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: 54 MINS)

LEGEND

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

HRO All stand. This hearing is resumed.

PO Thank you.

CA Good afternoon, Chair.

I have a letter to tender that was referred to in the evidence of Mr MAGOFFIN from the Department of Transport and Main Roads. It's a letter dated 21st April 2017. I tender that document.

PO I'll make that Exhibit 168.

ADMITTED AND MARKED EXHIBIT 168

CA I call Ms Rachael RANGIHAEATA.

PO Good afternoon.

W Good afternoon.

PO Would you prefer to take an oath or affirmation?

W Affirmation, please.

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. Thank you.

CA Good afternoon, Ms RANGIHAEATA. You were provided with an attendance notice for today?

W Yes, I was, thank you.

Thank you.

CA Is that the document?

W Yes, it is. Thank you.

CA I tender that document.

PO Exhibit 169.

ADMITTED AND MARKED EXHIBIT 169

CA You are the Information Commissioner at the Office of the Information Commissioner and been in that position since 2013?

W Yes, that's correct.

CA Prior to your current appointment, you were employed at the Office of the Information Commission in various leadership roles since 2005?

W Yes.

CA And have prior experience as public servant in both state and federal services?

W Correct.

CA You hold a Bachelor of Law degree with honours?

W Yes.

CA A Bachelor of Science and a Graduate Certificate in Public Sector Leadership?

W Yes, that's right.

CA And you prepared a joint submission with the Privacy Commissioner, Mr Philip GREEN, for the purposes of Operation Impala. I'll just show you a copy of that submission. Is that the document?

W Yes, it is. Thank you.

CA I tender that document.

PO Exhibit 170.

ADMITTED AND MARKED EXHIBIT 170

CA Would you like to make an opening statement?

W Yes, I would. Thank you.

The Office of the Information Commissioner welcomes Operation Impala, including examination of factors that facilitate misuse of information within the Queensland Public Sector and relevant features of the legislative policies and operational environment.

We support consideration of reforms to better prevent, detect and deal with corrupt conduct relating to misuse of information and lessons that can be shared with the broader public sector.

The Information Commissioner's statutory functions are set out in the Right to Information Act and Information Privacy Act, and relevantly include mediating privacy complaints against Queensland Government agencies, providing privacy guidance, training, tools and resources in conducting audits and reviews to monitor agency performance in compliance with the Right to Information/Information Privacy Act. Our office also reviews agency decisions about access to an amendment of information which comprises the majority of our current service demand.

I am supported in performing these functions by two Deputy Commissioners; the Right to Information Commissioner, who leads the External Review Teams, and the Privacy Commissioner. The Privacy Commissioner leads the privacy complaint and advice functions, including the advice about privacy impact assessments of key policy and project proposals, such as information sharing or adoption of technology. The privacy Commissioner also leads the annual Privacy Awareness Week Campaign in May supported by our engagement in corporate services team to promote awareness and engagement within the community and government.

In 2019 our Privacy Awareness Week Campaign theme was build privacy into our every day. We share a range of resources with agency CEOs to assist them to promote awareness with their staff and stakeholders, including posters, screensavers, and banners and draft email addresses. We also reinforce the messaging from our audit about training and awareness from February 2019 and reminded people about our free online training and other resources.

Our jurisdiction includes agencies diverse in maturity, size and resources. Queensland Government agencies subject to our legislation includes local governments, public universities, hospital and health services, Queensland government departments and statutory bodies.

This year marked 10 years of operation of the legislation. In performing our functions over the past 10 years, we have observed substantial opportunities and challenges for agencies in adopting new technology to meet community expectations, drive, innovation and efficiency.

The sheer volume of information generated and collected by agencies is a growing challenge for good information management. Rapid development of technology and increasing use of artificial intelligence and data analytics creates real opportunities for improved service delivery, but with it brings challenges to implement these in a privacy, respectful and ethical manner.

Government agencies collect and hold vast amounts of personal information as custodians on behalf its citizens. And citizen's trust and expect that the governments will use this responsibly and protect this information from unauthorised access, misuse and disclosure.

It is important to note the impact of privacy concerns on trust. The Australian Information Commissioner's privacy survey found that 1 in 6 respondents would avoid dealing with a government agency because of privacy concerns. Given people often have no choice in service provider, the impact can be considerable.

Our recent audit reports have shown that there is clear room for improvement in key areas relevant to this hearing. Given the Information Privacy Act has been in place for 10 years, and the increasing risk environment, it is reasonable to expect a high level of maturity across most agencies.

Training and awareness has been an ongoing focus for improving agency practices through our training and audit functions. Our awareness of privacy obligations audit and tabled in February this year, made recommendations for all agencies, including that all employees complete mandatory privacy and information security training at induction and regular intervals. We also recommended tailored training. The majority of our compliance audits of agencies in the past five years have resulted in recommendations for improvement to training.

Privacy impact assessments and management of privacy breaches were two key areas identified in our 10 Years On Report on the self-assessment audit completed by 195 agencies. The fourth in its series since 2010.

Agencies across Queensland confirmed in their self-assessments that they have less maturity and a greater need for focus in areas relating to technology, presenting greater risk in how technology is adopted without ensuring appropriate systems and processes are in place.

Importantly, only 25% of agencies reported appropriate processes for privacy impact assessments, a critical tool for assessing and addressing privacy risks. We've previously recommended that the Information Privacy Act be amended

to include data breach notification requirements consistent with the Australian Privacy Act, which introduced a scheme in early 2018.

We consider that a mandatory data breach notification requirement would support both the community and agencies to achieve better outcomes as part of an overall framework to educate, protect, monitor and respond to unauthorised access to personal information.

Thank you.

CA Thank you. The Office of the Information Commissioner has published a privacy breach management and notification guideline.

W Yes.

CA I'll just show you that guideline.

W Thank you.

CA I tender that document.

PO Exhibit 171.

ADMITTED AND MARKED EXHIBIT 171

CA Could you please walk us through that document highlighting the areas of best practice for agencies?

W Thank you.

Yes, as I said, we currently don't have a notification requirement in Queensland. However, we do encourage agencies to consider voluntary notification to both the individuals affected and our office, and there are also steps that they need to walk through, which may include other notifications that are required as well. And this guideline helps step them through that process. So if you would like me to just walk through some of those steps involved?

CA Yes, please.

W The guidelines.

So essentially there's four steps. The initial one is to contain the breach.

So when you first identify that there has been a potential breach, and often information may be patchy, and sometimes that's when people contact us, there's -- they may not necessarily know the full nature of the information that has been potentially lost and the circumstances, but that is where they really need to very quickly try and get in there and find out what they can, but also, at

the same time, escalate the two to the relevant people within their organisation the key information so that they can notify people in their leadership team, and others that they need to bring in as part of that team to respond, including those in the information security, it's relevant to the particular breach at hand.

So, for example, it might be that they need to shut down a system, or deactivate somebody's access, or something. It's just really – of course, the nature of potential breaches can be very diverse, so it really depends on the particular circumstances, but it really is a rapid investigation and assessment at that time, and it can evolve over a period of days sometimes.

So it really is trying to contain and gather information. Sometimes in that contain phase you are actually able to mitigate the breach and that's obviously the optimum situation there. And it's critical, as we say, with our hint there, critical to bring in the process, the privacy expertise at hand internally as well as externally.

One of the first things we often say is, "Well, have you contacted your privacy officer?" And sometimes the call we get is from the privacy officer, and that's preferable that we hear from them as well. But most larger entities do have a privacy team, or a privacy officer, or someone with relevant expertise, and they really do need to engage them as part of the solution.

So it's really a range of things that we step through in the guideline there, but they -- as we also highlight there, they need to think about what their obligations are at that point as well, because there are some mandatory obligations to notify certain regulatory authorities depending on the nature of the information, the consequences of the seriousness of the potential breach. And we've set out a number of things there, including the Commonwealth Mandatory Notifiable Data Breach Scheme for tax file number information and so on. So it is important that they really think through the range of information there.

So step 2, we say you need to really fully evaluate those associated risks and we have some questions to really prompt people through there, so we're really looking at, well, what's the nature of the information involved and who's affected there.

And it may not be a small number of individuals. It could be a large number of individuals. Or it could be one particular person. And again the circumstances can be so diverse there that it really needs to be a tailored approach. It is not a one size fits all at all in this situation.

You need to look at the cause of the breach. I think people often think about the information security-type reasons, but often it really does just go back to human error a lot of the time. It's – the wrong envelope or wrong email address and the -- there's a lot of very simple reasons, or, in this context in this hearing, failure to lock your screen and let someone access your account and someone takes advantage of that and can misuse information based on that opportunity.

So the insider threat. There can be very, very simple things that can have occurred there. And it may not be easy to identify how that has occurred at that step. So there's a range of questions there that can assist people to walk through that process.

And then, of course, you really need to think about, so what's the foreseeable harm to the individuals that are affected. And that can range from very minor impacts. And, of course, as I said, sometimes agencies are able to contain the breach and have a high level of confidence that they've contained the breach, and there should be no impact on the individuals. Right through to extremely significant threat of identity theft or physical harm, or threat to a family's safety, for example, and someone -- that's where timeliness is of the essence, and you really need to identify that person as quickly as possible and provide -- and that takes you into step 3 about notification of individuals.

But it really does go to how you approach that next step of notification and the support and assistance and the messaging. The communication is absolutely critical at that point as to what you tell people next and the -- and I know the Australian Information Commissioner has a section at the end of the recent 12 Month's Insights Report on the Commonwealth Scheme where the CEO of ID CARE, Professor David LACEY, has talked about the impact of poor execution of that communication can have on people, where it can really compound the experience, it can be more traumatic if, for example, I think – the example he uses is where someone's sent a message late on Friday and given some details for agencies that can assist late on Friday, but they're closed all weekend. And there's nothing you can do to take care of the threat to your identity, the potential identity theft.

If people don't know how to take action to protect themselves, or they feel even more vulnerable and they aren't able to look after themselves, or they feel that when they take steps to make a complaint and they're not treated with respect, or they aren't able to get the support that they need, it can be even more traumatic, and that can lead to a whole other issue.

So that part of this exercise, I think, we need to think about very seriously and because it is really critical to achieving better outcomes for the community in the event that there is a breach. And there will be breaches. We will do our best to minimise that risk, but we need to be prepared and execute that part well.

One thing our guideline does cover is the exception, if you like, where it's not always a given that you should notify individuals. Sometimes it will cause more anxiety, particularly where you have a high level of confidence that you've contained the breach, or you're -- and perhaps you don't have a high level of certainty about who's affected, so just saying, "Oh, we think we might have lost your information" isn't actually going to help a lot of people. They can't do anything with it, and they can't be sure whether they're affected. But, really, that does go back to ensuring that you have good information about the extent of the breach, who was affected and so on. And it rounds right back to ensuring

you have good information management so that you know what you might have lost and so on. So there's a whole lot of other issues there. So our guideline does give some tips on what to say and so on.

And of course you're not done when you finish that process. You really need to reflect, like in all these processes, as to how to prevent a repeat occurrence. There's much to be learnt from any incident like this. And a serious exercise, I think, needs to occur at the end of any process to -- and bring that back into a review each time. So, yes.

CA Thank you. And you mentioned Professor LACEY.

W Yes.

CA Is he referenced in the Notifiable Data Breaches Scheme 12 Month Insights Report from the Office of the Australian Information Commissioner?

W That's correct, at page 20.

CA Yes, I'll tender that document. I'll show you and then I'll tender that document.

PO Exhibit 172.

ADMITTED AND MARKED EXHIBIT 172

CA I tender that document.

And I believe the Privacy Commissioner, Mr GREEN, will speak to this report in more detail when he provides his evidence, but in relation to page 20, did you want to expand on what you touched on in relation to Professor David LACEY?

W Yes, well, ID CARE provides a service that people are often referred to in the event of such breaches. And there are now partnerships with New South Wales Government and many jurisdictions across Australia and New Zealand. And Professor LACEY has spoken at a couple of our recent Privacy Awareness Week events, and is highly regarded in this area. And as you can see in this report, he also talks about the more effective notifications explaining risks in plain English. He's talking about the key aspects of the communication that is so important. When you receive something that you have a high level of anxiety around, you need the very clear communication about what's happened, what you need to do next and what support you can get. And of course, being referred to ID CARE and other support services, of which there are a few that can support different people in different circumstances is critical.

CA Could you expand on those support networks?

W Well, there's people also refer to networks such as Beyond Blue, and so on, because it does raise a high level of anxiety for people in these sort of situations.

But ID CARE is really a key in terms of managing the identity theft risk. And they have counsellors there. So this is really a critical service, I think, in this area.

CA And in your opening you mentioned the 10 Years On, the report from the Office of the Information Commissioner.

W Yes.

CA Just while we're getting that, that's a recent report, isn't it?

W Yes, it was tabled in Parliament in June 2019. Thank you.

CA I tender that document.

PO Exhibit 173.

ADMITTED AND MARKED EXHIBIT 173

CA Could you explain a little bit about the report and have particular regard to the executive summary, on page 1.

W Certainly. So this report was the fourth in a series of self-assessment electronic audits that we have undertaken since 2010. So this fourth report really represented how agencies self-assess that they were travelling across the 10-year period and gave us some comparative assessment across some – quite a number of questions that really represented the right to information/information privacy obligations and practice.

We also asked a number of new questions that were relevant to technology, in particular, and topical questions that had come up, new guidelines and standards. Some of the key questions I think that are of relevance here relate to particular aspects of implementing privacy impact assessments. We also had new questions around camera surveillance. We expanded our questions in that area. Privacy of mobile apps, which followed on from a specific audit that we had done, we had tabled in 2017. And we asked some questions around privacy breaches.

And what we found was – in relation to this particular hearing, was there was lower maturity than we would have liked to see in, generally in information management. And I think it's important to keep in mind that many aspects of solid information management, such as record-keeping, provide the key foundations for effective right to information, information privacy.

CA Was that across the board of public – of agencies?

W Yes. And it's fairly consistent and something that we see in our work. For example, in our external review function, we consistently encounter many

review applications that raise issues about sufficiency of agency searches for documents due to record-keeping issues in many cases. And it's something that agencies struggle with. But – and there's also, of course, new requirements in relation to emerging formats and types of documents that I think are challenging for agencies to keep on top of and ensure employees are bringing documents into their systems and capturing them in that way.

We -- the most, as I mentioned before, most concerning and lowest maturity that we saw was in relation to the adoption of privacy impact assessments. So across all agency sectors it was 25% of agencies had answered "Yes" to all questions related to privacy impact assessments. We saw a higher level of maturity-

CA Is that -- we might just go to page 30 where I think there's some helpful visual material and talks about it in a bit more detail. Yes, if you could continue, please.

W So with privacy impact assessments, as I said, 25% answered "Yes" to all questions across the sector. However, there was a higher rate of maturity in the departmental and Hospital and Health Services sector, so for departments, which I know the agencies are in this hearing, most of which are, it was 50 – around 50%. And for the Hospital and Health Services sector, it was around 60%. So there was a high level of maturity in those particular sectors. Yes.

So that is of key concern for us, because it's a key message that we feel we really need to get through to agencies in terms of their -- the importance and the benefit, really, in managing those risks for the agencies and the community in adoption of technology, but new policies, projects. And, really, it is just a key tool for ensuring you think all the way through from the design stage -- and I know you will talk further with Mr GREEN later about this, but actually identifying what your personal information that you intend to use through a process and what the likely risks are and how you can address those risks.

So it is really turning people's minds to what's involved. And that's really what we don't see in some cases, and then people get to the end and there's a story on the front page of the newspaper, unfortunately sometimes, and that's because the community have reacted or we get a complaint because someone was really surprised by what occurred. And people just didn't really think about it because they hadn't gone through that exercise. So it's really ensuring that you build that in and into the whole process so that you turn your mind to: what are the impacts? Do we really need to collect that information? Is it necessary for what we're doing? And what can we do to ensure that we respect privacy throughout this process?

CA And there was a survey by the Office of the Australian Information Commissioner, and the published survey is entitled Australian Community Attitudes to Privacy Survey from 2017.

W Yes. Thank you.

CA I tender that document.

PO Exhibit 174.

ADMITTED AND MARKED EXHIBIT 174

CA (i), that provides a summary of the results. Could you go through that summary?

W I think the key things for this particular hearing here that are of note, we talked about trust earlier, and I think that's really fundamental here in terms of how people feel about their privacy more and more. I note that this survey was in 2017. I think that there's been significant developments since that time that have probably even heightened people's expectations around privacy since then.

So back in 2017 when this survey was conducted, 1 in 6 people, so 16%, of the respondents said they would avoid dealing with a government agency because of privacy concerns. And as I said, given people can't always elect to access a service from another provider, they don't always have that choice in terms of government services, and also while that may be stated, sometimes government generates the information about us. It's not necessarily that we have the option of whether they can collect it from us.

So I think it's a really high threshold in terms of that trust that we place in government to -- as custodians of our personal information. And we do see the difference there. So we really need to take that very – that responsibility really seriously, and that needs to really be borne in mind that – particularly, that it's the community's personal information. It's right across all the sector that's caught by this Act. It's not the agency's information, it is the community's personal information.

CA So there's quite a lack of distrust there throughout the public with respect to-

W I think it's concern, which can lead to distrust, certainly. It's a very fine line. And if you have one incident that can get a lot of publicity in particular, even within a local community; for example, if a local government has one breach that people can relate to and think, well, that could be me, or does that mean that they wouldn't be handling my information securely or in a respectful manner, does that mean that somebody can be looking at my information, anybody can access that database, it certainly diminishes trust.

CA And on page 13, there's a further problem, a further hurdle in that when someone does want to report, a lot of the time they don't know where to go. Could you just talk to the Reporting Problems portion of that page?

W Yes. So there's – people were asked which agencies they would report misuse of information to, and only just over half of people were able to actually

nominate any organisation. So that's – most often people thought I would report it to the police. And you can see that there's a range of organisations, such as ombudsman and so on. Privacy Commissioner (federal or state) is only 7%. But people really aren't quite sure what to do in this space as yet. So that was 2017, but -- and this is across a different jurisdiction, which includes the private sector as well. But, yes, there's certainly, in terms of the community awareness and concern, there are a couple of issues there, I think.

CA I tender that document.

PO Exhibit 175.

CA You've touched on a couple of these aspects and I'm going to your submission now, paragraph 13. You talk about the record-keeping obligations under a couple of Acts. Could you expand on that?

W Yes. Well, when we look at right to information, information privacy, it really is more holistic in the sense that you need to start from the ground up, you need solid information management across the board. And we really need public sector employees to have a comprehensive understanding of their obligations to keep the public records in an appropriate manner, because otherwise your right of access and your right to information privacy really aren't as effective as they should be.

So, we certainly expect agencies, when we're doing our audits, to have a broader information management governance in place. Of course our jurisdiction focuses more in on the Right to Information/Information Privacy Acts, but in terms of the general awareness training that we focus on in our training services, is that where you would like me-

CA Yes. So with training, you mentioned earlier that your proposal, or your recommendation to the agencies was some induction-

W Yes.

CA -and regular mandatory specific information privacy training.

W Yes. So we conducted an audit which we tabled in Parliament in February this year, which was about awareness of privacy obligations, which really focused on training and education of employees about the privacy obligations that the agency has. And we looked at three different agencies as part of that, but we came out with recommendations for all agencies across all sectors. And we communicated the outcomes to all agencies at that time.

And the four recommendations were that they include information privacy and information security training in the mandatory induction process for all employees; they mandate periodic refresher training on information privacy and information security for all employees; they ensure the training content on

information privacy and information security is comprehensive, contemporary and tailored to the agency's context. And I note that bearing in mind many agencies have their own confidentiality requirements and legislative context, so it's important that they tailor that, but also that it's practical and related to not just the broader agency perspective, but the specific functions that the employees are working within. And that they implement systems and procedures to ensure all employees complete mandatory training when it is due.

And that final recommendation, we noted very different results based on whether or not they followed up on whether the mandatory training had been completed. For example, one of the agencies that didn't follow up, had a 15%, if I recall correctly, completion rate. Whereas other agencies that followed up well had a significantly higher completion rate.

So having systems in place. A lot of agencies have automated systems that send out emails. I know we do, we get the emails if we haven't completed our mandatory training within the specified timeframe. It really helps ensure that people complete certain training within – the mandatory training within the timeframe and they don't just forget and it slips.

So there's a range of things that can help ensure the success of those programs. But the tailored training, I think, is really important. And we, within our functions, provide training, but also we have free online training, including privacy -- general privacy awareness training, which includes some scenarios to help people understand how it applies generally, of course, because it is for all agencies, but we also have some, sort of, activities and general assessment towards the end of the training. But that's -- you couldn't rely just on that because it is very high-level general awareness training, it is not tailored to the agency environment. It is expected to be part of an overall scheme.

We do go in and provide face-to-face tailored training that we tend to co-design with an agency. And often some of our officers will go in and do a day where they're spending some time with the HR section, some time with people, perhaps, in procurement, different areas, and some time with the executive team. Really, it is training, but it is also very much engaged in terms of the scenarios that they tend to be working through beforehand with the privacy and right to information officers as to what's coming up right now, what's relevant to our work. And I think that that's where it tends to be really successful because it is more engaging, and it's really relevant and it will actually be applied and useful. And we know that a lot of agencies do that themselves because the large agencies have their own teams and they are very highly skilled and able to do that themselves.

We also do face-to-face training that people come along to on various topics, including privacy impact assessments. That's a core session that we hold at least once a year, if not a couple of times, and we do it as a webinar for people that can't attend, including our regional agencies sometimes can't attend. And we have videos. And we have a range of things that can cater to and be concluded

within people's training. We find that agencies often ask us if we've got some videos that they can include within their training program. So I think it really needs to be tailored and useful and a comprehensive suite of training that is relevant to the environment.

CA And with that recommendation you made after examining the agencies earlier on in the year, when was that recommendation made?

W In February 2019.

CA Okay. And which agencies, even though it was-

W That we audited?

CA Yes.

W Yes, it was the Public Trustee, TAFE, and Department of Communities, Disability Services and Seniors.

CA But you made it be known that it was something across all public sectors?

W Yes.

CA How did you do that?

W So we wrote to all CEOs.

CA Yes.

W Yes. So we had specific recommendations for each agency, and then the set of recommendations for all agencies as well that I just mentioned, and we communicated those general recommendations as well.

CA And when did you communicate that to all of the Chief Executive Officers or Director-Generals, Commissioners?

W It would have been within a couple of days of tabling, so in February.

CA In February. And I take it that that went out to all of the seven subject agencies for examining?

W Yes, it would have.

CA In paragraph 15 of your submission, you talk about leadership being critical having found that from compliance audits, reviews and surveys. Could you explain a little bit more about what is so critical about leadership?

W So across – from our audit perspective, and we've noticed this across a range of our experience in our statutory functions, but we've seen it come through our audit, a range of audits, from self-assessment through to compliance audits, where we go in and we do a comprehensive test program. There are parts of the test program that relate to the leadership, which actually look at how the leadership team and the culture and so on is driven from the top.

When an agency is performing well in terms of leadership, we tend to find that overall the agency performs much better. It's really a clear trend. And we've seen that from, really, the very early stages of us performing that function. And it's certainly been the case when we look across the self-assessments and so on.

We also would say that we experience that when we're talking to leaders and their staff. You can see when the leaders, when that you talk to the CEO and so on, and then you actually go and talk to their team and you see that they understand that transparency and openness as well as specifically right to information privacy is considered an important value of the organisation, and what the expectations are, and they tend to have all the right governance and processes and policies in place.

There might be some gaps along the way, but they are also committed to ensuring that they get that in place. So it might be that they have the practices in one area, but they haven't yet got the policies in place. And when we conduct those types of audits, they tend to have implemented most of our findings before we get to reporting stage, or certainly before it is tabled. So there is a clear commitment all the way through, and the team knows that this is important and why it's important, and that it's important because of who they are and their role and what they're doing, and who they're here for.

CA At paragraph 16 you say that you consider training, cultural change, penalties reflecting the seriousness of the unlawful access and disciplinary proceedings being important components to the framework to deter employees from unlawfully accessing personal information. Could you expand on that a little?

W Yes. So one of the things with the Information Privacy Act is, of course, its obligations for the agency. And it needs to be clear to everyone that, throughout the agency, that while it is the agency's obligations, it's – everyone has a role to play through that, and I think that comes through the training and the culture and so on.

But if there's no consequences for people, and that's not clear through the various processes, it certainly has an impact, I think, on the success of the agency in that respect. And I know that we discussed that in some detail. And you may be talking to Mr GREEN about that in a bit more detail further.

CA Yes. .

W But I think that that is an important aspect of this. And in terms of the remedies for people, it's an interesting one because ultimately for most people, once the harm is done it is irreversible damage for – in many cases. And it's – there's very little that can really provide a great remedy. But people will look for some sort of remedy in some cases. And sometimes it will be an apology. It's acknowledgment that the agency's done the wrong thing, and you have had an impact on me. And I think that's where, like we mentioned before, that communication afterwards, and the harm that can come from the poor communication and handling of the notification of the breach, or the failure to notify somebody and they find out through another way, that can really go to how that process works its way out.

Sometimes there will actually be real cost to somebody as a result of what's occurred and – sorry, sorry, I shouldn't say "real cost", I mean actual costs in terms of incurred to the person. So there's a range of things that need to be considered in that area. And I know that that's been canvassed across these hearings. And the Privacy Commissioner will talk about that further shortly, but all of that framework is a really important part ensuring that this is dealt with appropriately. And I think that those aspects need to be fully understood by the employees of an organisation as well, because if they don't understand the harm and the consequences, the harm to the individuals and the consequences for them as employees, it doesn't really hit home either. So it's really a more holistic part of the puzzle.

CA Just going back to self-assessments. You mentioned that with the report tabled in June this year that the agencies were to do self-assessments. You communicated that with the-

W Yes.

CA -Director-Generals, Commissioners, Chief Executive Officers of all of those agencies?

W Yes, we did. So shortly after tabling of the report in Parliament in June, we – I wrote to all CEOs of all agencies, including those that didn't respond to the self-assessment. So there was a slightly different communication with them.

But the first group that had participated in the self-assessment, we provided a summary of their results at a relatively high level, but it was a summary of their results and drawing their attention to the key themes of the report and what we wanted people to focus on in terms of the emerging risk going forward. Which are really summarised in the Executive's summary on page 1 of the report.

We also invited them to approach us if they wanted to, get a detailed heat map of how they were travelling, relative to their results across all four self-assessments across the 10 years. And a number did. And we were also, as we go out and meet with agencies over the past little while, we've been

proactively taking that even if they haven't requested one and discussing it with them.

We – in that communication, I also said that I encouraged them strongly to repeat the self-assessment and as part of their internal audit program and report it through their – their progress through the audit committee and their leadership teams. And I think -- and that's something that we've been talking to people a lot about in terms of, really, "This is your responsibility." And we've been doing that for a long time. We've had the self-assessment tool on our website and we've done training for internal auditors, and so on, for a long time about how to complete it themselves. Some agencies have said to us "It's really big." We've said, "Okay, we'll focus on the high-risk areas for you. Chunk it up, take the bits that you didn't perform so well in, and what are the key risks this year in your internal audit program." Perhaps in the privacy impact assessments. But different agencies have different key risks. So they don't need to repeat the whole self-assessment, but there are different aspects that they can focus on as part of their internal audit program. It really is core business, and they need to treat it in that way. And I think that that's – you know, 10 years in we can't be looking at privacy as an add-on anymore, particularly with the risks that it presents verses not managed well and the community expectations and the risk to diminishing those expectations.

CA Thank you very much. I don't have any further questions.

PO Thank you.

Thank you for coming. You're excused. .

W Thank you, Chair. Thank you.

CA Chair, the Exhibit 175 has already been tendered -

PO 174, was it?

CA Yes.

PO Yes.

END OF SESSION