used to reinforce these measures. The regular reminder to staff will help foster a strong culture about the need to protect confidential information. And lastly improve prevention and detection systems, which include the ability for automated or regular manual audits of data access, highly visible and well published internal audits are considered a strong deterrent strategy to ensure that information is only accessed for appropriate purposes. If you think there's a fair chance you're going to be caught out it's a deterrent to you doing it in the first place. And prevention is always better than cleaning up a mess later.

So we've been requesting updates from the seven agencies involved in Operation Impala and I must say, pleasingly, most recommendations have either been implemented or in the process of being implemented. For example, a number of agencies including Queensland Health in the Hospital and Health Services have developed a process for identification of idle users, that is log on accounts that have not been recently accessed and have this information available to management to cancel inactive system access to prevent misuse. In policy reform Queensland Corrective Services have updated and developed three new policies for their employees about access management, acceptable use and a set of acceptable use standards for employees. This instructs employees on the appropriate circumstances in which they can lawfully access confidential information and empowers them to access information in the performance of their functions confident in the knowledge that are doing the right thing. We found during another public hearing into the prison system Operation Flaxton that every prison officer around the state had total access to every prisoner's confidential information on their database so you can be a prison officer in Far North Queensland but have complete access to a Brisbane prison prisoner and of course there was no basis to allow that, it was just an oversight frankly in their system and they've taken huge steps to clarify and strengthen the security of their system and limit access to those who need to know the relevant information.

Next there were awareness campaigns. The Gold Coast Hospital and Health Service last year developed a privacy awareness communication plan for staff that outlined an ongoing campaign to build awareness of relevant privacy issues. Elements of the campaign included a communication brief to leaders, fact sheets and frequently asked

questions sheets, screensavers, posters and other content on their Internet. A video outline employee responsibility and many other like initiatives. Similarly, Transport and Main Roads reported that they continued to implement privacy awareness campaigns which they been doing now for a number of years, to their credit.

Improve detection and prevention systems which are important. The Department of Education revisited its original process and definitions of vulnerable students and applied and adapted the vulnerable person's definition published by Queensland State archives and drafted an education specific definition. The definition provides guidance to a cyber security team when scoping, developing and implementing technical controls on information systems containing records of vulnerable people. This robust approach to safeguarding confidential information regarding vulnerable people is on track for full delivery by the end of June this year so I'm very, very happy to see that initiative.

And then improved employee accountability. We recommend several changes to ensure greater employee accountability to staff who improperly access confidential information. These recommendations included where employees are detected doing the wrong thing investigations and disciplinary responses should be timely and proportionate to the seriousness of the conduct. Where an employee accesses another person's confidential information, particularly if that information is then disclosed to another person, this should be taken very seriously. Agencies should make it very clear to those people that this type of conduct will not be tolerated and will result in disciplinary action and in appropriate circumstances referral to the Queensland Police Service for identification and investigation in relation to a criminal offence.

And to reinforce this message the triple C recommend the use of detailed, but identified case studies where action has been taken by the agency against an employee for misuse of confidential information. It's important that, this is not about naming and shaming and that's why these case studies can be de-identified. But they serve to underline the message that firstly the management of an agency will not tolerate this behaviour. Secondly, they take it very seriously and thirdly they are doing something about it and here's the result to send a very powerful deterrent cultural message. And hopefully that leads to more people thinking twice about exercising their curiosity.

In relation to the referral of appropriate matters for investigation, we noted that there was an inconsistent approach between agencies in relation to whether the particular type of conduct were being referred to the QPS for investigation of a criminal offence. Several reasons were identified for this including uncertainty about the type of conduct which would constitute a criminal offence. At present, most offences of misuse of confidential information, a prosecutor using the criminal offence of computer hacking and misuse which is an offence against section 408(e) of the criminal code. However, there are several aspects of this current offence which have given rise to uncertainty in its application. For example, the title of the section does not make it clear to public officers that accessing confidential information to which they ordinarily have access can be a criminal offence. If they do so for an improper purpose. Similarly, evidence given during operation Impala showed that employees who had password access to confidential information failed to understand the use of that password to access the information could still be a criminal offence.

And the definition of the word benefit in the offence itself has led to various judicial interpretations including the gaining only knowledge from the confidential information is not a benefit. We think clearly that's wrong but you can see that the offence provision, including its title computer hacking is not really fit for purpose. So to deal with those issues and other issues which we noted in the report we recommended a new criminal offence be created to deal with issues of confidential information by public officers and creating a new offence in the criminal code will leave public servants in no doubt as to the seriousness of accessing or disclosing confidential information, without a lawful reason. If the recommendation is adopted and we certainly hope it will be, it will mean these types of issues will no longer be viewed by public servants as minor indiscretions or misguided curiosity. A new offence will appropriately classify this type of conduct as criminal in nature and in our view, this aligns with the seriousness and consequences of accessing and disclosing Queenslanders confidential information.

So legislation reforms. The next category of recommendations related to legislative reform to improve the framework within which the privacy laws are applied and enforced.

One of those recommendations related to a new criminal offence as I've mentioned, we hope that's taken up. The other areas of reform included the provision of additional functions and powers of the Office of the Information Commissioner, such as requiring mandatory notification by agencies to the Office of Information Commissioner when there is a privacy breach. The Triple C agreed with the OIC's evidence during Operation Impala that this would complement and bolster its existing audit and the valuation functions currently available under the Information Privacy Act. It's an important measure to ensure affected individuals are made aware of any privacy breaches which may impact upon them and allow them to seek remedial action. Importantly, we noted that limited avenues are currently available for individuals affected by privacy breaches. It often results in individual having to litigate against large government entities which result in a significant power imbalance and time and expense for individuals even assuming they can afford to run such an action and of course for most they can't. For this reason, we consider the Office of the Information Commissioner should have own motion powers to commence its own investigation into compliance in relation to privacy laws and also act as a friend of the court and to intervene in QCAT proceedings where appropriate and with the leave of the court.

In improved outcomes for victims. Lastly, a series of reforms to improve those outcomes for victims included strengthening some of the existing protections for victims in the Information Privacy Act and ensuring the victims have access to adequate remedies in the event that their privacy has been breached. I think that's a very important initiative because too often the victims in this, in this series of issues are ignored and of course they have the most direct personal impact, which is often devastating. Another important recommendation was made in the Operation Impala report is for agencies to create a privacy champion. We recommended that a privacy champion comprised of a senior officer within the agency capable being able to influence the executive management level within the agency. The purpose of this position within agencies is to be an advocate for privacy in relation to the operation and planning of any significant changes proposed for the agency. I'm very pleased to hear the Privacy Commissioner is this week commencing an inter-agency privacy champion forum to ensure that issues and best practices shared between Queensland public sector agencies. It's another way in reality of making this

issue the forefront in every agency's response to this problem.

Six of the seven agencies involved in Operation Impala have created a privacy champion within their agency. I will now talk briefly about the harm from privacy breaches. During privacy awareness week it's also timely to remind the entire public sector about the very real harm which can be caused for privacy breaches. People can suffer a wide range of personal and financial affects because of a privacy breach. I want to focus in particular on privacy breaches that can have a significant impact on a person's safety and well-being. The key thing to remember in relation to the disclosure of confidential information is that once an individual discloses that information to another, they lose control of who else will get access to the information and most importantly what that person will and can do with it. At times some people in the community unfortunately have to go to considerable lengths to hide their location and personal information which can lead to their identification from others who pose a threat to them. We've seen the significant impact of domestic violence all too often in the media of recent times, and although these particular matters didn't involve a breach of privacy, it's a very real risk that if a victims confidential information is disclosed, it could end up in the wrong hands and have disastrous consequences.

While I realise this type of behaviour relates to a very small number of individuals who mis-use this information, it is incumbent upon all of us to take all reasonable steps to prevent this from happening. It's the similar stories and it is the, although it's a very very small minority who do this they have a disproportionately large and devastating impact on public trust and confidence in the public. So the fact that they're a minority doesn't allow us to relax in any way at all, in fact it just has us, or should have us on higher alert to reduce that minority further. During the public hearing it was noted that although individual agencies approaches may differ, it was evident that they all, they all viewed very sensitively any loss of public trust in their operations, that they understood the damage that can be caused to people who are impacted by the actions and that they're committed to improving their systems.

So what can individuals and agencies do to prevent the misuse of confidential information. Firstly, and obviously a culture and tone from the top developing and maintaining an

effective information privacy culture relies on the adequacy of internal policies, education, awareness campaigns and practical training. The use of deidentified case studies as I mentioned earlier, was found to be a very useful educative and training tool as they provided real-life scenarios that help staff interpret the intention of policies and improperly apply them in the real world. A common issue identified was decentralisation and the challenges it created for lead agencies in guiding and monitoring their smaller devolved entities. It's very important that we have a across-the-board approach that doesn't have massive variations that aren't justified by different requirements of different entities. A consistent approach will lead to a better outcome on every occasion.

Sitting above all the policies, procedures and education is a culture that permeates the agencies. What CEOs and executive managers do and say within their agencies plays a significant role in relation to how all staff carry out and perform their functions. For this reason it's incumbent upon executive managers with public sector agencies to set the right tone about the importance of managing privacy. This can be done in a variety of ways as we all know and the methods adopted often depend on the make-up and profile of the workforce you manage. The one truism that is consistent across all sectors is that agencies which have strong values and zero tolerance for corruption will call out poor behaviour and create a workforce that has pride, in its agency's reputation. The desire to protect an agency's reputation is critical when it comes to managing privacy. A poor report card when it comes to managing privacy will result in a falling reputation for any agency.

Now I believe, although as Impala demonstrated there does need to be, there needs to be security within IT systems to make it more difficult to improperly access databases. But the solution is not IT generated. This is truly a behavioural issue. It's a cultural issue and the culture simply has to call it out and it has to be recognised across the agency wide that this behaviour should not be tolerated. You know for instance in the police service the former Commissioner and the current Commissioner sent out emails on three occasions between them over a number of years that drew the line in the sand and said this is unacceptable behaviour. It could well be career threatening if you continue this from after this day and whilst we've seen a decrease in the frequency of unauthorised access there is still an unacceptably high level of unauthorised access. And whilst we

haven't done a detailed study right across the public sector, the figures I've spoken about already in this presentation would suggest that that's not unique to the police service. So there's a delicate balance between making the IT system secure enough to mitigate the risk of unauthorised access, but not so secure that it prevents or makes some impossibly difficult necessary information sharing, that's the other side of the equation. Those of us in law-enforcement but it applies more generally across the entire public sector need to share information.

You can't underestimate the importance of information sharing, we see it everywhere. Disastrous consequences through inadequate or non-existent sharing of information. The classic example is 9/11, the terrorist attack at New York, the review of that event established that all of the United States security agencies all had pieces of the puzzle that had they shared it would have alerted them to the plot was unfolding and was successfully executed. They didn't have the entire story because they didn't share. Whether that was through mistrust, the difficulty of it or the lack of understanding of the need for it we'll never know.

We see it here in our youth justice and child safety systems. These infant deaths we have various agencies invested in that process necessarily having pieces of the puzzle which had they shared or brought to attention lives of those young individuals may have been saved. It's important so that has to be taken into account when you're looking at an IT system that you still have to share information, but you have to do that appropriately and is not rocket science frankly, it's just as we say here culturally understanding what you can and can't do, not just from the policies and procedures, but from case studies that are published by your agency to help you understand the practical application of those policies. And just protecting as you should the reputation, the important reputation of your agency which will do so much to enabling the public to have confidence in your ability to properly protect their information.

An effective deterrent message must be based on consequences and sanctions that reflect the seriousness of offending. A disciplinary response must be timely and proportionate as I said before, to the offending. And I mentioned earlier, one of the recommendations was the creation of a new criminal offence in response. The two

mechanisms that is disciplinary and criminal for deterring improper access need to work hand-in-hand. I can tell you my experience in the police service because we've had a campaign running about that. Our approach was to reflect the seriousness of this conduct was to, in every case of the unauthorised access the assessment and ultimately investigation of those matters should commence with a criminal investigation and, where possible, if the evidence was sufficient charge a criminal offence, simply to raise the bar about how serious this behaviour was.

Now I'm saddened to have to report that an issue which I thought was a winner has proved to be less than effective and reason being that, well there are two reasons. One is if you charge someone criminally goes into the court system which regrettably takes forever so if you wanted to send a deterrent message quickly and proportionately you don't get it through the criminal process. I'm not being critical of the court system, it's just a fact we have to live with. Secondly when it gets to court we found that the courts are imposing sanctions that don't reflect the seriousness of this conduct. Again I'm not being critical of those judicial officers involved, it's simply a fact that they don't appear to regard this sort of conduct as seriously as we do, and they should we would say. It is possible to change sanctions sentencing levels by presenting evidence about community expectations and so forth but again that can take an extended period and often will defeat the purpose you're trying to achieve in having the rapid deterrent message sent.

So what I've now done is we have now a concentrated effort or not the criminal offence unless it's something like selling information to criminal enterprises, which is so serious it can't be ignored as a crime, but in the routine complaint we get in this area we're going to escalate them and have been escalating them internally in a disciplinary sense. The idea being you have more control, it's quicker, you can raise the sanction because if you've sent a message out which we are going to do in the police service and we think it should be done across the sector more generally that from today, your choice, you're in control of what you can and can't access. If you do it after today, you can expect an increased level of sanction internally and it could even be career threatening, your choice. And I think moving forward in that fashion we hope to achieve the appropriate deterrent message and to mitigate the risk of this corrupt activity. I don't think we can ever expect to eliminate it. Although there's no reason why it shouldn't be eliminated, but we can

certainly reduce it to a manageable level hopefully. So that's the current plan I'll be reporting on back to you in sometime to come about the success of it.

So the agencies responses to misuse need to be simple and precise in order to accurately convey the intended messages to staff and to ensure they're understood. So the common theme I mentioned before was about decentralisation. the challenges that creates for lead agencies in guiding and monitoring their smaller devolved entities. If a employee decides to do the wrong thing, the consequences for his or her actions should not come as a surprise to them. A robust disciplinary system internally includes ensuring employees are fully aware of the consequences of their actions should they behave in a way that is not consistent with the values of the agency, and that's just about education and training awareness.

Like many things in life prevention is always better than the cure. As an independent agency we're dedicated to combating major crime and reducing corruption for the benefit of Queenslanders and our agency produces as you'd expect lots of resources to help you prevent corruption in your own agency and we have our corruption allegations data dashboard that is updated every six months with allegations data that you can drill down into to see what issues may be impacting your agencies, including seeing how many allegations are made about this topic. Misuse of confidential information. You can access this data, in a visualised format on the Triple C's website and I encourage you to do so.

If you don't subscribe for updates from us I encourage you to do so. Our corruption prevention resources are practical and can be delivered straight to your inbox or if you prefer you can follow Triple C on Facebook and Twitter to get our latest news, who would have thought. Beside the point that I don't use any of this because I can't but my team are all over it. So you've got no excuse for not accessing information you might need, and of course if all that fails, you can come to us directly in person.

In closing, I urge everyone here to find at least one thing you can do to make privacy your personal priority during privacy awareness week whether that's talking to a colleague about it or asking staff if they got any questions about how to manage confidential information or getting on the front foot and initiate privacy awareness campaigns within your agency this year. So again, can I close by saying you cannot over-state the

importance of this. It's an agency public sector wide important issue, but ultimately it comes down to individuals believing in it, engaging in it and promoting those values every day of your working lives and it being mainly a cultural thing it won't happen overnight, but you can make a difference and I urge you to do so. Thanks very much.

Privacy Commissioner, Phil Green

Well I don't know if can say anything more. Thank you Alan, that I think gave us some extremely good examples of, and food for thought in terms of what we can do to make privacy a priority. And he has foreshadowed one of our big initiatives, the creation of privacy champions network, we are heading that off tomorrow and it's really heartening to see that a lot of the departments have taken that extremely seriously, they have appointed high level executives and I think that's critically important to driving the culture that we are all trying, the cultural changes that we are all trying to achieve.

Some of those stats from the Attorney General and from Alan and from Rachel are really not surprising. Another step from the OAIC survey work is that 85 percent of people expect government to do more about protecting their privacy. And I think that is absolutely critical as we accelerate the use of technology and also service delivery through electronic means and this last year has really seen this acceleration. It's actually seen an increase in human error as well which I think is no surprise with more of us moving online and you know simple things like losing your device or having it stolen because it wasn't properly secure are really important things from the ground up in organisations. We put out a resource as part of Privacy Awareness Week to look at human error and the ways we can avoid it and I think that's absolutely critical.

But the real pointy end as Alan said and it's really good to have the Triple C in our corner is the serious harm that can arise from the misuse of data are real and they can involve criminal and corrupt conduct at the very far end. And that common occurrence and the number of complaints is disappointing and I think we all have a responsibility to do our part. The launch of Privacy Awareness Week by the Commonwealth Privacy Commission and co-presented by the UK Privacy Commissioner highlighted how multi-disciplinary approach is really necessary in the privacy space. We look, and are increasingly looking to other laws such as the criminal law or consumer and competition law as part of this

puzzle of solving improper use and the technological challenges. The Human Rights Act in Queensland I think is a really important partner for us in this privacy space as well as information management in general.

The surveillance laws also that the Attorney General has talked about and the (ui) commission is really a critical part as well in gaining that trust and making sure that it isn't misused so that public confidence is lost. Information sharing is probably one of the biggest roles of the privacy team at OIC. We were recently involved in the police unions youth symposium on how we can better exchange information. So the public expects government to be joined up and also can lose trust where we don't appropriately share. So it's getting that balance right. And if you have the cultural settings right I think that that will to do good and share information appropriately is absolutely critical. From our part and the OICs part our focus this year particularly in the privacy is on trying to get a contemporary and also consistent privacy legislative framework. We are on record in parliament, we are on record in the enquiry into Operation Impala and I must say it was a bit daunting getting cross examined by the Triple C Counsel but it's really good to see there was some great recommendations coming out of Operation Impala and that they are being implemented by some of the agencies that were involved but also more widely. And I think that's the critical thing. That wasn't just about, and just like our audit work at OIC, it's not just about the agencies that are there but it's showing that OIC moving in its role from a regulator to an enabler to actually get good practices happening and not to just use the big stick.

Alan has got the biggest stick in town I think but there are other laws as well in law enforcement and the QPS as well involved in that enforcement action. The fines are probably smaller then they should be in our jurisdiction at present but they are going to be increased at the Commonwealth level and I think the Commonwealth is currently looking at legislative reform as well to even further their powers and further their investigative powers, but also their fining powers. And their own motion power I think would be important in the Queensland context as well as Alan has mentioned.

I think we are over time so what I'm going to do is just do some thank you's. So thank you to the attorney general who's not here but certainly it was great to have her support

and showing how privacy is a priority for her as well. Alan you have given us a great sort of synopsis of initiatives that all of us can take into heart from the bottom up and the top-down in agencies and we can all play our part. And really thank the TSR team at OIC. Adeline, Steve and Lesley for putting this event together. It's been great to actually have a physical event as well as a virtual event. And g'day to Bundaberg and Lemm and the folks up there, really good to have you online. Really exciting that we can do something physical as well. Make it bigger and better next year. Lastly I guess as far as the playbook for privacy is concerned I would urge you all to make privacy a priority. Not just today, not for the week but every day, thank you.