EDUCATION, EMPLOYMENT AND TRAINING COMMITTEE

Members present:
Ms KE Richards MP—Chair
Mr JP Lister MP
Mr MA Boothman MP
Mr N Dametto MP
Mr BL O'Rourke MP
Mr JA Sullivan MP

Staff present:
Mr R Hansen—Committee Secretary
Ms H Koorockin—Committee Support Officer

PUBLIC HEARING—INQUIRY INTO THE INFORMATION PRIVACY AND OTHER LEGISLATION AMENDMENT BILL 2023

TRANSCRIPT OF PROCEEDINGS

Monday, 13 November 2023

Brisbane

MONDAY, 13 NOVEMBER 2023

The committee met at 10.30 am.

CHAIR: Good morning. I declare this public hearing open. My name is Kim Richards. I am the member for Redlands and the chair of the Education, Employment and Training Committee. I want to start by acknowledging the traditional owners of the land on which we meet and pay my respects to elders past, present and emerging. We are very fortunate in this country to live with two of the world's oldest continuing living cultures in Aboriginal and Torres Strait Islander peoples whose lands, winds and waters we all now share. Other committee members with me here today are my deputy chair, Mr James Lister, the member for Southern Downs; Mr Mark Boothman, the member for Theodore; we hope to have Mr Nick Dametto, the member for Hinchinbrook, joining us shortly; Mr Jimmy Sullivan, the member for Stafford; and Mr Barry O'Rourke, the member for Rockhampton.

Today's hearing forms part of the committee's inquiry into the Information Privacy and Other Legislation Amendment Bill 2023. The Hon. Leeanne Enoch MP, Minister for Treaty, Minister for Aboriginal and Torres Strait Islander Partnerships, Minister for Communities and Minister for the Arts, introduced this bill in the Legislative Assembly on 12 October 2023. The bill was then referred to this committee for its consideration. The committee has received eight submissions on the bill which have now been published on the committee's website. Today we will be hearing from some of the stakeholders who made submissions to the committee. Would any members like to declare any interests relevant to today's proceedings?

Mr SULLIVAN: I would just note that I have had previous professional dealings with the LGAQ, including Ms Smith, but nothing that would preclude me from dealing with issues today.

CHAIR: Thank you, member for Stafford. The committee's proceedings today are proceedings of the Queensland parliament and subject to the parliament's standing orders. The proceedings are being recorded by Hansard and broadcast live on the parliament's website. Witnesses will not be required to give evidence under oath, but I remind everyone that intentionally misleading the committee is a serious offence.

SMITH, Ms Alison, Chief Executive Officer, Local Government Association of Queensland (via teleconference)

SUTHERLAND, Mr Angus, Lead, Intergovernmental Relations, Local Government Association of Queensland (via teleconference)

CHAIR: I now welcome our first witnesses on the phone from the LGAQ. Good morning and thank you for joining us here today via phone. I invite you to make some opening comments, after which the committee will have some questions for you.

Ms Smith: Good morning and thank you for inviting the LGAQ to participate in this hearing. I, too, would like to firstly acknowledge the traditional owners of the land on which we gather and pay my respects to elders past, present and emerging. Joining me today is Angus Sutherland, our intergovernmental relations lead.

As you know, the LGAQ is the peak body for all local governments across Queensland. To get started in our opening remarks, local government operations are becoming increasingly digital and councils very much understand the need to safeguard information, and that is a key priority. Accordingly, that is why local governments are turning their minds to the growing threat of cyber attacks and the need to direct their resources towards cybersecurity to protect information. They are doing that now and it is why a key plenary presentation at last month's LGAQ annual conference included the guest panellist Rob Champion, who is the Queensland government's Chief Information Security Officer.

Local governments are facing considerable budgetary challenges, however, to mitigate and manage cyber risks. They are aware of it, they are doing it and they have to weigh up what is required to dedicate resources where they are needed and weigh it up against the provision of other community services. They are doing that now. While we understand that the objectives of this bill are about further measures, we want to draw the attention of the committee to the fact that the operating

environment of local government is different to state government and this new regulation would pass on a considerable new financial impost to councils. What I mean is that the expected costs for local councils, if they were to adopt a single set of privacy principles and if they were to adopt a mandatory data breach notification scheme, will cost and we are not confident that they can be achieved in the time frames that this bill proposes.

We also believe that there is a significant and huge unintended consequence with what is being proposed because we believe that extending these obligations to contracted service providers and subcontractors will place a further administrative burden on councils and this could serve as a significant disincentive for local businesses to be working with councils. As I say, that to us is a huge unintended consequence because councils are focused very much on how they can buy and support from local businesses. It is why the LGAQ set up Local Buy as a subsidiary and as a procurement aggregator and it is why the state government itself has this year signed up to use Local Buy as its single procurement solution. As drafted, this bill will increase the regulatory burden on councils, on their local partners and on their suppliers, so we do not see the aims or the time frames that are being proposed are achievable and we shudder at this unintended consequence.

Our submission includes three recommendations that we feel would make this legislation more workable for local councils: firstly, that council-specific codes and guidelines could be developed to ensure that the requirements on councils are consistent and fit for purpose and do not put unreasonable costs on already strained council budgets. Councils are not resourced like a state government is. They are different and this does need to be acknowledged. Secondly, we recommend that councils in Queensland continue to be subject to the current voluntary data breach notification scheme. They are currently doing it, but if they had to move to a mandatory scheme then we are saying that local governments should be given an exemption to this. Finally, our third recommendation is that we feel a process should be established to allow council service contractors and their subcontractors to apply for waivers or modifications to privacy principles requirements.

With these three recommendations, we are seeking to make constructive suggestions to the state government and to avoid what we feel would otherwise occur, which is a heavy-handed approach that will set up councils to fail and which will have that unintended consequence of reducing local purchasing and of reducing how councils are supporting local businesses. With those opening remarks, I again want to thank the committee for its consideration. That concludes my opening statement and we are happy to take any of your questions.

CHAIR: Terrific. Thanks, Ms Smith.

Mr LISTER: Thank you very much, Ms Smith, for your appearance today. What would the likely cost impact be for a council to implement a mandatory scheme and would that be common to all councils so that a smaller council would effectively face the same implementation and management costs as a larger one?

Ms Smith: I thank the committee member for the question. It is a good question because it is one of the key bases of our opposition to what is being proposed. It is a hard one to answer because we think that if the state government is going to move towards having this type of scheme councils are going to have to do a degree of work to understand what would be involved. They would need to understand whether there would be sufficient time to (inaudible) appropriate staff, would they have existing staff who can be trained, what that looks like, what the time frame would look like and how they manage workforce and training issues when, as you say, in those smaller and rural and remote councils we know that we have a skills set problem, so there is a scarcity of skills in the market. This is the reason (inaudible) solution of funding that could be used towards a centralised cybersecurity operation centre for all local governments as a shared services concept. This would mean that we would have a centralised approach to local government cybersecurity management. You could be sharing those resources and therefore not having the issue of not having the skilled people in the individual communities and you would therefore be able to improve response preparations for local government infrastructure.

Mr LISTER: Thank you very much.

Mr BOOTHMAN: Thank you for your very comprehensive support so far. When it comes to the skills shortage, which we are seeing well and truly throughout Queensland in a lot of sectors, what types of incentives do you think the LGAQ would feel would need to be pursued to get individuals to work in these council areas in, say, places like Quilpie where there are very small councils where the CEO is the local steamroller/operator, so to speak? How can these types of councils attract those individuals?

Ms Smith: Thank you, member, for another great question and it does go to the heart of what we call the new wave of issues confronting Queensland at the moment. It is a wave where you have cost of living, you have a housing crisis and you have a lack of relevant skills based in communities across the state. It is one thing to attract skilled workers to a community; it is another to be able to have the housing to accommodate them and their families, so it is rather a complex and intertwined issue that we are facing. I do want to also point out that in our proposal in terms of what we are saying to the committee we are not saying that councils should be notifying. Rather, what we are saying is that it is about enabling councils to continue to notify (inaudible) today which is voluntary without having onerous reporting and difficult financial imposts, and we are concerned that if that happened ultimately it is the ratepayers who would have to pay.

Mr BOOTHMAN: So there are no incentives for councils in terms of government funding, state or federal, where they can apply for grants to help cover these costs? Is that in the equation at all?

Ms Smith: We are not aware of anything that exists to that point. We have certainly made previous budget submissions for both federal and state government funding for cybersecurity initiatives for councils, but we are not aware of any grants that you are talking about that would help to attract these types of skilled workers to those communities.

Mr BOOTHMAN: So it would be just a pure impost on the ratepayers then?

Ms Smith: If there is a whole lot of red tape and new onerous reporting requirements that are put on councils, councils will have to have the appropriate resources to undertake that work and if it requires further skills or training or different employees then that is additional cost. At the end of the day, if there is an absence of state or federal funding to compensate for what is now being asked of councils, councils would have no option but to have this go through to rates increases which will impact their ratepayers.

Mr SULLIVAN: Ms Smith, in terms of resources, the committee has been briefed—and it is published—by the department that the OIC itself will be receiving resources for the purpose of training and rolling out this implementation and that the mandatory requirements will not come into place until 2026, I think it is. So with those extra resources from the state government, does that not help your members? Whether we are talking about smaller councils or larger councils, whether it is a CEO or a delegated officer, doesn't that extra support from OIC itself help in this particular point?

Ms Smith: I thank the member for the question and say that we have a really good relationship with the Queensland government Chief Information Security Officer, Rob Champion. He has made a strong virtue of talking to us about what is available to support councils that is either low cost or no cost. With regard to the money that you are talking about—the funding—we are not aware of how much that would be and how appropriate that would be to cover what would be needed through what this bill is proposing and whether or not it would be for all 77 councils. It is certainly one thing to train people to do a new piece of work, but a new piece of work itself is an additional resource that the council would have to undertake.

CHAIR: I would hope, as a ratepayer, that councils already have in place cybersecurity that protects the data that councils would hold on ratepayers and its businesses within its communities. I would like to think that this would just be building on their requirements. In terms of the current system, if it is a voluntary scheme, do you have any information on how many councils voluntarily reported data breaches—knowing how big cybersecurity is across agencies and businesses alike throughout Queensland and throughout Australia?

Ms Smith: As I said in my opening statement, councils are acutely aware of this growing need and that is why we are doing work in this space. It is why we made it a focus of our annual conference as a keynote session last month. I do not have information available to me today in terms of how many councils are voluntarily reporting or notifying, but certainly that is the system that is in place today.

CHAIR: There is no data at the moment on the number of times any particular councils have voluntarily provided data breach information?

Ms Smith: I do not have that for you.

Mr DAMETTO: Thank you both very much for your comprehensive opening remarks and for your submission to the committee. Has the LGAQ done any work to quantify what the implementation of this proposed bill would cost different councils, understanding that we have different councils and different, you could say, bandwidths: large councils across Queensland, city councils, all the way through to the smallest regional councils" Has the LGAQ done any work in that space to quantify what this is going to cost, not just for the implementation but long term?

Ms Smith: We have not undertaken that sort of research. As I mentioned before, if this proposed bill and its regulations were to go down this path, the very first thing that would have to happen would be to understand what the workforce challenges are for councils—whether they have the staff with the necessary skills to comply with the mandatory breach notification scheme; and, if they do not have them, how would they get them and what would the ongoing focus look like. It will also depend on the new guidelines, which we would need more information about. That is why we go back to our proposal that the current system is in use, councils are aware of the issue and they are doing more and more in this space and that already is a juggle between how much they have to expend on that activity versus other services that they provide in their communities. That is why we are incredibly grateful to have a great relationship with Rob Champion and the cybersecurity unit. We appreciate what they are doing to help. The LGAQ has been running cybersecurity maturity assessments across Queensland councils. We have been doing that to help to inform their ongoing work to focus on cybersecurity maturity. I mentioned earlier that we have put in a proposal for a centralised security operations centre for councils. We estimate that it would cost $300,000 a year to do the job for all 77 councils. That does not include organisational resources and training.

Mr DAMETTO: Off the back of that, local government being a product of state government, do you think there is a responsibility on the state to help out if there is perhaps to be a centralised resource or pool of resources to try to manage this long term?

Ms Smith: I think there are responsibilities at both state and federal level. Certainly there are different areas of support and agencies at both tiers of government that could help local government in such an event. I guess I would keep going back to what you are talking about today with this bill and that is that the regulation is a change at a state level. If there is a change at a state level that impacts councils, and councils are quite different to state government agencies in the way they are set up and resourced, then to compensate for those changes there would need to be appropriate support from the state government.

CHAIR: I want to confirm that you have not had a chance to read the department's response to some of those issues that you have raised within your submission?

Ms Smith: No.

Mr O'ROURKE: With regard to contractors and subcontractors, the department has advised the committee that the proposed mandatory data breach notifications only apply to the agencies and not the contracted services or subcontractors. Does that alleviate some of the concerns of the LGAQ about the impact of the proposed mandatory reporting when it will only be on the agencies and not on the contractors?

CHAIR: That specifically refers to the Local Buy scheme.

Ms Smith: No, it does not alleviate our concerns because obviously if you have contracted service providers and subcontractors who have to be subject to these obligations, what it means for councils is that they have a further administrative burden to ensure that the contractors or the contracting agencies are compliant with the legislation and they are not in breach of their obligations. We see that that creates a disincentive for small local businesses to be contracting with councils.

Mr SULLIVAN: I am not sure if you have had a chance to read the other submissions to the committee's inquiry, but can I refer to the CCC's submission. We have spoken a lot today about smaller councils. We are probably talking about larger councils in the context of questions when it comes to council controlled entities. Do you have a view one way or the other on whether or not this proposed mandatory reporting system should apply to council controlled entities?

Ms Smith: I have not had a chance to read other submissions to this committee so I would be happy to take that question on notice and come back with some more fulsome comments.

Mr SULLIVAN: Thank you. I was about to ask that. That would be helpful.

CHAIR: Thank you very much, Ms Smith and Mr Sutherland, for appearing before us today. We note that there has been one question taken on notice in regard to the controlled entities of councils. For questions taken on notice, we would appreciate getting those responses by close of business on Monday, 20 November 2023. Thank you again for appearing before us. We appreciate your contribution.

BOOTH, Mr Paxton, Privacy Commissioner, Office of the Information Commissioner.

RICKARD, Ms Anna, Acting Right to Information Commissioner, Office of the Information Commissioner

WINSON, Ms Stephanie, Acting Information Commissioner, Office of the Information Commissioner

CHAIR: Good morning and thank you for agreeing to appear before the committee today. I invite you to make a brief opening statement and the committee will then have some questions for you.

Ms Winson: Good morning. Thank you very much. We appreciate the opportunity to speak to you today in respect to this bill. Before I start, I would like to acknowledge Aboriginal and Torres Strait Islander peoples as the first Australians and recognise their culture and deep connection to the lands, waters and seas of Queensland and the Torres Strait. I also wish to acknowledge the Turrbal and Yagara people as the traditional custodians of the lands on which we meet today and pay my respects to their elders past, present and emerging.

My name is Stephanie Winson, and I am the Acting Information Commissioner. I am joined today by Mr Paxton Booth, the Privacy Commissioner, and Ms Anna Rickard, the Acting Right to Information Commissioner. We have made a written submission to you and I will assume that you have had the opportunity to consider that submission so my remarks today will really just be focusing on a few key aspects. Before I make substantive comments, I do wish to acknowledge the work of the Department of Justice and Attorney-General in their consultation and engagement on this bill.

If passed, this bill will modernise the information protection framework in Queensland and it will certainly streamline the information access processes that are currently in law. In our view, it addresses a number of the recommendations and a number of findings, which the explanatory notes certainly sets out. This, in particular, includes the recommendations made by Professor Coaldrake in his review of culture and accountability in the public sector—recommendations such as the mandatory data breach scheme and the release of cabinet documents.

In respect of the Information Privacy Act proposals, our submission addresses a number of subtle yet important aspects which will, in our view, strengthen the legislation by providing, in particular, the necessary regulatory tools for the Office of the Information Commissioner. These are outlined on pages 2, 3 and 4 of our submission. We have also drawn attention in our submission, as others have, to the continuing review of the Commonwealth Privacy Act. It remains our view that it is highly desirable that there is consistency in national privacy legislation, but we do recognise that that review is still ongoing and it is in Queensland's interests to advance this legislation now. Given that, we do urge government to continue to actively monitor those Commonwealth amendments and be prepared to make further amendments to the legislation in Queensland for harmonisation.

In respect of the proposed changes relating to the Right to Information Act, our submission also raises a number of important and technical issues which we consider relevant to the effective operation of this legislation. A number of those relate to drafting which we suggest will improve clarity for agencies and give certainty regarding the Information Commissioner's regulatory powers and functions. These points are made on pages 7 to 9 of our submission.

Finally, there are two points in our submission that relate to community rights and interests and I will mention those very briefly. The first is on page 7 of our submission and it relates to the proposed amendments to defining the processing period for access applications. While the proposed changes provide certainty, it makes no particular provision for effective remedies for applicants who make noncompliant applications in a context in which the agency then appropriately fails to action that noncompliance. In our view, this lacuna is essentially undermining the overarching intent of the legislation.

The second, which is mentioned on page 10, is the opportunity to recognise, through the addition of dedicated public interest factors favouring disclosures, the significance of government held records to Aboriginal and Torres Strait Islander peoples. We consider that there could be value in incorporating this into the RTI Act as public interest factors favouring disclosure which is expressly recognising that significance. Thank you very much for listening and we are happy to take any of your questions.

Mr LISTER: Thank you very much for your appearance today. Can I take you to page 4 of your submission. At the top, you speak on the one hand that the bill proposes to give you the power to make preliminary inquiries of persons in certain circumstances, but it does not give you the power to

make preliminary inquiries regarding privacy complaints of persons other than the respondent and the complainant. In the following paragraph, on my reading, it says that you do, in fact, have that power. I am sure you are making a logical point there, but could you run me through that please?

Ms Winson: I will pass to my colleague, Mr Booth.

Mr Booth: The difference in the powers relates to the different functions within the act. The first one, at the top of page 4, is in relation to the powers to mediate a privacy complaint. In circumstances where a member of the public has a privacy complaint against an agency and they cannot resolve that complaint or they do not get a response within 45 business days, they can contact the OIC. We can attempt to mediate the complaint with the department and with them at the same time. What we are suggesting here is preliminary inquiry powers to contact or speak with not just the complainant and the department but also third parties who may hold relevant information.

The other paragraph you referenced was in relation to our function for mandatory data breach powers or investigations. In that instance, the bill does contain powers to make preliminary inquiries for a broad range of people. We are seeking the same, I suppose, scope of powers in relation to our complaints mediation powers as well.

Mr LISTER: When you are talking in the first instance about the distinction between persons other than the complainant/respondent, am I to take it that the complainant would be somebody who feels they may have been the subject of a breach but there could be a third person who is aware that a breach has occurred; is that correct?

Mr Booth: Essentially, yes. If the complainant is a person who has been impacted by an allegation of a breach of the privacy principles by an agency, we are talking about third parties so a person who is not impacted by a breach but may have relevant information about a potential breach.

Mr DAMETTO: Commissioner, from your point of view, why is this legislation required in a world where we are seeing more of our data go online and more of our data becoming available and the increased threat of cyber attacks?

Ms Winson: Our view is that fundamentally policy views on cybersecurity are not for us. In the context of our jurisdiction, it is important that Queenslanders have assurance and confidence in public sector agencies that hold their data that they are doing so securely and are maintaining security and are notifying if there has been a breach. I will check if my colleagues wish to add anything to that, but that would be our general view.

CHAIR: I would add that it has been interesting to watch in the media over the past few days the reporting on Optus and what has happened in terms of consumer and customer confidence, given that people are walking away from Optus on the back of those data breaches. That has been interesting reporting to read.

Mr O'ROURKE: The previous submitters, the LGAQ, want it to remain a voluntary data breach requirement for reporting. To what extent do the councils currently report voluntary breaches?

Mr Booth: I was listening intently and did contact my office. That is the benefit of mobile phone technology. Last year we did have 11 breaches reported by two councils. A total of 40 data breaches were reported to our office last year and 11 of those related to councils.

CHAIR: What happens when they report a breach? What does the process look like and how does that feed back into the average ratepayer who has had their data exposed?

Mr Booth: At the moment that is a matter for the councils, whether they go forth and contact the people who have been impacted.

CHAIR: So there is no requirement to do that?

Mr Booth: There is no requirement at this stage for them to do that. I must say, the majority of breaches, in my experience, have been what I would describe as low level in the sense that they are not of the nature that we are seeing in the media about Optus and Medicare. They are not of that size or volume. Often they are breaches that have been caused by someone sending an email to the wrong party with confidential personal information in it. In those circumstances, it is relatively easy to contact a single person or a few people who have been breached by that kind of action.

In terms of the council response, what we generally do when we receive a complaint is contact the council. Actually, our form gives them an opportunity to indicate whether they would like contact from us. In the past we have contacted and provided advice on whether they should be contacting the relevant parties, the types of information that may be pertinent to advise the affected people about the breach and how they can support them.

Mr O'ROURKE: If data breach reporting is to be mandatory, do you have any thoughts about what improvements that would make for councils around their data security information provision and that sort of thing? Do you have any thoughts there?

Mr Booth: Not just for councils but for any agency, the introduction of a mandatory data breach scheme has the benefit of uplifting trust in the community that our information is being managed appropriately. The significance of data breaches really cannot be understated and they can impact people in all kinds of different ways. What I would say in response really is that it is an increase in trust. It also brings an increased oversight to the agency itself by having to maintain, monitor and report those data breaches. At the moment, one of the gaps that we have is that we are not really clear about the visibility of data breaches inside agencies and how well they are being reported internally. I think the introduction of a mandatory data breach scheme would help improve that governance around breaches and how agencies are responding to them.

Ms Winson: The other thing is that there are significant harm risks to members of the community if their data is breached. The example that is front of mind for me is victims of domestic violence. If that information is given to the wrong person, their inability to know that their data has been breached and to take appropriate action to protect themselves is significantly magnified. That is an example of the value of that breach notification.

CHAIR: Given that it is only a voluntary scheme, there is no requirement on councils to actually report that sort of interaction currently. There is no audit type process of councils in terms of what their cybersecurity profile looks like, is there?

Mr Booth: Not that we undertake. Whether someone else undertakes an audit on their cybersecurity protections I probably am not able to comment on.

Mr BOOTHMAN: You were talking about human error in data breaches—accidentally sending emails. What other type of data breaches were reported from councils recently?

Mr Booth: I am told that all of them involved human error apart from one which was a software glitch in relation to the migration of some data from one database to another.

Mr BOOTHMAN: To solve that issue, better training and understanding of sending emails may be appropriate to make sure that that does not happen again. That brings me to my next question. Having professional IT staff really will not solve that problem because people will make errors from time to time. My concern is around how we are going to fund the smaller councils to attract IT professionals to the more remote areas to look after their IT systems. Are there going to be incentives put forward? How does the department envisage solving that issue?

Ms Winson: What the department envisages I do not think we can comment on and I am sure they will. We can say that the Office of the Information Commissioner provides considerable resources and assistance to agencies in relation to the obligations arising under this legislation. What you have described fundamentally goes to the heart of culture more than IT, although the two will go together—systems and processes support. We certainly spend quite a considerable amount of our effort, time and resources, as part of the role of the Information Commissioner, to support agencies to meet their statutory obligations. It is envisaged that, if this legislation passes, we would provide a significant role in assisting agencies to meet those obligations.

CHAIR: Following on from that, presumably in the corporate world not everything is done internally and you will use external consultants, depending on the services that you are procuring. I would imagine that it is not a one size fits all for every council in terms of how they deliver their IT cybersecurity. It might be that they have internal team members delivering that but they similarly might engage external consultants to assist with cybersecurity?

Ms Winson: I am not sure we could comment on that, but, presumably, that would be the case.

Mr SULLIVAN: I want to come at this from a different perspective, which is the other side of privacy. There is a need to share information in government. When it comes to particularly vulnerable people, for example, there is a need for sharing information on health, housing, education, engagement and the like. Obviously, council plays a role in that when it comes to housing or engagement with community organisations et cetera. Is there anything in this legislation that would put up a barrier to councils and/or state agencies sharing information for a legitimate purpose? Does it send a signal to not share information when we want people to collaborate?

Ms Winson: I will go first and then open up to my colleagues as well. I think fundamentally the Right to Information Act and the incorporation of the Privacy Act provisions for access to information is part of this legislative proposal and we welcome it because it will bring greater clarity and consistency across the two. The tension between protecting privacy and the Right to Information Act,

which is all about releasing information, is a real and ever-present tension. I think the way that the legislation is drafted it provides a good balance. We are certainly very positively supporting the changes being made to make the synergy between those two statutes much easier for users and, therefore, the implications.

Mr LISTER: You mentioned that you anticipate that your current practice of assisting agencies in complying and dealing with you will continue under this act. Obviously there is going to be a requirement for additional personnel in your agency to be able to implement and oversee this. Can you give an indication of how many extra people might be needed and how you will recruit them given the widely known shortage of cybersecurity and IT professionals?

Ms Winson: I will pass to my colleague Paxton shortly to give you the details, if you would like. We are finalising an updated submission for centrally held funds that were allocated in the budget for this purpose. They have been centrally held because, until the legislation was presented, it was not a given that this is necessarily going to happen.

We anticipate about nine FTEs, additional to our establishment, approximately. Paxton, who is across the figures deeply, will be able to correct me if I have those numbers wrong. Our focus predominantly for the implementation is on the expanded regulatory powers of the Information Commissioner. Most of those FTEs, and ongoing, will relate to that. However, our office already has existing resources that we will supplement through the implementation period to address the introduction of the legislation and then fall back to a standard number. We are not necessarily seeking ICT security specialists in that process. I will pass to Paxton to see if he wishes to add anything.

Mr Booth: The only thing I will add is that we are planning a two-stage process of implementation. We will have an implementation team that will focus on preparing guidelines, information packs, resources and training to the entire sector. It is not just local government; it is all the agencies that will be impacted by the changes in legislation. Post commencement or around commencement we will then move to a slightly different model where we will have team members designed to better enforce the regulatory side of the process, but we will have a focus in probably the first 12 to 18 months on training and uplifting the sector.

Mr SULLIVAN: It is not as if this is the first time that you are going to engage with those bodies. It is just building on the existing work that you do.

Mr Booth: That is right.

Mr SULLIVAN: Your bread and butter.

Mr Booth: We do already have, for example, a privacy champions' network across three different areas: one for the departments, one for the hospital and health services and one for local government. That is an existing network of people within agencies who have taken on the role of being a champion to promote privacy and that will be continuing, obviously. It is a great forum for people to engage and find out more information about the changes.

Mr BOOTHMAN: When it comes to working from home—and since COVID there are more and more people working from home, and I know security specialists in Gold Coast city council as an example would be working from home—what are your thoughts when it comes to security issues, particularly in these less resourced smaller councils?

Ms Winson: The only thing I would say is we are a very small organisation; we are less than 50 people. We are adopting a hybrid working model right now. I think there are some basic steps that all entities, big or small, need to take to ensure the security of information that they hold is protected. I think you can rightsize your offering. It does not require necessarily the large-scale layout that may be envisaged. There are some tools that make that possible.

Mr BOOTHMAN: We were talking about these rightsize tools. How affordable would that rightsize software be for these smaller councils?

Ms Winson: I am not sure I can answer that question. I am not familiar enough with council funding.

Mr BOOTHMAN: They would obviously have portal systems.

Ms Winson: Yes.

CHAIR: As a ratepayer—or anybody dealing with an agency—I would hope that they have existing frameworks that just need enhancing. It is not recreating it.

Mr BOOTHMAN: The issue too is human error which, as Mr Booth alluded to, is the main cause of the breaches.

CHAIR: That has been voluntarily reported on today. Thank you so much for your time and your contribution today. We are all much more enlightened for that, so thank you very much. No questions were taken on notice. Thank you again. We really appreciate your time, your submission and you appearing before us today. I now welcome our next witness.

STEPHENSEN, Ms Nicole, Partner, IIS Partners

CHAIR: Thank you for appearing before the committee today. Would you like to make a brief opening statement and then we will have some questions for you?

Ms Stephensen: I thank the committee for inviting me to appear today on behalf of IIS Partners. Before I take a moment to read from a prepared statement I, too, would like to acknowledge the traditional owners of the land on which we meet today and pay my respects to elders past and present. I would also like to acknowledge that I have travelled to you today from Yagara country where I live near the site of the old Deebing Creek mission, which is a place of profound importance to Queenslanders and particularly traditional owners in this space.

I am here today to speak on behalf of IIS Partners. We are a privacy and data protection consultancy founded by former Australian Privacy Commissioner Malcolm Crompton about 19 years ago. Our organisation provides expert advice to entities on meeting their privacy and data security obligations, managing privacy and security risk and implementing a privacy-by-design approach to technology deployments, product deployment and services. We have worked extensively with public and private sector clients across Australia, including in Queensland and the Queensland government. We bring a practical perspective to law reform, particularly how privacy law is implemented on the ground and the challenges entities tend to encounter. At IIS Partners, I am the partner responsible for leading our privacy services function across Australia and within the Asia-Pacific region.

I would like to acknowledge that privacy resourcing in Queensland agencies varies and so, too, does privacy maturity. Privacy maturity is the ability for our agencies to apply the privacy principles in their decision-making and to be compliant with whatever the privacy law requires them to be compliant with. This includes collecting and managing personal information in accordance with privacy rules but also, importantly, and as we have heard today, community expectations.

I also comment that privacy and information security are not the same thing. I think that is a really important thing for the committee to take away today. However, the bill does acknowledge that these two concepts work in concert with each other and they must work together to support the protection of personal information through its life cycle. At IIS Partners we believe the proposed mandatory data breach notification scheme furthers the intent of robust privacy law and practice. This is while empowering the community with vital knowledge through the notification process around how to protect themselves in the unfortunate event of a data breach.

Finally, it is relevant to acknowledge the importance of the bill from the perspective of modernising Queensland's approach to privacy management. Privacy is too often considered a compliance burden that is to be risk managed by our agencies, and we particularly see this in our lower resourced agencies, including local government. This is largely a navel-gazing exercise for our agencies where privacy risk is seen as a compliance risk. It is seen as the risk to the agency if the agency does the wrong thing in terms of how it collects and manages personal information. There is not often that view from an agency perspective around what that compliance risk does in terms of the flow-on privacy harm to the individuals whom we serve, and in the Public Service focusing on the community we serve is vitally important. At IIS we feel that the bill goes a long way to addressing this.

Mr LISTER: Thank you very much Ms Stephensen. Imagine I am the CEO of the Bullamakanka west shire council and I have 38 staff and every Wednesday it is the CEO's turn to drive the grader and the council is now facing the implementation of the requirements of this regulation. You say that you provide expert advice on meeting regulatory obligations, managing risk and having a privacy-by-design framework. If I am the CEO of that council and I come to you and say, 'We currently comply. We are satisfied. Please steer us through complying with the new act,' assuming this passes, how much will it cost?

Ms Stephensen: This is one of the most difficult questions that we answer for our councils or other agencies at IIS Partners because instead of the proactive and preventative activities of privacy and personal information management, the cost is usually in relation to the reactive and remedial activities. In the event that there has been a data breach or in the event that the community is concerned that something has reared its head in the media, that is where councils now tend to apply their privacy related costs.

Similarly, although councils would say they comply, our experience on the ground has been that anyone with a designated privacy officer role in council, unless you are one of the larger councils, has found that that role has been deviated largely to the management of access to information and correction of information requests made by the public because of the statutory obligation to address those quite quickly. The rest of the privacy function falls by the wayside. A level of at least an AO8 officer to manage the privacy function in a council or any other agency is really the only thing that we

see being the barrier between attempts to comply and appropriate efforts to comply with rules, whether they are new rules or the existing rules and actually risk managing that activity. It would be at least one full-time person.

Mr LISTER: Assuming in the ideal world they have that person and you are engaged by them to steer them through compliance with the new arrangements, what sort of cost are you looking at? While you are at it, since you talked about the real world experience, what is the cost there? Can you enlighten us?

Ms Stephensen: The cost of engaging a consultant will certainly vary depending on the needs of the organisation. Hopefully consultants are not going to charge like a wounded bull for a small 28-person council. We do see variability within the industry. There are only a handful of privacy and data protection consultancies within Australia that work towards on-the-ground compliance. I think it is something that would require a scope of work to understand exactly what it would cost a consultant to provide that service.

CHAIR: In terms of where their current systems are at and where they need to be.

Ms Stephensen: Yes, even some kind of a gap analysis or a maturity assessment, even something as simple as being asked to advise on a technology deployment depends on the nature of the technology. If it is CCTV cameras that are embedded with facial recognition capability, that might be more significant and more costly than upgrading the telephony system.

CHAIR: Possibly not at the Bullamakanka shire council.

Mr LISTER: I think they are getting telephones there next month!

Mr BOOTHMAN: How often do you think government agencies should audit their own cybersecurity? What is the benchmark in ensuring that no breaches have happened at that organisation? What period of time is recommended to look into auditing these?

Ms Stephensen: There are a couple of things. The first is that looking at privacy maturity is different from looking at cybersecurity maturity. The cybersecurity maturity helps to enhance and support privacy maturity, but it is only one component of robust privacy practice. What we often see in many organisations—even larger departments in Queensland—is that maturity sits for the larger departments that are well resourced, say, around a two to a three out of five and there is only a few of those. Other maturity tends to be at a one or a two. We are looking at ad hoc and maybe there are some repeatable activities that are being done in relation to privacy. That says to us that more needs to be done in terms of the regularity of this kind of audit activity but it is expensive to do that regularly if you are engaging externals.

What we always suggest to our clients is to get your house in order as far as possible and as quickly as possible and routinise your own self-assessment internally. That can actually help to eliminate the need for their regular external review—not taking it away altogether because I feel you need that level of assurance, but to routinise that internally. There are some Queensland government departments as an example that do this as a matter of course on a yearly basis. They have a look at where they are at in terms of their privacy program, whether they need additional assistance, whether they need to roll out additional projects. Usually that is in accordance with something like a privacy management plan but not every agency has that.

Mr DAMETTO: Thank you for giving us your very comprehensive opening statement and also submitting to the committee on this bill. Have IIS Partners done any body of work to quantify what it is costing Queenslanders per year when it comes to data breaches, whether in the public sector or private sector?

Ms Stephensen: No, we have not. We do follow the statistics that are released by relevant privacy commissioners that do have mandatory data breach notification schemes. As opposed to the cost, it is more about the cost to the community—the expectations of the community in relation to what is happening with our government. If you look at the Office of the Australian Information Commissioner's community attitudes to privacy survey, for example, they often reference their data breach statistics when it comes to gathering that community sentiment. We are finding that the community is more and more concerned about what is happening to their personal information. That is not just at your usual state agencies level; that is also at local government where you actually see local governments collect, use and rely on vast amounts of information from our community to provide those essential services.

Mr DAMETTO: Have you been able to quantify or have you had any feedback from Queenslanders on how high or low the confidence is in the current state, local and federal governments' ability to protect their data?

Ms Stephensen: No.

CHAIR: Following on from that, I would imagine—and based on what we heard before—it would be extraordinarily difficult to quantify the cost to community because it would be very different. As we heard, if data were released on a person who is fleeing a domestic violence situation, how do you put a value on what that data breach looks like?

Ms Stephensen: No, you do not. What you do instead is aim for the highest possible standard, assume that the community expectation is that their data will be kept secure through its life cycle and take steps as an agency to make sure that happens. The thing about the mandatory data breach notification scheme that is so appealing is that over time those reported instances of data breach, whether or not they are found to be notifiable—whether or not the community needs to be notified—will allow the OIC to have that body of knowledge that it needs to actually start that quantification exercise. We just have not had that in Queensland to this point.

CHAIR: And to continually improve systems.

Ms Stephensen: Yes.

CHAIR: I think it was interesting and telling that, under the voluntary scheme, of the 77 councils we have here in Queensland there have only been 11 breaches voluntarily reported.

Ms Stephensen: Yes.

Mr SULLIVAN: In your opening address, Ms Stephensen, you spoke about the need for agencies to be people centric, as opposed to their own reporting. To that regard, whether you are in a regional council or whether you are in Brisbane or the Gold Coast or Cairns, if you are a DV victim and somebody is released back into your community and somebody has been given your personal information, you deserve to be told about, right?

Ms Stephensen: Absolutely.

Mr SULLIVAN: It does not matter where you live.

Ms Stephensen: Yes.

Mr SULLIVAN: I think you raised that it needs to be run by somebody at an AO8 level. Is that in terms of management? A lot of these breaches can be done inadvertently and honestly by an admin person who just puts in the wrong email address. We are not talking about trying to grade people in terms of who is responsible. It is more about the management of it. Is that your point?

Ms Stephensen: Yes. That is a finger-to-the-wind test as well. The level at which a person is employed will be for that agency to decide. Where I was going with that is that once you hit that level—say, a principle policy officer level—a couple of things happen. The first is that you are no longer in the administrative ranks of the day-to-day business of the agency. You are now likely a decision-maker. You maybe manage a team and you are imbued with the necessary power and responsibility within your role to go and seek advice from leadership or go and speak to your executive about issues that you are seeing on the ground and how those might need to be tackled. What we have noticed at IIS over the years is that, where staff who are tasked with managing privacy outcomes for the agency are not sufficiently empowered, those outcomes do not materialise.

Mr SULLIVAN: I think you were in the room when I said previously that it is double-edged sword when it comes to privacy. To search for outcomes and to try to provide good outcomes from government you actually want agencies to share information when appropriate.

Ms Stephensen: Yes.

Mr SULLIVAN: I do not know if you have any reflections on the previous answer to that, but do you think that this legislation can still provide that need for Education, Health, Housing, Communities and others to talk to each other for good outcomes as opposed to a silo effect that does not help anyone?

Ms Stephensen: The way that privacy law is structured in Australia generally, and certainly with the proposal for this bill, is that the sharing of personal information for legitimate government purposes would ordinarily be allowed within the relevant Queensland privacy principle. What you notice is that the principles are structured so there is a rule—for example, there is a prohibition on disclosure—and then there are a number of exceptions to the rule. Usually the ability to share falls within one of those exceptions to the rule.

Mr SULLIVAN: It is about the culture too and the signalling.

Ms Stephensen: Yes. The culture is: 'We can't do that because of the Privacy Act.' They call it the bot path phenomenon: 'Because of the Privacy Act we can't do anything. We can't even tell you your own information.'

Mr SULLIVAN: The computer says no.

Ms Stephensen: Right. You do see that happening, but that is a culture shift within our organisations. To the Privacy Commissioner's previous comment on the privacy champions network, these are not officials from agencies that are low level. These are strategic placements for privacy championing, so it is at the executive level—director-general level or CEO level or maybe a DDG of corporate services or whomever—that they are leading the strategic charge in relation to privacy management. They have the ability to take that message through into the ranks of the agencies.

Mr SULLIVAN: And the drive probably too.

Ms Stephensen: Yes. If you see your executive officer who has a deep care factor for privacy, that tends to rub off.

CHAIR: Comes from the top down.

Ms Stephensen: Yes. There are unwritten ground rules: 'Here at the department we only manage personal information in accordance with the privacy principles.' Those messages start to percolate and that can start to cause a culture shift.

CHAIR: Thank you very much for appearing before us today, Ms Stephensen. We really appreciate your submission and your contribution. There were no questions taken on notice, so thank you again.

Ms Stephensen: Thank you so much.

HOLMES, Ms Neroli, Deputy Commissioner, Queensland Human Rights Commission

LEONG, Ms Rebekah, Principal Lawyer, Queensland Human Rights Commission

CHAIR: I now welcome our next witnesses from the Queensland Human Rights Commission: Ms Neroli Holmes, Deputy Commissioner, and Ms Rebekah Leong, Principal Lawyer. Good morning and thank you for appearing before us here today. I will hand over to you to make a brief opening statement and then we will have some questions for you.

Ms Holmes: I acknowledge the traditional owners of the land on which we meet today and pay respects to elders past, present and emerging. I thank the committee for the invitation to appear today and make submissions on this bill. Information privacy and the right to access government-held information is essential to promoting and respecting the right to freedom of expression and the right to privacy and reputation both of which are protected in Queensland under the Human Rights Act.

The commission is supportive of legislative amendments that seek to improve protections for personal information and improve the functioning of privacy and right to information laws. We also endorse corresponding increases in funding to the Office of the Information Commissioner to support implementation of these changes and the continuation of the excellent work that they do.

However, the commission holds concerns about just one part of the bill—the impact that these legislative amendments may have on First Nations data and the rights and entitlements of First Nations peoples. As outlined in our written submission, the bill proposes that information privacy and the right to information laws do not apply to entities established by letters patent. Entities established by letters patent include charitable and religious organisations. Historically many of these organisations ran missions and dormitories and had significant involvement with the lives of Aboriginal people and Torres Strait Islander peoples. They are likely to hold critical personal information about people's identity, childhoods, family, employment and community.

Removal of these entities from the scope of right to information laws and information privacy laws leaves a gap in the rights for Aboriginal people and Torres Strait Islander people to access their own information and limits their cultural rights. Neither Path to Treaty processes nor the complaints process under the Human Rights Act can compel production of this information.

The commission submits that changes to the definition of 'public authority' which would exclude entities established by letters patent must carefully consider the flow-on effects this change will have on the cultural rights of Aboriginal peoples and Torres Strait Islander peoples. This is consistent with the approach that was taken in the review and amendment of the Public Records Act. For similar reasons, the commission also supports the Office of the Information Commissioner's submissions that the interests of First Nations peoples be expressly included as one of the public interest factors favouring disclosure under the Right to Information Act.

CHAIR: Thank you very much, Ms Holmes.

Mr LISTER: Am I to take it that the barriers you speak of apply not only to Aboriginal and Torres Strait Islander peoples but to others who may need access to records held by organisations established under letters patent?

Ms Holmes: Yes, that would be the same issue, but I am not quite sure how many of those organisations exist in Queensland and how much influence they have had over a broad range of individuals' lives. Certainly we are aware that they have had a specific influence over Aboriginal and Torres Strait Islander people. We know, for instance, that Aurukun and Mornington were governed for a long period of time by the Presbyterian Church, which is an organisation established by letters patent. They have had a very specific impact on Aboriginal and Torres Strait Islander people.

Mr LISTER: If you were to recommend amendments, would they apply only to Aboriginal and Torres Strait Islander peoples or would they be broader to benefit others who might need access to information held by bodies established by letters patent?

Ms Holmes: Under the court case that was decided recently that this amendment is addressing, it would give a right to anybody impacted whose information is held by letters patent, because taking the letters patent organisations out of this regime means that everyone's individual information that is held by those organisations is being removed. People do have a right to information under the Human Rights Act and have a right to privacy under the Human Rights Act. The committee should probably consider those issues as well. Our point is that, because of the unique involvement with Aboriginal and Torres Strait Islander people, that is a particular issue that should be looked at.

Mr LISTER: How do you reconcile that with your stated view in your submission that you agree with the purpose of excluding organisations established by letters patent from having to perform under the act? How do you have it both ways?

Ms Holmes: It is the responsibility of the parliament to look at where gaps are created.

Mr LISTER: We are asking you. You are here to tell us what you think.

Ms Holmes: Well, I would like a specific piece of legislation to be enacted that looks at those particular issues similar to what was done in the Public Records Act and what is being done in the Information Privacy Act to try to address the gap that will now be created by those people losing that right. That is an issue specific to Aboriginal and Torres Strait Islander people because of the strong impact it has on them and the cultural rights they have to try to get that information back. It may apply to single women who had babies or people who were adopted. There may be a whole group of people who may have information that is very valuable to them and their families. We think this does need addressing, and it is the responsibility of parliament before taking rights away to consider how those rights can be protected.

CHAIR: Thank you. That was very helpful. I think you have comprehensively answered that question for us and you have given us a lot to think about. We are very grateful for your time here today. No questions were taken on notice. We are very grateful for that contribution. It was very useful. That concludes our public hearing. I now declare the hearing closed.

The committee adjourned at 11.41 am.