CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19/0006

DAY 9 - FRIDAY 22 NOVEMBER 2019
(DURATION: 2HRS 20MINS)

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KIMBERLEY SAUNDERS
W Witness – PHIL GREEN
LR Legal Representative – N/A

CA I call Mr Phil GREEN.

PO Mr GREEN.

CA I'll let you get settled.

W Good afternoon.

PO Do you prefer to take an oath or affirmation?

W Affirmation, thank you.

HRO I solemnly affirm and declare.

W I solemnly affirm and declare.

HRO That the evidence given by me.

W That the evidence given by me.

HRO In these proceedings.

W In these proceedings.

HRO Shall be the truth.

W Shall be the truth.

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

CA Mr GREEN, you were provided with an attendance notice for today?

W Yes, I was. Although I'm here very voluntarily. Thank you, that's it.

PO Exhibit 175.

ADMITTED AND MARKED EXHIBIT 175.

CA I tender that document. Mr GREEN, you are the Privacy Commissioner for the Office of the Information Commissioner in Queensland and you were appointed to that role in December 2015?

W That's correct.

CA Prior to that appointment you were the Executive Director, Small Business for the Department of Tourism, Major Events, Small Business and Commonwealth Games and were in that position since 2008.

W Correct.

CA You, prior to that, held policy roles at the Department of Transport and in the Department of Premier and Cabinet?

W Yes.

CA You hold a Masters of Laws Degree majoring in Technology Law and Information Privacy from the Queensland University of Technology?

W Correct.

CA And also a Bachelor of Arts in Economic Law from the University of Queensland?

W Correct.

CA And you are on the Cyber Security Steering Committee?

W Yes, correct, for Queensland.

CA Could you please provide an outline of the complaints jurisdiction of the Office of Information Commissioner and the advisory function for agencies?

W Certainly. Our functions under the Information Privacy Act include the complaints jurisdiction. It's probably a third of the business that the privacy team works on. It's not a high volume. Over the past years we've been averaging around 50 to 60 complaints per year. The last year's figures have risen to almost to100, and that trend team seems to be staying around that for this year so far.

It's, as I say, part of our role, we do spend a lot of time on the education and training functions which the Information Commissioner's outlined earlier, that is spread across all of our functions, but privacy particularly we spend an awful lot of time on the training and education functions. On the advisory front we spend an awful lot of time on new proposals and projects involving privacy, privacy impact assessments where agencies do them, although the performance there in terms of who was doing them is less than ideal. We do advise on legislation that has privacy impact or potential privacy impacts, such as the current Youth Justice Act where they're considering using body worn cameras and video surveillance in institutions. That's just a small example.

We're not mandated to be consulted on new legislative proposals, unlike the Human Rights Commissioner. And unlike the Federal Privacy Commissioner who also has that mandate. And I personally wouldn't mind seeing that sort of mandate because at times we don't get consulted, although with privacy being in the Human Rights Act I think that loop will get closed somewhat because the Human Rights Commissioner will no doubt seek our advice if he has a privacy concern as well.

So those sort of legislative and technological projects do form a lot and a lot of agencies are doing quite novel innovative technological solutions and they do seek our advice. Although, again, not as often as we'd probably like. On the complaints front, we've sought in our legislative reforms to perhaps get a better understanding in terms of the data of complaints in the entire system. The agencies don't have to report to us on the complaints. They do under the financial accountability legislation have to have a system for dealing with complaints, that doesn't necessarily differentiate between privacy complaints and other complaints about service, for example, or staff performance.

So it would be good to get a better grip what's happening in the ecosystem. The low level of complaints I think is a reasonable indicator that, you know, that agencies handle complaints about privacy well, but we do see some that don't do so well. We don't see any enormous amount of complaints landing on our desk considering we do regulate all of Queensland.

In the complaints function that we have, our powers are somewhat limited. They extend to preliminary investigations, so conducting first inquiries about whether it's within our jurisdiction and what evidence is available. If we determine to accept a complaint, we have power to compel documentary evidence in the conciliation process. Our role there is to play an independent conciliatory function, not a determinative or decisional-making one. Although there is a distinction where we've seen systematic or continual breaches, serious repetitive breaches, we have power to issue a compliance notice. We haven't done that in recent times because the threshold is sort of proven in beaches and those breaches sometimes are quite difficult for us to make a determination. Unless QCAT has actually made a finding and whether being referred to QCAT and they're clear of the appeal periods, they may be not a solid finding of fact that there was a breach. So the compliance function is somewhat limited as well.

We may have a role to appear in those conciliation matters, although that's less clear in the information privacy role than it is in the right to information role. That's something, again, we've suggested there might be a legislative change to just clarify that role in the QCAT Tribunal that we perhaps could appear as an amicus, not representing a particular party and maintaining our independence, but at least making submissions on law where appropriate.

CA How do you think that would assist the victims of privacy breaches in that process?

W In the Tribunal we've seen, I guess, quite a number of instances where departments have lawyered up considerably, and QCAT has taken a view, I think, that legal representation is useful for it in the interest of justice to have one party represented. So, although it's not as a right, they often give leave for one side to be represented. That takes away, I think, from the – well there is an imbalance of power, perhaps, particularly where a department might have its own legal team, Crown Law and even a senior barrister at times, I've seen representing them against a potential victim or complainant who isn't legally qualified. So for them to make submissions on how the law applies in their particular circumstance and to, you know, deal with the Rules of Evidence and put their case is quite a challenge. I think unrepresented litigants have been the subject of law right debate currently and it is something that's always vexed the court. But the Tribunal was envisaged, at least in the first instance, to be a place where consumers could sort of have some equal representation.

CA And you think you could make a real difference if you-

W I think we could in some instance. I think we could help them put our interpretation of the Act reasonably well in some instances. I'm not sure that it would be appropriate in all cases, but again to have that role might assist the Tribunal as well as assist, not so much to guide the complainants, but, you know, it would give them probably some comfort to have at least the law stated and perhaps we have tried to give them some guidance on how do you present evidence. And QCAT has actually got a video, although not specific to the privacy jurisdiction on, you know, how to, you know, conduct yourself in the Tribunal. But more can be done there, perhaps.

CA How would you be able to, in what manner, provide that assistance prior to the actual hearing?

W Well, prior is difficult because, again, we don't take sides, and our role is to be independent. So in that conciliation process it's probably hard for us to go to representative. We can provide more education and training in that regard, and QCAT could. The other thing, we've talked to the QCAT registry about is having a clearer sort of complaint form that pleads their case more adequately because, again, to try and succinctly put your privacy complaint into, if you like, legal technical terms or in terms of the information privacy principles or the national privacy principles it can be quite technical because our law is principles-based. It is a bit grey even to some lawyers.

CA I'll show you Exhibit 70. That is one of the attachments to your submission. The Office of the Australian Information Commissioner Guides to securing Personal Information - Reasonable Steps to Protect Personal Information June 2018.

W Yes, I'm familiar with that document. There's a slight difference in the law between Queensland and the Federal jurisdiction. They're reasonable and this test applies more to our national privacy principle 4, although our information privacy information principle had has this concept. It's a little bit differently worded, but it's a useful guide nonetheless and we've submitted that we should merge the NPPs and IPPs into a version that follows the Federal jurisdiction.

CA With the information privacy principle 4 pertaining to Queensland, the wording at subsection (1) (b) is the agency to take all reasonable steps.

W Yes, correct.

CA So the reasonable steps, those two words-

W It is very similar. In fact, the best pronouncement, I brought along, the best pronouncement is the perhaps the GDPR which is almost the global standard now in this area and it has an Article 32 which has a very fulsome definition.

CA Could you just explain in full what the GDPR is?

W The GDPR it is the General Data Protection Regulation that's been enacted in and adopted in Europe. It has been in place for over a year now. The UK has enacted it into its domestic law and under it's currently non-exited Brexit. But as it intends to it's enacted into its domestic law. GDPR has had the benefit, I guess of quite a lot of European experience on privacy and a lot of input. A lot of countries are looking at that and indeed the ACCC, I think, has followed some of the law there and its recommendations on Australian law reform.

CA And when did the ACCC make recommendations on the law reform?

W In its report and technology which the Federal Government is yet to respond to.

CA When was that published, roughly?

W I think it's another - I can't remember the date. In the last year, I believe.

CA In 2019?

W Yes, correct.

CA Sorry, continue about the-

W So, yes, the GDPR, just if I can refer to, because I think it's quite relevant to what agencies should be expected to apply in terms of what's reasonable.

CA To comply with reasonable steps?

W Yes. So this is sort of the security principle under privacy law. In Queensland, State agencies, I think Andrew MILLS has given testimony about information standard 18. And information standard 18 is this standards-based approach to security which covers privacy. Privacy and security are obviously not the same thing, you can't have privacy without good security. You can have security without any privacy. And some of those totalitarian regimes are very good at their security but very poor on their privacy.

IS 18 is probably what we would apply if we were to audit an agency under IPP 4 in terms of what's reasonable. And it sets out sort of the adequate controls. It's not just a tick box compliance mechanism, but the Federal Government has issued its essentially eight security measures, the ASD and the essential eight. There's an essential four that's sort of a shorter sharper version of that and then there's some other standards. One of the world standards right now is ISO 27001 and 27002, which gives far much more technical guidance on what are risks and controls that would be appropriate without being absolutely specifying them. But they include some things like white listing of applications and for security on systems, particularly things like two-factor or multi-factor verifications. So when you get onto a system they really know who you are and you've proved it and it is harder to hack than just to say a straight password. So that's a longer explanation, but that's the sorts of things that we would look at under IPP 4 and NPP 4 in terms of what is reasonable.

CA Did you look at IS 18?

W Yes.

CA And the European one?

W Well, the European one has better wording in terms of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alias appropriate encryption, things like restoring the availability. And then on the most relevant one to this is a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

So besides all of those, you know, the good preventative things like training and minimising data and stuff, I'll talk about later about Privacy By Design, those sorts of control measures, the GDPR really sets it out how ideal practice should be and gives a much more fulsome iteration of it, how it's evolved to best practice. But it really does zone in on - you get the training and the access controls right and then the full life sort of principles, but you really need to demonstrate that you're doing it through regular audit and regular review of it and then reporting on it. So you actually report and say how you're going in terms of performance. And we're seeing that through some of the audit work of the audit offices across the country right now in terms of cyber security. IPP 4 and the, you know, the access controls on data particularly within that domain.

CA Do you have the copy of the GDPR?

W Yes, certainly I do.

CA You do.

W Yes.

CA Okay.

W I could tender it. It's my only copy.

CA No, we can photocopy it. How many pages are you referring to?

W I was only referring to Article 32 and that's only a couple of pages.

CA So Article 32 that's just the part about reasonable steps?

W Yes.

CA So if we can just take that and copy it while you continue to speak and then number it as an exhibit.

W Yes, certainly. It isn't the law as it applies here right now, but it's probably a standard we should aspire to. And so particularly in that Privacy by Design arena I think we should have an eye onto what's best practice as it evolves. You know we apply the law as it stands today in terms of the complaints, but we certainly need to be looking at best practice worldwide.

CA Okay, we'll take that from you for a moment if that's okay. Have you got IS 18?
.

W I don't have that with me. I thought it was tendered into evidence.

CA It hasn't been, but we're just going to obtain a copy of that as well.

W Okay. And I look at that because I believe our office is bound by that, or Parliamentary Services are and no doubt the CCC would be bound by that in terms of its security around its systems. So it's something that still evolving but the Queensland Audit Office did an audit on performance of three agencies under that. They didn't name the agencies, but they are highlighting some of the best practices and maturity in terms of agency compliance. That's really the security side of it but, again, when you're sort of putting access controls of your own staff on security it's really critical, particularly, and I think the work here is absolutely critical because an individual can have an impact on an individual, and we've seen some severe damages done to individuals or anxiety caused by that, but an individual theoretically could bring down an entire department through a cyberattack or through, you know, a threat to democracy through the electoral system as we've seen elsewhere.

ASIO was speaking today about foreign threats. And the foreign threat actors and the bad cybercriminals and the organised crime people and, you know, the paedophile child abuse networks, they're all working through systems where if you have an individual susceptibility that can be exploited. So it's really critical that we get these individual access things right and we do have really good controls, because it's not just the threat of that rogue, it's the threat of that rogue being bought by someone else, or, you know, extorted for something else through exploitation of some other material. So the threat is really very real and accelerating, I think, in that area.

CA So just going back to the June 2018 report, that mentions Privacy By Design. Could you talk about where that comes from and your views on Privacy By Design and how it works out in practice?

W Certainly. I had earlier had a little aide mémoire for that, a little pie chart that I was going to try and tender into evidence.

CA Yes, we have the pie chart. We'll tender that now. Yes.

W I think it would be a useful aide mémoire for me. Privacy By Design is a concept-

CA I'll just grab it.

W Okay, certainly.

CA It's up on the screen now. So if you could-

W Yes, I'm always looking for these sorts of things because I think they look really good in reports in terms of focusing people's attention on them. Professor Ann CAVOUKIAN-

CA I'll just show you the document, the hard copy is here.

W Yes, that's it, thank you.

CA I tender that document.

PO I think the previous matter, the report itself, the June '18 report I'll mark as Exhibit 176.

CA That was Exhibit 70.

PO Oh, 170, was it?

CA 70.

PO 70, it's already in evidence. Okay, sorry.

CA Yes.

PO Okay, so I'll make this pie chart 176.

ADMITTED AND MARKED EXHIBIT 176

CA Yes, Mr GREEN if you could continue.

W Sure. So Dr CAVOUKIAN who was a former Privacy Commissioner in Ontario Canada in 2009 promulgated this concept and I believe it has its roots in design-led thinking which you may be familiar with in terms of thinking about problems or products. Particularly in Apple, Apple is probably the exemplar product of having design-led thinking all through its whole chain of products and advertising and look and feel of usability and things like that. But in privacy it's basically thinking of privacy impacts holistically. It's involved to concepts like privacy engineering now and almost privacy and data security and ethic designing or here, privacy and human rights by design, which Ed Santo, the Federal Human Rights Commissioner is talking about now. Because it basically means identifying all of the holistic risks of what you're doing and being proactive and embedding good privacy principles and practice or human rights practices into products or legislation or policies and procedures from the outset. So it's proactive, not reactive. It actually repeats itself and says use Privacy By Design as one of the guiding principles.

Visibility and transparency is another one. Full functionality and positive some not zero some. So don't use some other public good as a trade-off for privacy. Try and achieve an outcome of the positive good that actually is privacy respectful. It doesn't necessarily have to be a trade-off. End-to-end security, so the full life cycle going to disposal of the data when it's no longer necessary and also when you're holding it, making sure that it's secure and encrypted, for example, if it's UI sensitive.

And privacy as a default setting is a concept linked to GDPR as Privacy by Default or, you know, for example, if you sell a product it actually has the privacy settings set in your favour to preserve privacy rather than in the product design as a favour to, so say location services when you buy an app they're turned off rather than they're turned on. And then they're proactive, not reactive. So one of the things we've talked about earlier was privacy impact assessments. That tends to look at the whole picture as well and look at all of the data flows, look at all of the risks and then put mitigation strategies in place to deal with the risks.

CA So how important are privacy impact assessments when you're looking at an agency's compliance with IPP 4 or NPP 4 with respect to reasonable steps?

W I think they're very important, but they're, again, one thing. So you can have the security without the privacy. The reasonable steps security would be, say, you know, put two-factor or multi-factor authentication on the password entry to the system, but if you don't say look at, well, how can we minimise access or how can we - which could be an IS 18 issue as well, say, hey we restrict the access to only key individuals, and they do that with the administration rights to systems. So they say administrative rights to systems should be very limited in an agency so that they can basically cook behind the scenes the system or change it, and those administrative rights in the best practice should actually be isolated entirely from the internet. So say a hacker can't get through to the administrator's computer because it's air-gapped, as they call it, air-gapped from the rest of the system. So it's quite compatible and a part of that, and certainly privacy impact assessments should take into account the security assessments. A lot of departments and a lot of agencies when they're designing new ICT systems do security impact assessments, but they don't necessarily think of the privacy aspect.

So I think, say, for example, the QPS roll out of the QLite system, the iPads.

CA Yes.

W We had some visibility on that. I don't know if they ever did a privacy impact assessment on that, but I certainly know they did extensive security testing. They designed the security at probably the platinum standard from what we saw. So there was some level of comfort in terms of hacktivists or other unauthorised use by non-QPS staff and say for the loss of a QLite device they could wipe that remotely through, I think two system. There is a redundancy built into it, not just relying on the Apple store wiping the device. So there was a lot of thought and attention put to the security and physical security. But you can do that without thinking well what would be the chances of unauthorised access and how could you limit that, for example. Or could personal information be used from, you know, entire systems that might have been isolated from others.

CA With privacy impact statements there isn't a good percentage of agencies who are undertaking those assessments?

W Yes, well Rachel referred earlier to, and I think you did as well, to our 10-year survey agency performance, overall I believe was 25%.

CA Yes.

W And departments reported a high level, I think that was 50 from memory. It's, I'd say, because it's self-assessment I'd be slightly sceptical that even 50% are doing them because at times they may not recognise the need for doing one. And we've seen in the Victorian context in the My Key incident where the Victorian Privacy Commissioner intervened and reported on My Key data which was supposedly de-identified. So in that case they actually did a privacy impact assessment, but they very cursorily dismissed the risk of re-identification

and based the privacy impact assessment on it not being personal information because they said it's all de-identified therefore there's no personal information, therefore the controls that they put on it were very limited. And that was heavily criticised by the Victorian Privacy Commissioner.

CA And are there any instances where there are retrospective assessments being undertaken by agencies?

W Yes. So IOC in an earlier audit did an audit into apps that were deployed by Queensland Government agencies and we looked at three apps in particular.

CA Is that the privacy and mobile apps applying the legislation guideline?

W Yes, that is. That's the guideline that's come out subsequent to that report.

CA Yes. I might just put that up on the screen and you can speak about the issue and then go to the guideline.

W Certainly. Thank you.

CA I tender that document.

PO Exhibit 177.

ADMITTED AND MARKED EXHIBIT 177

CA Just before I go into that one with you, yes, retrospective privacy assessments and how you uncovered those.

W Yes, so you can do a peer any time, and indeed we encourage in that audit report, actually encouraged as you evolve your product you should reassess them and re-do them. And that was a feature that we didn't see happening and thought there could be some improvement on as well. So as you add functionality to it you've got to continually assess privacy impacts and risks and security impacts and risks.

The app world, as you probably know, just from reading the media, there's been some extremely poor practices in app development and app deployment across a number of platforms, not just iOS or the Google platforms or Microsoft platforms, but in general private apps. There was one flashlight which apparently sucked all the data out of your mobile device and allowed them to sell it to anybody they could anywhere in the world and transfer the data. So you wouldn't generally expect a flashlight to be sending your location data or your heart rate monitor data or your steps per day data, but that's probably the worse kinds of atrocities in terms of the privacy jurisdiction. The app development we saw in Queensland actually demonstrates some very good practices. Indeed the TransLink app demonstrated one of those privacy by

design principles of data minimisation and not collecting personal information at all. So the risks there were highly mitigated by simply not collecting data.

CA And do you think that's important for agencies to have a long hard think about exactly how much data they need for each individual member of the public to function?

W It is a concept. In fact, we had a speaker and trainer from the United States, and they produced a book called Strategic Privacy By Design. But the minimal data for operating or viability of the product is something he speaks about. That's Jason CRONK. He's one of the leading proponents of privacy by design and getting into the detail of how you do it appropriately. And that really is a key principle, what do you need to do the operating, and what's the lawful basis of collecting that, and what do you need to do your business.

And it's built into the information privacy principles as well, but as a concept it's, you know, data minimisation. Don't collect that which you don't need to do the product, and in that case the TransLink app gave you the information. Yu know they could have added additional user functionality at the time that might have been able to use location data to give you a more tailored product. And that's been one of the big, I think with apps, they want to collect as much as possible because they don't know what extra functionality they might be able to deliver in the future. So that's one of those sort of data exuberance principles of let's collect as much as we can because then we can maybe make value out of it and do cool stuff. That's not necessarily best practice in the privacy arena.

The app audit actually showed how you could do privacy impact assessment and indeed the QPS in their app for reporting on Police Link hadn't done a privacy impact assessment, they thought because they were just replicating quite a lot of functionality from their website and putting it onto the app that there really wasn't the need. But the app does create additional challenges and additional threats. So they recognised that. And did one following the audit. I think they recognised a need to then do further work as the functionality increases.

CA And I'll just look at the guideline for privacy and mobile apps. Is there anything else in there that you would like to speak to by way of good practice, best practice?

W Yes. It's actually something in the whole app community, whether consents are a really good model for collection of data now. This was raised by the ACCC in the context of imbalance of power. And I think it actually is probably not dealt with in our guideline either. It has arisen more subsequently to that audit where government might seek consent of an individual to share or collect data and, you know, legally document those consents. The issue of, you know. whether it's appropriate for government to do that I think will be raised because it's being raised in the case of the big corporate, if you like, data companies, like Google and I'd add Apple in there and Amazon, where they're getting consents

but people don't understand, so they're not fully informed, contemporaneous necessarily consents and whether that's actually an appropriate model now has been raised.

I think government, in our app development we've been fairly light weight in terms of collection of data, but for using new tools I think we need to make sure that people are fully informed and that consent is freely given. And where you've got a monopoly government service provider, whether it's freely given, if you're dealing with the Tax Office and you have no other alternative supply, then there maybe questions raised about that subsequently.

But I think in this, it just showed do privacy impact assessments, try to minimise the data. I think there's some risk, too, where you're dealing with technology such as Apple or the android systems that they can have access to government data. So whether we have the technological expertise to assess that data flows aren't going from devices to major tech companies is another question that's coming up. Indeed, there's the possibility of malicious code. In that audit report we relied on agency's self-assessments there. We didn't have the technological expertise to audit fully all of the code in those apps to make sure there wasn't any malicious malware or any behind the scenes collection of data, which some of the more preposterous apps have done without people's knowledge. And hopefully government as a good corporate citizen isn't doing that kind of thing. But, you know, it is a real issue in the wider world and especially in the bigger corporate end of town.

CA I've got a copy of the portion of the general data protection regulation from Europe that you were speaking about, Articles 32 and the start of 33. Was it Article 32 you were focusing on?

W 32 is the focus but 32 is actually the notification-

CA Yes.

W -regime in EU, which the Australian one is based on largely. It is not the same. But and I'd say if Queensland or a State or Territory was to enact the regime at the State or Territory level it should follow the Australian one, just for a consistency perspective particularly where agencies operate across jurisdictions. And to help avoid confusion which is raised in that Australian report about where do I go to complain. Well, if we have the national privacy principles in Queensland that can confuse people. They apply to health agencies currently. So there can be confusion particularly if there's differing timeframes or different regimes.

CA I'll just show you a copy of that, Article 32. And also IS 18.

W Thank you.

CA And I'll tender the article 32 for the general data protection regulation.

PO Exhibit 178

ADMITTED AND MARKED EXHIBIT 178

CA And then IS 18 is on the screen now. If you could just talk to that in summary. You've already spoken about it. But if there's anything in particular you wanted to draw our attention to with respect to reasonable steps when you make that assessment.

W I guess the beneficial thing about our transmission or a maturity in this space in the cyber security and information security space which Andrew did speak about, I believe, is that it goes from a sort of tick box compliance method to a risk assessment and then appropriate measures commensurate with the risk. So it's very good for the reasonableness test. But like how much does it cost and how much additional risk mitigation do you get from that? Currently you know governments could spend billions of dollars on cyber security and it won't eliminate the risk entirely.

So it's a question of costs and the state of the art what technology is available. So I believe when QPRIME, say, was developed or the TransLink, the TRAILS system and the TICA those sorts of systems back in 2009, algorithmic auditing practices weren't of such a standard that they could be, you know, applied when those databases were incepted or designed and created and put into operation. Now retrospectively we can see well if you were going to redesign that or replace it there's additional tools you could use, but at the time it was put in place what was reasonable. And I think IS 18 has that sort of flexibility for agencies to say, well, what's – you know, really what are these risks? And it will take some further maturity for them to really get good at identifying and then quantifying the risks and then, you know, having the technological expertise depends a lot on the maturity of their ICT departments. And the big end of town obviously has more resources and more technical capability but it does provide this principles' approach which I think is very, very healthy and a far greater step along maturity.

It is where we're headed in privacy as well. There's an information's ISO international standard for privacy that's in draft right now in Europe, which sort of goes above the law as it stands sort of as best practice in some jurisdictions and says, well, really what are we about in terms of privacy? A bit like the security stuff has. So it's not just tick-box compliance, it is concepting it from the beginning of a project and looking at risks in a much more holistic and mature way.

CA I'll tender the IS 18, together with the general data protection regulation article 32 as one exhibit.

PO That's still 178.

CA Going back to Privacy By Design and with the report, the 2018 Reasonable Steps Report as a focal point for looking at that, how important are proactive audits as a reasonable step for every agency?

W I think they're absolutely critical. It's well understood, you know, in the Privacy By Design circles. In fact Jason Cronk in his book talks about demonstration. And there's the logging, so the capability of logging is one of the things that's absolutely critical first before you can audit.

CA Access is by way of a password unique to the employee.

W Yeah. And not just access to the system, but being able to track the individual's journey through the system.

CA So accessing every-

W Yeah, so if you did access your customer relationship management system, you know, which customers and which documents of those customers and at what dates and what times. And so if you don't have that login capability then you can't put an algorithm in place that says after hours access is a bit odd for this individual. You know and that sends a flag or whatever. But having a systematic audit process is one of those absolute, sort of, critical things in terms of demonstrating to the public that what you say you're going to do in a privacy impact assessment to mitigate risks you're actually doing. Because if you can't do that then you blow the trust away in a second. So and we've talked about it, sort of in our own audit arena, as follow the data. A bit like the Auditor-General can follow the cash. We're not quite that sophisticated yet, but I think following the Cambridge analytic and Facebook; Facebook didn't even – or wasn't even very good at following the data. You know, in how far it had permeated and where its instances had gone. So if you don't log that and can't sort of follow that trail retrospectively you can run into a lot of trouble. And, yeah, the report – the other thing is not just the logging and the auditing, but then reporting on it. So you get that transparency as part of the Privacy By Design principles being you know forthright and transparent is critical I think for government, especially you know where we have Right to Information laws and human rights laws with an overlay coming soon that we're transparent and accountable. And so the reporting on those audits is critical too and that would link with a notification scheme.

CA Yes. I'll just move on to that with your proposals for improvement in Queensland. There was the notifiable data breaches scheme 12-month insight report by the Office of the Australian Information Commissioner. And I believe that's Exhibit 172. If Mr GREEN can be provided with Exhibit 172? While that's happening, so-

W I've actually got a copy, if that's okay.

CA Okay. So we'll go to a couple of pages in a minute. But can you explain what happens nationally and why it should happen within Queensland?

W The scheme, like I said earlier, was based loosely on the GDPR notification scheme and notification schemes have been in place in other jurisdictions. The US had a couple of instances of it.

CA That's mandatory application of breaches.

W Yes, sorry, so mandatory data or notification. And it's generally called data breach notification, but GDPR was bringing that in. Australia actually was ahead of the game in terms of implementing and had quite a long lead-in time to do it. It's sort of a two-fold scheme where you assess risks. So one of the problems is if you tell people and the Information Commissioner referred to this, if you tell them their data is breached but you don't know enough about that breach to kind of let them make adequate informed decisions, then you can do them more harm. Likewise, if, say, there is an inadvertent breach but that data's gone nowhere, or the personal information's gone nowhere and there's no harm that's been assessed then you don't have to actually tell the individual in that instance, but you still notify the Australian Commissioner. The notification scheme is seen really as best practice in the cyber security arena and that's why IS 18 builds that in to say what are the threats and how do we learn about them and how do we guard against them?

So, say, if Health in one hospital gets hacked or has a – you know a loss of personal information somehow – which has happened in Victoria recently where a ransomware attack locked down systems in Victoria – them telling, say, the national defence signals or the cyber security centre – then they can disseminate that knowledge and then the others can guard against those risks and assess you know whether they're susceptible with the same sort of attack or same sort of loss. So there's the benefit in the defence side of things and the prevention side of things of the scheme which is why you tell you know the OAIC because then they can identify systemic or wider issues and they can notify public if there's harm and then the public can take steps to mitigate the risk to them themselves. So the individual's affected, it's an important part of harm minimisation that they can take steps.

So it's illustrated, say, for example, if their credit card details are lost by a transport department and, say, there were 100 individuals affected, well, they'd be at risk of credit card fraud. They can go and take steps to cancel their credit card and that might mean that they don't have as adverse financial impacts as they would have had otherwise. And it's a two tiered sort of scheme of assessment. And Australia has longer to assess than in Europe. So we have seen how that can cause a bit of imbalance. And I've said let's stay as uniform as possible because one of the international breaches was a firm called Page Up where financial and HR records were potentially lost by a big company that supplied multiple agencies across the world. That company notified in Europe and they really then had to trickle down to their customers who were located all

over the world. The time limits that they had for assessing were different in Australia, but it caused some angst amongst customers who couldn't assess risks here of Page Up in Australia. And there were Federal and State agencies as well as private sector corporations caught up in it. So it was a very complex notification environment. But it did help, I think, people put a rigor around assessing what was lost and, you know, where it was lost and what were the risks – what was the type of information lost and then what should they do about preventing further loss, what should they then do about notifying individuals affected and reducing harm.

CA Thank you. And on page 4 and 5 it says Report at a Glance and there's some pictures to help. I note that it says there that there was a 712 % increase in reporting.

W Yes. So the previous system was somewhat voluntary. That isn't surprising that the numbers I think are still running around just over 900 of mandatory breach. So considering the jurisdiction, it's not – and there's some where multiple notifications in one agency have occurred. So it is not astronomical. It hasn't been quite – you know there's been some rigor in terms of how you do it to minimise the impact on resources and what not as well. So the OAICs put in place some systems and procedures to deal with the volume and to make the assessments clear.

The UK systems actually developed a phone triage system. So they have a phone notification system in the first instance to try and triage ones that need more urgent attention or ones that are more serious, again, to try and minimise impact. So say if one health authority was notifying of a breach, then how do you get that disseminated more widely to take preventative action?

CA And then, at page 21, there's some best practice tips. Is there anything you'd like to elaborate on there that you haven't already covered?

W Yeah. They're all really good tips and I think we would adopt the similar ones in this jurisdiction. Training has come out in their literature in the – because of the human vector that I spoke to before about how even the bad serious organised crime or national bad actors would try and take advantage of weaknesses in individuals, that individual training is an absolute critical factor.

And a number of the breaches are through accidental non-malicious or mal-intended action as well. So reducing those accidental mishaps, reducing the susceptibility of your staff, training has become absolutely critical and that's come up in our audit work as well. And you know not so much repetitive training but some kind of system to make sure it is frequently sort of reassessed as threats evolve as well. So we're in an ever-evolving threat environment.

So, say, for example, some new vector came in of how you can send a malicious SMS message that would get into your email somehow versus say a Word document or an Adobe was seen as a way of getting into systems in the past, but

there's more far more sophisticated attacks happening now. The preventative technologies and processes idea I think we've seen some airing of that in terms of algorithms being used to proactively monitor systems and I think there's quite a lot of merit in investigating those as costs come down. Again, that involves staff surveillance. The Law Reform Commission is looking into workplace surveillance. So I think staff need to know about their systems and how they work at least you know to an extent that they're in operation, not necessarily so they can circumvent them. But it's important we're transparent and that we use those sort of technologies or state of the art things that are available to stop bad actors particular. But also the stickybeak feature I think can be controlled and particularly, you know, flags on systems are appropriate.

Preparation and assessment of harm I think is a critical thing and sometimes beyond the technical capability of an agency. So we're seeing agencies having to bring in technical experts to sort of audit systems and forensically see where the breach might have occurred to fix it. And that's a thing, I think, the resourcing of the technological stuff is a challenge for all entities across the country and across the world right now. So we're seeing training particularly in cyber security and cyber defence and information management security as being a critical thing. But training of our staff on how they can be compromised is a critical part of that.

CA And by way of improved regulatory framework, you are keen to have own motion powers?

W I think I expressed there's some limitation in our preliminary inquiry powers to actually get to the bottom of these things in a timely fashion. And then that would assist us – it would assist if there were mandatory data breaches and we saw systemic matters where they weren't necessarily proven but we could do some more investigation or at least questioning of agencies I think that would be useful. Other agencies are looking at more or stronger investigative powers.

So the ACCC has recommended more power for the Federal Commissioner. The ACCC has also recommended considerable turnover fines along the lines of the GDPR. So in terms of the appropriate fines for data breaches or for, you know, breaches of privacy, personal information, the high watermark I think was a fine by CNIL in Europe of 50 million Euros to Google which probably gets to the attention of boards. I'm not recommending that, even at the Federal level for Federal agencies necessarily because I think it would be counterproductive. We want more of that investment to go into preventative measures, I mean other measures rather than fines. But fines and penalties have their place as well in terms of the arsenal end. And own motion power which at least could allow you to get to the bottom of the thing, and even if it was still conciliated or went to QCAT for a determination on any damages, would be an enhancement in this jurisdiction.

The Victorian Commissioner's exploring, as I understand it, more of a determinative role, but that changes our role to some extent in the IOC context

of independence. And I also think right now with the Human Rights Commission coming online going much further was probably, until we see how that ends up working and interacting with our jurisdiction, it's probably one additional tweak too many. But, yes, certainly we're on the record, and our submission on public record, to say own motion power would be useful, mandatory data breach should be looked at and we'd suggest that even more strongly today. And that was a submission two years ago.

And the privacy impact assessment being mandatory is another thing which we've seen maybe is a need for. That's – it actually is enacted as a mandatory subordinate code through the OAIC, so Federal agencies have to do the peer assessment at State level that's not mandatory. In Europe under the GDPR it is mandatory and essential that you've demonstrated a good practice of doing it. And I think additionally we've lended some weight to combining our IPPs and NPPs and updating them a bit to make it more understandable for the public so it's less complicated law in this State and more consistent with the Federal jurisdiction. That's our wish list of legislative reform.

CA And we touched on with another witness who came to talk about the causes of action including a new potential new statutory tort which you mention has been raised in several reports and inquiries over the years, and most recently in the ACCC report from 2019, Australian Competition Consumer Commission Digital Platforms Inquiry Final Report June 2019 at page 35. You mention that at paragraph 31 and 32 of your submissions. I'll just show you Exhibit 75, and page 14.

W Thank you.

CA Just page 14. This is where this report – the Commissioner for this report for this inquiry was Professor McDONALD, and she was the one who gave evidence so that's how it's came to pass that it's part of the exhibits for the purpose of the recommendations for the new statutory tort of serious invasion of privacy misuse of information.

But there's one pertaining to the Privacy Commissioner's role and functions, and that's Recommendation 16, new regulatory mechanism for the privacy Commissioner to investigate complaints about serious invasions of privacy and make appropriate declaration. Such declarations would require referral to a court for enforcement. So given what you've just I'm taking that that's a step too far in your view currently?

W I believe it – it does take the role of the Federal Commissioner perhaps too far in terms of advocating for a particular individual against another entity. I support fully consideration of the tort or a statutory cause of action as it's been recommended by the Law Reform Commission and ACCC. I think it is better done, perhaps, by individuals or classes of individuals on their own to pursue, not necessarily through an investigation or prosecution by an entity. I certainly wouldn't see that as being ideal at the State level because, again, it compromises

our independence, and it could be used by individuals to, as sort of a witch hunt as an against the particular entity.

I do think a tort would be useful in our context as part of the arsenal of, if you like – or repertoire of tools to use to further privacy and good practice. Because I think those higher level penalties in a tort situation, you know, they may well exceed the 100,000 jurisdiction say that's in the Queensland jurisdiction because they could go to the actual damage. So certainly in the identity theft, if someone, you know, through unauthorised access compromised someone's whole asset base the damages could far exceed the 100,000 quite easily if they lost their house or you know their share portfolio, or something like that. Or their motor vehicle would certainly sometimes exceed that if I see the Lamborghini shop up the road.

So I think you know severe penalties have their place and certainly they're well In place in Europe. And some individuals unfortunately – but those best placed to pursue their legal remedies might be able to afford the legal representation to pursue such action. So I think isn't a panacea necessarily but it could be an additional benefit. And certainly I'm interested to see what the responses to the ACCC recommending that – I found it interesting that they pursued that further and I think you know there's some merit in us considering it. Particularly at the Federal level. I think it needs to be done nationally and consistently to be effect.

And again I think Human Rights Act will be an additional benefit of raising awareness and better practice. So hopefully the Human Rights Commissioner will agree with me in terms of do proper privacy impact assessments otherwise you know you won't necessarily be compliant with the Human Rights Act if you haven't considered those things upfront.

CA And it was touched on earlier this afternoon in evidence about information sharing. Yes. I'll show you Exhibit 141. So that's the relatively new Part 5A Information Sharing for the Domestic and Family Violence Protection Act 2012. And there's also the guideline Information Sharing Guidelines, May 2017, published by the Department of Communities, Child Safety and Disability Services. There's some reference to the Information Privacy Commissioner being consulted in the process of this legislation and guidelines coming about. Could you explain what-

W Certainly I'm happy to explain. I mentioned in the sort of functions of our office a lot of the work that we do is actually commenting on legislation and proposals that might have privacy impacts, particularly in our privacy jurisdiction, and we also consider the policy implications from the RTR perspective where just good information management is at play.

There has been a huge push to share data particularly for beneficial and optimal outcomes and for innovative service delivery. So the IOC, our office, had the Productivity Commission speak at our privacy awareness event two years ago when the Productivity Commission first said, "Hey, we should get better at

sharing information in the domestic violence and the child protection arenas and youth justice where there's wicked policy problems are involved and there's multiple agencies which sometimes buck pass say they won't pass on information." There's been great pressure to do better information sharing to minimise risks to vulnerable people.

This is one of those sort of regimes and it has happened quite across the country. I think Queensland was leading in terms of putting some legislation in place. Where that legislation is in place, it's actually exempt or not covered by the Information Privacy Act, so it's a legislative scheme for sharing of the information. It's permissible that use and disclosure where it's where the information's available in multiple areas there's increased risk of inappropriate use or accidental use. So there needs to be a balance I think in these legislative schemes of where it's really critical to keep vulnerable people safe and then how you go about balancing that and making sure the security's in place so if you do disseminate it more broadly it stays secure because it often very highly sensitive information.

So we were consulted in this instance on the legislation and feel reasonably comfortable that it you know not so much overrides but it provides some safeguards and balances the sharing of information in a kind of safe harbour environment in a legislative scheme which gives people the permissions and the certainty about when they can and they can't share. The guidelines were designed by the department to interpret that legislation and sort of put it into operation. And we were consulted on it at the time. We haven't heard too much more about how it's going in that scheme, but since then there's been further information sharing arrangements put in place, I believe, for State Penalties Enforcement, collection of fines, things like youth, the Justice Act as I've said before to make sure that, you know, appropriate information flows to appropriate agencies that have responsibilities.

And I believe there's a mechanised system, the acronym escapes me. SCRAM. SCRAM was the mechanised system for sharing that information where you know notifications under legislation are supposed to occur to appropriate agencies. So those information flows often are legislated as, you know, you need to notify or share this information with this agency and generally they're supported by some high risk event. I think SCRAM covers things like weapons licensing where if there was a conviction for something they'd lose their licence so people need to know quickly. And in this case, the same where there's potentially grave harm to vulnerable people, it's appropriate that we share information. It's just getting the balance right that's critical.

CA And just to cover off on available remedies, we talked about the potential for a new tort. Are there any other suggestions that you have in mind?

W A magic wand. I think the Human Rights Act is going to be beneficial in our jurisdiction. I think done Federally it would have had more impact. But, again, in terms of raising awareness and making sure things are considered,

particularly at the legislative stage, that will be useful. The tort will be good. Some legislative reform, particularly our legislation was probably 10 years out of date when it was enacted. It didn't really update on what we'd had before administratively and the world has moved on rapidly.

Since then the velocity and volume of data and the data analytics capability and even artificial intelligence in the last few years has grown exponentially. So the challenges for good data management and practice are ever increasing. One thing I would like to see actually in addition to the legislative changes, and I think this will be considered at the Federal level, too, is an awareness that you're subject to artificial intelligence. So GDPR, again, I'll refer to it, but it has a requirement that data processes tell the subject that they're subject to analysis or data analytics and probably our most recent example and I don't really think AI was at play here, but rather bad programming, but the robo data example at the Federal level where decisions were being made about debt collection that weren't subject to human oversight. That's been a lesson learned I think in the Australian concept. And perhaps in Queensland you know before we get too involved with using artificial intelligence you know for good public outcomes and benefit that we be able to have a similar provision that people are aware of, you know, the gist of what's behind the algorithmic decision-making, perhaps have a right of review to have it explained or overseen by the human decision-maker, particularly that's a challenge for judicial review in administrative law generally. But also that the data into the algorithm and the algorithm itself there's some transparency. So that cuts across the other function of our office in terms of Right to Information. People should know, one, that they're being processed, two, that they're being – yeah, that the algorithm makes decisions and they might have a right of review. But also what's the data that's gone into both the development of the algorithm and the machine learning and also then the data that's been used for the decision. And that's a challenge that's being considered worldwide right now. But before we go too far it would probably be useful in this jurisdiction to get that into law sooner rather than later.

CA And do you consider that the quantum of damages currently available is sufficient?

W IOC has actually got a guidance on what's the price of a privacy breach. And I mentioned before the Google fine which is I think one of the world's greatest fines in the privacy arena of 50 million Euro. Our current jurisdiction under the Information Privacy Act is the $100,000. I think that's pretty low. But the damages awarded so far have been considerably less than that. We have a guideline called How to put a Price on a Data Breach. It relies largely on other jurisdiction's decisions; New Zealand, the Australian and UK even. Because there aren't that many QCAT decisions on damages.

Some departments I think settle matters where they have, you know, clearly breached privacy and they might be confidential. So we don't see them. They might exceed what the QCAT awards are. But generally they've been less than

10,000. They're more likely to be awarded where there's actually quantifiable rather than psychological damage. So say, for example, a physical fence has been paid for where there's a bill for the fence versus the angst and anxiety that's been caused.

I think the psychological harms are much more difficult to put a price on and QCAT hasn't been all that keen to do it but has in a couple of instances. There's a matter that's quite recent called CH that's awarded some psychological damage or impact, but I think they're quite low. I don't know that they're actually a disincentive when departments are perhaps prepared to spend 50 or $100,000 on legal representation to fight a case when they could have perhaps settled considerably less and caused considerably less stress to some impacted individuals.

CA And what's your fact sheet entitled?

W How to Put a Price on a Data Breach. It doesn't have the two most recent decisions of QCAT on that because they may be subject to appeal. But I'm happy to tender that or provide a link to the Commission.

CA Yes, if we can tender that document.

PO Exhibit 179.

ADMITTED AND MARKED EXHIBIT 179

CA Now, for the members of public who are victims of privacy breaches, is there sufficient – are there sufficient mechanism in place for quick assistance financial if there's a need to relocate urgently, emotional counselling support and the like for victims? Or is it something where there's a lot of hurdles and delay can ensue to obtain some assistance?

W Certainly for privacy breaches where we deal with them as a privacy breach, there's firstly a requirement for the agency to consider it for 45 days and then a mandatory requirement for us to try and conciliate it before it's referred to QCAT and then QCAT itself can take considerable time. So, you know, it could be a year lag before they're in QCAT quite easily. And then some time for the QCAT decision and then an appeal period.

So that's not a means of really getting quick compensation or certainly not emergency relief for a privacy breach. Victims of crime, again, that assistance I think generally requires a conviction. So say a 408E conviction might result in an award of some compensation, but again those trials can last years. You have more experience I think as the Commission in those matters. But certainly the criminal justice system isn't exactly super quick, and there can be appeals.

So, you know, as an interim measure I know there's emergency relief but I don't think it's particularly adequate for sort of – it might be emergency shelter-type

relief. But not I think particularly adequate in some of those risks of harm, identity theft and where there could be major sort of damage financially. The Information Commissioner spoke earlier about the work of ID CARE and they're an absolutely essential service nationally and in New Zealand. They – I don't – I think their counselling service can be invoked quite quickly for identity theft matters. But actually getting compensation or say if you've had your driver's licence stolen and it's being misused, there can be some trauma in terms of dealing with the impacts and getting things done quickly and getting financial compensation.

I believe the banks are getting better. You know, if say identity fraud is quickly proven and you know you can get your credit card reimbursed or reversed, you know, the charges reversed, but more could be done in that space. I'm sure Mr LACEY or Professor LACEY could give more evidence on that, but certainly their research suggests that victims of identity fraud particularly have not the best journey and certainly sometimes the response can be worse than the actual privacy breach.

CA Do you see any areas where you've got some considered improvement ideas?

W I think it would have to be considered more broadly in the criminal justice system whether there's some sort of emergency relief or further requirement. I know considerable work has gone into the domestic violence dedicated courts and tried to improve the justice system response in that area, violence and family violence. More could be done no doubt. There's no quick answers. I think there's, you know, there's a lot of victims across the spectrum in the criminal justice system, not – you know some sort of emergency funds might be better, or more funding for emergency accommodation that could help. There's others probably better placed to see what's available and the adequacy of that than myself say. Mr Anthony REILLY from Legal Aid or something like that or the testimony you've heard from some of the previous witnesses. But, yes, I think you know the general feeling is is that more can be done.

CA And just turning to paragraph 9 of your submission. So there you list in a non-exhaustive manner some of the potential consequences for victims. Could you expand on that from your experience as Privacy Commissioner having regard to if you wanted to talk about particularly sensitive matters we are able to close the hearing for you?

W Yes, I've seen personally in our complaints all of this potential or, you know, actual damage. I said earlier that the risk of threat actors, say, organised crime and, say, mal-intended national States, I think that is another area where if you've compromised an individual's access to systems we could even see more broad threats or the worse extremes perhaps are of threats of our very democracy and system of government. I think in a malware attempt we've seen some cities in the US where a city has been held to ransom and the city has run things like the courts and the hospitals. So our cities are susceptible, particularly the

services to humans. The actual, the range of impacts could be quite catastrophic and that's in the whole cyber security arena.

A massive concern is in terms of the more connected our infrastructure is the more quickly a country could be brought to its knees and certainly an offensive cyber security capability is something that I believe Western democracies are considering and perhaps are on the record as having or being capable of. So that whole stake-raising – it's not so much – it's multiple impacts across society far beyond these ones.

I think that these ones you know the impacts on the specific individual in a specific case cannot be underestimated and psychological harm and, you know, mental anguish can't, you know, they're hard to put a price on. But obviously the worst – you know there's this high suicide rate in this country and I think any impact on mental health through these breaches could contribute to that too. I don't think it is documented. But I've certainly heard the voice of anguish in complaints. And, yes, it's seriously impactful on some individuals and particularly difficult to recover from in some instances.

So once something's known it can't become unknown necessarily and the Information Commissioner alluded to that. You know that there's some that's just irreversible. Death I suppose is the worst sort of physical outcome that's irreversible. But, yeah, the whole gamut of damage can occur. And I don't think the courts have heard a lot of it. And certainly the research at Sunshine Coast University in identity fraud has highlighted some of the serious consequences for financial, but those emotional impacts are high on their agenda as well, that's why they have the counselling service.

CA Thank you. Thank you very much, Mr GREEN. I don't have any further questions, Chair, for Mr GREEN.

PO Sorry?

CA I don't have any further questions for Mr Green.

PO Thank you. Thank you, Mr GREEN for coming. You're excused.

W Thank you kindly.

CA Thank you.

W UI your paperwork but I don't believe it contains personal information.

PO We'll have you closely surveilled.

CA Thank you. Chair, that was the last witness for the public hearings in Operation Impala. I understand that there may be one further witness to provide evidence next week, but due to the sensitive nature of that evidence it will take

place in a closed hearing. The Commission will be drafting a public report in relation to the evidence collected during Operation Impala and intends to produce a public report. I'm instructed that the Commission is not seeking further submissions from agencies or witnesses who attended the hearings as a draft copy of the report will be provided to those agencies and witnesses to the extent that the report relates to their evidence. Thank you.

PO Thank you very much. So we'll just adjourn generally. Thank you.

HRO All stand. The hearing is adjourned.

END OF SESSION