# *LEGAL AFFAIRS AND SAFETY COMMITTEE*

**Members present:**
Mr PS Russo MP—Chair
Ms SL Bolton MP
Ms JM Bush MP
Mrs LJ Gerber MP
Mr JE Hunt MP
Mr AC Powell MP

**Staff present:**
Ms R Easten—Committee Secretary
Ms M Telford—Assistant Committee Secretary

## PUBLIC HEARING—OVERSIGHT OF THE OFFICE OF THE INFORMATION COMMISSIONER

### TRANSCRIPT OF PROCEEDINGS

**MONDAY, 30 AUGUST 2021**

**Brisbane**

# MONDAY, 30 AUGUST 2021

**The committee met at 9.03 am.**

**CHAIR:** Good morning. I declare open the public hearing for the committee's oversight of the Office of the Information Commissioner. I would like to respectfully acknowledge the traditional custodians of the land on which we meet today and pay our respects to elders past and present. We are very fortunate to live in a country with two of the oldest continuing cultures in Aboriginal and Torres Strait Islander people, whose lands, winds and waters we all share.

My name is Peter Russo, the member for Toohey and chair of the committee. The other committee members here with me today are: Mrs Laura Gerber, the member for Currumbin and deputy chair; Ms Sandy Bolton, the member for Noosa; Ms Jonty Bush, the member for Cooper; Mr Jason Hunt, the member for Caloundra; and Mr Andrew Powell, the member for Glass House.

Under the Parliament of Queensland Act 2001 and the standing rules and orders of the Legislative Assembly, the committee has oversight responsibility for entities including the Information Commissioner. The Right to Information Act 2009 and the Information Privacy Act 2009 set out the functions of the committee under the acts. These include: monitoring and reviewing the performance of the Information Commissioner against its functions; reporting to the Assembly on any matter concerning the commissioner; and examining the annual reports tabled in the Legislative Assembly under the acts. The purpose of the hearing today is to hear evidence from the Information Commissioner, the Acting Right to Information Commissioner and the Privacy Commissioner as part of the committee's oversight of the Office of the Information Commissioner.

Only the committee and invited witnesses may participate in the proceedings today. Witnesses are not required to give evidence under oath, but I remind witnesses that intentionally misleading the committee is a serious offence. These proceedings are similar to parliament and are subject to the Legislative Assembly's standing rules and orders. In this regard, I remind members of the public that, under the standing orders, the public may be admitted to or excluded from the hearing at the discretion of the committee.

The proceedings are being recorded by Hansard and broadcast live on the parliament's website. Media may be present and will be subject to my direction at all times. The media rules endorsed by the committee are available from committee staff if required. All those present today should note that it is possible you might be filmed or photographed during the proceedings by media, and images may also appear on the parliament's website or social media pages. I ask everyone present to turn mobiles phones off or to silent mode.

## GREEN, Mr Philip, Privacy Commissioner, Office of the Information Commissioner

## RANGIHAEATA, Ms Rachael, Information Commissioner, Office of the Information Commissioner

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

**CHAIR:** I welcome Ms Rachael Rangihaeata, Ms Anna Rickard and Mr Philip Green. I invite you to make a short opening statement, after which committee members will have some questions for you.

**Ms Rangihaeata:** Thank you for the invitation to make an opening statement. I would also like to acknowledge the traditional custodians of the lands on which we meet and pay my respects to their elders past, present and emerging. Today I am joined by the Privacy Commissioner and the Acting Right to Information Commissioner, Ms Anna Rickard. I intend to highlight key themes relevant to the 2019-20 annual report and comment on how those themes have developed through 2020-21.

We have experienced a clear increase in demand for our services over the past five years, with a record 787 external review applications in 2019-20. We also received record inquiries and an increase in privacy complaints. The workload involved also went far beyond sheer demand and numbers. I am very proud of how OIC continued to achieve strong results in 2019-20 in the face of high demand and significant challenges, including record high review closures and responses to inquiries.

It is phenomenal that we have gone on to break these record highs in 2021. We have been agile, working with stakeholders and partners to adapt how we deliver our services in an evolving environment. I would like to congratulate our team on their outstanding work and service to the community. I also thank my executive leadership team—Louisa Lynch, Adeline Yuksel and Philip Green. I acknowledge Phil's important contribution as Privacy Commissioner over the past six years as he moves on later this year to seek new and different challenges.

We have looked at key drivers of the substantial demand in recent years and focused on how we can influence these over the past two years using all our oversight and support functions as appropriate. When we think about the push model of right to information and the formal access application process as a last resort, we want to reduce the unnecessary applications coming through so people have better access to information and we free up resources to deal with other applications and reviews quicker.

Our external review applications featured a significant increase in applications where the agency had not made a decision on the initial application within the statutory time frame. This meant a substantial increase in work as we were essentially starting from scratch. Applicants are already frustrated at the extended delay and trust is diminished or lost. Dealing with such applications at external review is not an efficient use of resources for OIC, the agency or the applicant who has, as I said, experienced significant delay.

The Queensland Police Service comprised 24 per cent of all review applications in 2019-20. We engaged with the QPS executive in October 2020 to escalate concerns about delay resulting in and during external reviews. The QPS has worked openly and constructively with us to achieve greater adoption of proactive and administrative release and improve its capacity to deal with formal applications effectively. This process will take time to embed and we will continue to support this work. The approach we are taking with QPS reflects the importance of our work in promoting greater adoption of the push model and an open-by-design approach to information access consistent with the Right to Information Act. This work helps ensure better information access for Queenslanders every day—easier and simpler access at their fingertips or on informal request. Our upcoming campaign for International Access to Information Day focuses on open by design and government transparency everyone can see.

Our right to information audits have reinforced the importance of the open-by-design approach. Our disclosure log audit and recent review of minimum publishing requirements found that, even where technical requirements may be met, the user experience can be improved to ensure better access, including timely and easy access for the community. Proactive release is not effective if people cannot find it or the delay is so great people resort to formal access applications in the meantime.

In 2019-20 we reported on the implementation of recommendations from local government compliance audits. We also finalised an audit that was tabled in July 2020 about managing the risk of re-identification in public datasets. This was a critical audit for our stakeholders in revealing the existing risks in their published datasets and has attracted international interest. We have spoken extensively on this topic to a range of audiences and provided recommendations to all agencies to manage risks.

Our privacy work has evolved through the past two years with substantial growth in voluntary data breach notifications. Our work is focused on the cultural change to minimise harm to the community. We know human error is an issue in Queensland, similar to other jurisdictions. We continue to implement the recommendations out of the CCC's Operation Impala, strengthening OIC and supporting our stakeholders to meet their obligations. We amended our online training package to address specific requirements raised in Operation Impala. Training is fundamental to a strong privacy culture. Our awareness of privacy obligations audit and follow-up audit showed good results across the agencies that all fully implemented our recommendations.

There are a number of Operation Impala recommendations that require legislation, such as a mandatory data breach notification scheme—similar to those now being adopted in other jurisdictions. We are taking steps to better manage our voluntary data breach notifications that will assist in a transition to a mandatory scheme, including providing new tools for reporting to OIC.

While we have achieved outstanding results, challenging workload and increasing unreasonable behaviour towards our staff has impacted our team. Our 2020 Working for Queensland survey results showed the substantial impact, with about a 30 percentage point increase in the one year in staff being overloaded and burned out by work. We reinforced reasonable expectations with our team and stakeholders and we implemented fair and appropriate strategies to manage behaviour and deliver timely external review, privacy compliant and inquiry services. We welcomed the approval of a temporary FTE increase for OIC for two years from July 2021. This will provide an additional 2.6 FTEs

for external review services during that period to help address the high demand and on-hand file load. We will also be able to temporarily fill the 2.2 FTE outstanding positions recommended to be made permanent by the 2017 independent strategic review of OIC. Our cash reserves will fund these positions until 30 June 2023.

Finally, I would also like to note that our team has not only provided high-quality service to our stakeholders despite the disruptions associated with COVID-19; we have also been committed to supporting the public health response with high-quality advice. We have worked with our Australian privacy authority colleagues in the national privacy COVID task force to ensure consistent advice. If I may, I would like to invite Mr Green to make a very short opening statement as well.

**Mr Green:** I thank the committee for your interest in privacy. We are reporting on the 2019-20 annual report and we are about to drop our current one for the immediate past, so my head is full of those facts and figures as well but it is also informing our work into the future and the future challenges. I am going to draw on a couple of examples from the privacy jurisdiction that actually span the whole period and they are going to be challenges for us going into the future.

The first one is the Operation Impala submission that we made in 2019-20 to the CCC as part of its inquiry. That inquiry was initiated from data and reporting to the CCC by Queensland government agencies specifically about unauthorised access and use of information in agencies. The figures there are fairly high. Those figures do not translate to privacy complaints that we see a lot of the time. As Rachael has explained, we have had an increase over the past few years but those are still under 100 complaints per year. The CCC was getting in the high thousands for some agencies. It is a significant issue and we put a lot of work into that.

We also based some of our submission on an earlier submission about legislative reforms and a contemporary legislative framework for privacy from 2017. We have continually advocated for a contemporary legislative framework since then. It is a fast evolving landscape internationally and nationally. The national government already has a review of the Commonwealth Privacy Act. They have amended it several times and introduced the notifiable data breach regime at the federal level a couple of years ago, so there have been continuing reforms internationally and we think that is critically important.

Of the Impala recommendations, the OIC spent quite a lot of the last year, and is continuing into the future, implementing those recommendations. A key initiative is our privacy champions network, which we launched in Privacy Awareness Week in 2021, but we are also continuing to expand that and hoping to expand it to the HHSs and to local government because we see those agencies as needing further help. The maturity from our survey work and from our audit work has shown that there is improvement needed in some of the smaller agencies, which is understandable. Some of the bigger departments that do a lot of work and have a lot of employees have got their act together more fully.

The other thing I suppose about the contemporary legislative framework, as Rachael has indicated, is we put into place a voluntary notification scheme, and we are getting notifications and those are increasing as people become more aware. The survey work done by our counterparts at the national level, the OAIC, has shown that the public expect to be told if their data is compromised to minimise harm and to allow them, say, if they had identity theft, to take steps to protect themselves. It is fundamental, commonsense stuff in terms of a reaction. Agencies are doing that on a voluntary basis, and we are seeing an increase in that as they become more mature. I think it is a critically important thing into the future. It gives us the intelligence to actually understand where the complaints are happening and what is causing them particularly.

As Rachael has also indicated, human error continues internationally to be one of the root causes of privacy breach—at 38 per cent in one of the last surveys. That accords with our experience in privacy breaches and it can particularly impact on thousands of individuals or millions. One particular security incident in New South Wales has reached well over 100,000. If something happens with databases that hold millions of people, like a ransomware attack—the UnitingCare hospital service actually had this in Queensland in the past year, and the meat industry has been affected internationally by ransomware—that can have huge repercussions. It is a particularly important area.

The other area of work in 2019-20 which is continuing to evolve is the COVIDSafe app work that we did with our national counterpart, particularly led by the OAIC and the federal commissioner. Rachael and I were at the inaugural meeting of a national COVID privacy working group that was established to face the challenges of introduction of that COVIDSafe app. As it turns out historically, the app may have proved less useful than it was expected to be, but I think it is an example of an extremely well-thought-out privacy and data security exercise for introduction of new technology. I believe that as an app it has helped pave the way for some of the check-in apps that have been

developed by other states and territories and public acceptance and trust of them. In particular, some of the initial private sector apps were not as privacy or data security sensitive. It has actually been really critically important.

One of the things they did with the federal app was release the privacy impact assessment. They also undertook to release the actual coding behind the app to assure people that no untoward data collection was occurring. They also introduced federal legislation which gave the federal commission unprecedented power of audit into even the state and territory health systems about the use of the data. There were really good privacy practices and data security practices around the development of that app. We are using that to inform development and further development of the check-in app as it evolves and is extended. I think that will also be useful work going forward into the vaccine passport arena as we are looking at how we can technologically have a verifiable system for introduction of that.

The complaints and performance area, as I say, is actually a small part of our overall work, even though they have gone up. That is quite heartening to see, and I think it reflects that a lot of agencies do handle privacy complaints well. Out of that volume that came through the CCC reporting in their dashboard, which is an online dashboard, 100 complaints a year is not too bad. I think there are possibly some unknown breaches that have occurred that maybe are not reflected in that. As part of our legislative reforms, we suggested that we get better reporting on that. Also the notifiable data breach would give us better intelligence on the number of breaches and the volume and the health of the overall system of privacy and security.

The complaints performance figures are impacted heavily by the small numbers that are actually accepted and even fewer go to QCAT. The QCAT proceedings are actually at the behest of the complainant, so even if we have attempted to mediate and cannot mediate a complaint, those complaints sometimes do not even proceed to QCAT for hearing and determination. The numbers of decisions are quite low. It is somewhat frustrating at times because we do not have a lot of jurisprudence in our jurisdiction about what the law actually is from the judiciary or the tribunal members.

Finally, as Rachael has indicated, December brings the end of my second term as Privacy Commissioner. I have been honoured to serve. I think we have made some great contributions in the last six years. We have strengthened our national and international connections, which are critically important in this area. As I said, the law is developing rapidly, but with the technological challenges that we all face it is really critical that we network well. We built those relationships as well with the research community in Queensland and internationally.

We have also done some great work in terms of trying to move the culture forward. The chair of the CCC, Alan MacSporran, addressed Privacy Awareness Week last year. The year before we had the eSafety Commissioner as well as the federal commissioner speak. That rapidly evolved into an online event and was broadcast rather than an in-person event. It was fortunate, I think, we could still go ahead in that manner. Last year we did that as a hybrid so we could go either way, and we fortunately had a physical presence too. We do hear from the people who we serve that they do miss those physical interactions. It is great that we can meet in this environment as well.

I have been honoured to serve as Privacy Commissioner. I am hopeful that the foundations we have laid in some of our recommendations will go forward to the future and serve us well.

**CHAIR:** Thank you, Phil.

**Mrs GERBER:** I will pass to the member for Glass House, who has a question.

**Mr POWELL:** I have a couple of questions but I am happy for you to pull me up anytime, Mr Chair.

**CHAIR:** How many do you have?

**Mr POWELL:** We will see what the answers are and we will go from there.

**CHAIR:** I will not interrupt your train of thought.

**Mr POWELL:** Thank you all for your attendance this morning and for your opening statements, Rachael and Philip. Philip, thank you for your service over the 5½ years, nearly six now, and all the best for what is after. Rachael, you mentioned that most of the external reviews are now starting to demonstrate that even an initial decision has not been made in the time frame that is required under statutory law. Is there any commonality within the agencies as to why they are missing those deadlines?

**Ms Rangihaeata:** In 2019-20 there were 122 out of the 692 we received that were of that nature—where there had been no initial decision. That rose to 146 in the past year. It jumped up from 69 I think in the previous year and before that it was down in the 40s, so it has been a big increase.

Certainly, resourcing is always an issue that people mention to us. Of course, over the past 18 months there has also been some diversion of resources within some agencies to COVID activities and in some cases possibly other activities as people have been manoeuvred around to deal with other priorities.

I think all agencies have been stretched through this period to meet important priorities across the board. The key agency for us in this area was QPS, and I think I heard that 25 per cent of their resources were diverted to COVID activities so that is a really large increase. Anytime we see a big activity like the Commonwealth Games or the G20, resources out of the RTI unit are diverted to operational duties so it does have an impact.

**Mr POWELL:** A number of other agencies sought to modify statutory requirements through some of the COVID emergency power legislation. Was any conversation had with, say, the police but probably more broadly the government agencies that during COVID, given resourcing like that, we needed to look at a temporary extension of time so that it was not falling to you to then have to make decisions?

**Ms Rangihaeata:** There is capacity within the legislation for them to seek an extension from the applicants, and in many cases they do and in many cases it is granted. Some of these applications come to us after a number of applications have already been given and an applicant says, 'That's enough. It's not working. Time to go onto external review.'

We also have capacity within our external review provisions within the legislation to grant a further extension to deal with the application back to the agency, and we grant those extensions where we believe that it will work and it is worth doing. In some cases we say, 'No, it's not going to actually work out. It's best staying with us.' That is an individual consideration of the circumstances in each case. We need to think about whether there have been previous extensions. If the agency has a decision they literally are about to issue and they say, 'It's going to go out within the next three days,' it makes so much more sense for us to give them another week to do that rather than coming to us and starting the process here. I might ask if Ms Rickard has something to add to that.

**Mr POWELL:** Ms Rickard, as well as resourcing, can I also ask whether there are any other systemic issues you have identified as to why those decisions were not being made in their time frames?

**Ms Rickard:** I think over the past period since COVID lockdowns began—probably a bit less so this year but more last year—when agency staff were working from home they may not necessarily have had access to the databases where they would be able to search for documents responsive to applications. I think in the initial months that probably had a pretty practical impact on the ability of a lot of agencies to get the documents to make decisions about them. That probably has been less so this year as agencies have adapted to the on/off lockdowns.

With deemed decisions, once they come to us, as Rachael mentioned, we do have discretion in how we deal with them. They can be referred back to the agency. In some instances, if we are talking with an applicant and we realise that it has become deemed because the scope of what they are requesting is incredibly broad and unspecific, we can speak with the applicant to try to pin down a scope that will allow the agency to identify and locate the documents that they are after.

If it is a case where it seems that it is better for us to deal with it—if the applicant is really at the end of their threshold for trusting the agency and it seems as though we can deal with it faster—we then track the progress by putting in time frames, speaking to the agency about what is realistic. In circumstances where there has been ongoing delay we try to negotiate with the agency to come up with a way that that review can be prioritised and dealt with.

**Mr POWELL:** On some rough calculations, not meeting the initial deadline comes to about 15 to 20 per cent of the external review cases you are reviewing. Are there any other primary themes that you would identify of the remaining external review cases that are coming to you?

**Ms Rickard:** In terms of delay or just in terms of themes generally?

**Mr POWELL:** No, more broadly—other than delay.

**Ms Rickard:** A very common factor is sufficiency of search. That is where an applicant has applied for documents and what is located by the agency is not what they are after or the extent of it is not as broad as what they are after. That is a very common one. Another one is personal information—people applying for their personal information if there has been information redacted within that. Understandably people come to us on review seeing that there is information about them redacted from documents and wanting us to assess that.

**Ms BUSH:** Rachael and Philip, thank you for your opening statements. We could listen to you all day. Philip, you are clearly very passionate about your work and we wish you all the best in wherever you are moving to next. Rachael, I think you mentioned QPS were responsible for 24 per cent of the applications that were made to you. I was interested in whether that is usual or whether that has gone up. If it has, is it because of Impala or what might be the reasons around that?

**Ms Rangihaeata:** Yes. That was the external review applications. In fact, in 2021 it has gone up to 29 per cent. As I said, the work that we are doing with QPS will take some time to embed. They publicly announced that they were allocating additional resources to the RTI unit to deal with their applications. They have been trying to recruit, but my understanding is that they still do not have a net increase because of some promotions within the unit. It will take some time. As I said, they have been really open and constructive in dealing with us about looking at opportunities to increase proactive and administrative access. That is right across the ELT.

Anna and I met with the ELT in February, I think, this year. An action out of that meeting was an invitation to us to identify insights from our external review work as to any administrative access opportunities that we could see and provide a list to them to consider—and we did that. We have also met with a number of groups from the QPS ELT to talk about their specific business and opportunities. They have not come to sit and listen to us; they have come to engage with us. They have asked questions and they have proposed things to us. They are very much in the driver's seat, and that is really good to hear—but they also have to operationalise that. That is something that will take some time to work through. As I said, we know that they are working on the front line with COVID as well. They have a lot on their plate, but it is very important work and we have a lot of applicants come to us in that area.

I have been in this office and in this work for a very long time. QPS has been the No. 1 agency for our external review work the whole time. I think it goes to the complexity of their work: the interactions they have with the community; as Anna said, the nature of some of the documents tends to have third-party information in it; the level of trust that often occurs in relation to some of the interactions there; and the need people have to see that information. There is a range of issues around that. I expect that it will continue, but the work that we are doing with them is very important. Philip may just add something about the privacy complaints.

**Mr Green:** From Impala we have not seen a marked change in the numbers of complaints about QPS privacy breaches. However, the CCC has set up an electronic dashboard which will be really good to watch going forward. I believe the Police Commissioner is taking it extremely seriously, and we have seen a cultural shift or an embracing of change. We have seen a very stern approach to unauthorised access from the QPS since Impala. They have also resourced their privacy complaints area better. That is all positive, I believe.

**Ms BUSH:** Excellent. I imagine that a big consideration of a lot of the requests that police field invokes the public interest test element as well around ongoing investigations potentially. Is there an issue there?

**Ms Rickard:** We do at times see applications for information about investigations that are ongoing. There is an exemption ground in the act that if that is the case then the information can be refused. If that comes before us, we usually do note to the applicant, 'At this stage the information can be refused on this basis. Possibly in future, if you are still interested, you may want to reapply.' With police, probably the other primary grounds of refusal that come up are personal information that we mentioned before and at times if the information would prejudice a method or procedure used by police.

**Ms BUSH:** That is an interesting tension. I can see Sandy has questions too.

**CHAIR:** Go on. One more.

**Ms BUSH:** I have a thousand.

**CHAIR:** You are not going to get a thousand.

**Ms BUSH:** I will think about my best one then. I was interested in how you work with organisations to manage the tension around accounting for human error but also ensuring they can still operate efficiently as an agency. Having worked in the Public Service, you are aware of data breaches and the need to have to double-check your work and have buddies, but that of course slows everything down in an agency. I am curious how you work with agencies to risk-manage that.

**Ms Rangihaeata:** I think it all comes down to culture overall. That is where the training and awareness really comes to the fore. As we have been talking about, Operation Impala has been really important for us. It has been complementary to our work and we have done a lot of work together, as

Phil said. The chairperson of the CCC spoke at our Privacy Awareness Week this year. A lot of their recommendations have reinforced recommendations from our legislative review and our audit work—the awareness of privacy obligations work that went to training and improving that culture.

We did our initial audit just before Operation Impala and then our follow-up audit afterwards. Always when I go to speak with agencies I say, 'You must ensure everyone does general awareness training because every single person in your agency handles personal information.' We can all send an email to the wrong person. We see in our complaints the very simple errors when people send something to the wrong person. The other one is putting the wrong attachment on. We have seen attachments with contact lists go out. The impact of that can be devastating. I think the worst ones for us where it impacts on people who come to us with complaints—we have some of those at the moment unfortunately—are victims of family and domestic violence. The impacts on them when they have just settled—I know you understand the impacts—are devastating. It can be absolutely catastrophic, yet it is such a simple human error.

People say—and this is the same as the notifiable data scheme—you do not always know what those impacts are. That is why it is important that people are notified, because we, the people who are impacted, are the only ones who will really know the impacts on us and be able to manage those impacts. I think that is really important. That is why it is so important that that culture changes, so that we are also aware of the impact of our everyday actions. That is what we have been trying to reinforce in every aspect of our work—that ongoing training and tailoring that to the work that people do, not just in general in an agency but in their HR function or in their procurement function—in everything they do, because sometimes it has additional implications. Phil, is there anything you wish to add to that?

**Mr Green:** The human error is a really big thing in the ransomware vector as well. It is particularly critical. Those lens covers for your computers are not just tongue in cheek. Every one of us needs reminding. The smallest thing—the lowest employee in an agency or a contractor of an agency—can bring the agency down. That is what we are seeing more, even SMS on your phone that is connected to a server. Human error is a really big factor in some of the big cyber attacks as well. The latest reporting by the Australian commissioner has shown I think a big increase just in the last quarter of ransomware attacks. It is critical to think—we say, 'Think before you click,' or 'Think before you send.'

**Ms BOLTON:** Thank you for your extensive introduction. It took away a lot of my questions, so you did an awesome job. I want to go back to talking about resourcing. In three years you have had a 53 per cent increase in the case load. That is extensive, and you have spoken about the impacts including burnout that has occurred from that. In those increases in resources, you have mentioned using cash reserves. Is there any further resourcing required or do you need any reviews on certain parts of legislation or change to be able to assist overall in what you do and how you do it?

**Ms Rangihaeata:** Yes, there has been a significant increase. While we can do all that we can within our functions on the proactive side to try to engage in pushing down that demand—and we feel it is our responsibility to do that within our remit—we are not going to be able to push down all of that demand. We have a further strategic review due next May. We expect that that will be something that will definitely be considered at that point. There is definitely resourcing.

Also, our privacy function, as Phil was talking about, has evolved significantly in the last six years. When we started out with the privacy function in 2009 it was very much focused on complaints. That is a very small part of our work now. In the future, with recommendations that have already been made through Operation Impala and through the legislative review of the Right to Information Act and the Information Privacy Act, there are a number of recommendations pending for legislative change that will impact our work and require us to take on new functions—and possibly the QLRC recommendations around the civil surveillance as well. There are things that could change and expand our functions and certainly bring additional work and definitely stretch us, not just on external review but also on privacy. Of course, there are the community expectations and demand at the same time. They are really changing.

The ICT side has changed significantly and continues to, and that is really challenging us in terms of our supplies and services. We definitely are engaging with Treasury and Justice and Attorney-General in relation to what we need to do there in terms of some of our systems. We were very fortunate that in the 2019-20 year we had just transitioned to a new ICT environment with Datacom shortly before COVID-19 and we were able to take advantage of those new tools and resources when we moved online for remote work. Our CRM for all of our external review in particular—we know that we are going to have to do more work there and we cannot afford it within our current budget. There are a range of things, and I expect that they will be considered in our strategic review.

**Ms BOLTON:** Further to that, with the strategic review side—obviously through this time when it has been really intense and resource stretched, like the last 18 months probably, the complaints regarding the process itself and the work of the commissioner have come forward. Will that be reviewed within that strategic review as in what can be improved in the process of when someone has a complaint about the commissioner function itself?

**Ms Rangihaeata:** Yes, we will certainly put those forward to the strategic reviewer. We have a database of all complaints made in the various complaint grounds and systems under different legislation, so we can make those available to the strategic review. We review those ourselves, including all feedback we receive through formal and informal satisfaction surveys and so on. We are very committed to continuous improvement and innovation, and I would say that we have sped that up over the past 18 months. We are looking for anything we can do to find time and resources from those innovations. It is a necessity. Moving online for COVID-19 actually found us some further improvements and enabled us to cut some people out of the process where we reflected and decided we could do things a little differently—at least try it out and see if it worked. We have done things like that, but it just will not overcome the sheer increase in demand. We are doing everything we can; I can say that.

**Mr POWELL:** Philip, you mentioned a lot of the positive steps that have been made in the privacy space. You also mentioned the rather sizeable ransomware attacks on the likes of UnitingCare and JBS. I have seen a reluctance on companies in particular, but government agencies as well, to invest in cybersecurity protection. They end up paying huge ransomware payments rather than an ongoing, what I would consider, insurance payment through cybersecurity. Do you have any comments on that?

**Mr Green:** It is interesting that in my first week of being appointed as commissioner I was asked to be on the Queensland government cybersecurity steering committee, which has evolved quite a bit in that six years as well. The Queensland government has given, through CHDE, cybersecurity investment quite a boost, I believe, in the last state budget. That may have come up in their estimates hearings, but I have seen the budget bids and what it would be put towards. I think investments there have been weak in the past, but they have been improving. I know that they have a policy on ransomware and that is to not pay at a Queensland government level, but at one point that could be escalated to, say, a parliamentary or cabinet situation if it was a grave, life-threatening threat, I believe.

I think with the prevalence there, we need to be ever vigilant. One of the problems is that that group does not actually extend across local government and some of the other agencies that we regulate through our patch. The actual cybersecurity unit has less reach than it probably needs—say, it does not cover the university sectors. I believe that, yes, it is going to be an ever-increasing issue with notification, which is another matter because the federal commissioner has seen some companies have not been notifying her office and using this as an excuse that they have not actually discovered that data has been compromised or lost for good if they recover it. There needs to be a joint multidisciplinary approach to that.

At times those ransomware attacks might not even involve personal information. They might be on a systems internet of connected infrastructure—for example, power grids—so it does need to go beyond our office. We play an important role in there to protect the personal information, because often that is the crown jewel that the attackers are after. Health is particularly vulnerable. I know when UnitingCare was hit their actual health people in Queensland government, because they do not—I do not regulate; I do not cover what the federal commissioner does, but we all made sure that everybody was being extra vigilant during that time. Extra vigilance and awareness is a critically important part of that and the culture, but investment needs to follow.

There is an insurance scheme for Queensland government. The QGIF does cover some cyber coverage. That is in its infancy, but the coverage there can look at the risks and the risk mitigation strategies of agencies, too, so it helps uplift the skills. We have a huge skills shortage in this country as well, and particularly the federal government has lifted its investment, but we are watching in that cyber space particularly, as are other states and territories, and it is one critical area where we have to work together.

**Ms BUSH:** I am interested in the RTI audits that you mention that you do. Just broadly, what informs that or what informs the organisations or the issues that you might target in an RTI audit?

**Ms Rangihaeata:** We have an audit strategy. It is informed by external and internal data and intelligence. There is an annual report from the Department of Justice and Attorney-General—the Attorney-General's report about the operation of their right to information and information privacy acts, with data from all the agencies in their jurisdiction. That is one source of data. We also have our own data, and we do an environmental scan across our area. We are in a range of committees and associations with our peers internationally and nationally, so we have a range of information and intelligence at our disposal that feeds into that as well.

One of the things we have really focused on over the past few years as well, and we are keen to do moving forward, which helps maximise our resources, is ensuring that, particularly across Australia, we are not duplicating work and in fact we are maximising the resources by feeding off each other in a way. We will not do an audit that is very similar to one that our Victorian counterparts are doing, and if we see something that Victoria is doing that is very relevant to us we will promote the findings and the learnings from that up here. We do not need to repeat the investment of the resourcing of that, but we can promote that. I mentioned the re-identification audit of public data. That is one that we shared very broadly and spoke to a whole range of groups. We have done that with other audits from elsewhere.

We have a very small audit team. We have to really strategically target what we spend our resources on. We have probably moved away from the compliance audits in the past few years and more to the strategic topic audits which are key issues for the whole sector. In the earlier years of implementing legislation we more heavily focused on the comprehensive compliance audits of an agency. We would go in and we would really look at pretty much all of the aspects of how they implemented their RTI and IP obligations. Even when we do a compliance audit, like we are doing with the Sunshine Coast Regional Council right now, we have looked at what their risk areas are based on their self-assessment electronic audit that we conducted back in 2018-19, I think it was, and we are focused in on that. We are really targeting the resourcing, even within that audit, to what the risk areas are and the risk areas for that sector.

There is a range of data, intel and also looking at what we want to align with our strategy priorities, because it helps when we are engaging about the key strategic priorities. For us, at a very high level, we knew privacy impact assessments were important. Really, privacy by design at the broadest level is important for us, and really pushing the greater adoption of the push model—the proactive release, admin release, so trying to find audits that really tied in with those so that when we are doing our engagement all of our work comes together along those lines. I am not sure if that—

**Ms BUSH:** That is fantastic, thank you. That is really comprehensive.

**Ms BOLTON:** Mr Green, before you head off into your next role, with regard to the Queensland app, there have been community concerns regarding not only the data but also privacy security. How concerned should everyone be?

**Mr Green:** I think we need to be concerned but not alarmed and certainly aware. Our act when it was enacted was probably 10 years old, so we are getting a bit dated. We did identify some very positive things in 2017 and the CCC has affirmed pretty much all of that, plus more, and there is currently a Commonwealth review. I have always advocated that we should follow closely the national approach so that we are consistent and we can share resources, so that people are not confused with jurisdictions. Western Australia is about to enact legislation, we believe. They promised that in the former term. New South Wales is looking at introducing notifiable data breaches. The Commonwealth is looking at future things like artificial intelligence. That is going to be one of our big challenges. In Queensland we have already rolled out artificial intelligence projects, like detection of distracted drivers and seatbelts in cars. That is a low-ish AI matter. The discriminatory impacts of that are probably relatively low, but the human oversight matter is something that we need to keep a close eye on. The Commonwealth had some projects where it has gone rapidly wrong and south in terms of human oversight of AI. Queensland Health is using a lot of AI in the detection of disease and assisting doctors, but they kept the doctors extremely in control. I think there are plenty of areas—oh, the app, sorry, not the legislation. Pardon me.

**Ms BOLTON:** Correct. That is all right.

**Mr Green:** The one thing that we identified in the early stages with the check-in app was that it did not have legislated prohibition on access. The one case of access that we are aware of in Queensland has been through a formal process of a warrant. I believe the police did the right thing; they are acting within the law there. Western Australia probably went a bit further. They have reacted with legislation. I think the more we use that to gain public trust and to be transparent about who is getting the data and for what purposes is really critically important. I am hoping that I might see some change in my term, but I do not think we need to be alarmed. The private sector apps were all subject to police and law enforcement. The paper systems were. Other states and territories are. The COVIDSafe app is not, obviously. It is locked down, possibly locked down too tightly.

The one other issue I have been pushing was the privacy impact assessments. There has been a privacy impact assessment on that. Because it has been continuing to evolve, they have not publicly released that like they did for the COVIDSafe app. They have not released the code. Two other states and a territory are using the same technology, so the technology and the security behind it is probably

pretty well tested and proven. It would be good to see some legislative clarity on what it can be used for—secondary use. The health directive in Queensland right from the outset said no secondary use, but that is subject to other laws. That was the flow-on. I think there was some public confusion around secondary use, because some media statements said it will only be used for contact tracing and that was perhaps a little bit misleading, even though the privacy statements did refer to other lawful uses.

I do not think we need to be as alarmed about that, but I do think we need to keep an eye on it, especially as it expands, and it would be good to be up-front about the privacy impact. I think as best practice the federal government mandates, as part of its legislative code, that agencies actually do PIAs, and they are continuing to push for public release of them. That is a good practice because then the bad people and the good people can all have good debates about what is appropriate and whether the controls, particularly the technological controls, are sound or there is a smokescreen there. So it is good practice.

**Ms BOLTON:** Who is actually monitoring and watching?

**Mr Green:** With the check-in app, the buck stops with us for the moment. Mind you, the cybersecurity people are involved in terms of the security risks—and the agencies themselves, because they are responsible under the act for the use of the data and the sharing and use and disclosure. If police do access it currently under a warrant under their powers, they are subject to scrutiny as well for that. I do believe there are some checks and balances. I believe a clear legislative prohibition might be appropriate to help keep the trust. It is absolutely the essential tool for us going forward and it seems for the foreseeable future.

**CHAIR:** That concludes the hearing with the Information Commissioner. Thank you to the secretariat and Hansard reporters. A transcript of these proceedings will be available on the committee's parliamentary webpage in due course. In closing, I would like to thank you, Phil, for your contribution and the important work that you have done as the Privacy Commissioner. You have always been helpful and very informative.

**Mr Green:** Thank you.

**CHAIR:** I declare this hearing closed.

**The committee adjourned at 10.02 am.**