LEGAL AFFAIRS AND COMMUNITY SAFETY COMMITTEE

Members present:
Mr PS Russo MP (Chair) (via teleconference)
Mr JP Lister MP (via teleconference)
Mr SSJ Andrew MP (via teleconference)
Mr JJ McDonald MP (via teleconference)
Mrs MF McMahon MP
Ms CP McMillan MP (via teleconference)

Staff present:
Ms R Easten (Committee Secretary)
Ms M Westcott (Assistant Committee Secretary)

PUBLIC HEARING—OVERSIGHT OF THE INFORMATION COMMISSIONER

TRANSCRIPT OF PROCEEDINGS

MONDAY, 30 MARCH 2020

Brisbane

MONDAY, 30 MARCH 2020

The committee met at 10.01 am.

CHAIR: Good morning. I declare this public hearing open. I am Peter Russo, member for Toohey and chair of the committee. With me via teleconference are: James Lister, member for Southern Downs and deputy chair; Stephen Andrew, member for Mirani; Jim McDonald, member for Lockyer; Melissa McMahon, member for Macalister; and Corrine McMillan, member for Mansfield.

The purpose of the hearing today is to hear evidence from the Information Commissioner, the Right to Information Commissioner and the Privacy Commissioner as part of the committee's oversight of the Information Commissioner. 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.

Only the committee and invited witnesses may participate in the proceedings. As parliamentary proceedings, any person may be excluded from the hearing at my discretion. I remind witnesses that intentionally misleading the committee is a serious offence. The proceedings are being recorded by Hansard and broadcast with a live audio feed on the parliament's website. I ask everyone present to turn mobiles phones off or to silent mode.

GREEN, Mr Philip, Privacy Commissioner, Office of the Information Commissioner (via teleconference)

LYNCH, Ms Louisa, Right to Information Commissioner, Office of the Information Commissioner (via teleconference)

RANGIHAEATA, Ms Rachael, Information Commissioner, Office of the Information Commissioner (via teleconference)

CHAIR: Good morning, everyone. I invite you to make a short opening statement, after which committee members will have some questions for you.

Ms Rangihaeata: Good morning, Mr Chair and committee members. Thank you for the opportunity to make an opening statement this morning. Firstly, I would like to acknowledge that we are all currently operating in very different and complex circumstances and we are thinking of you, your families and communities at this time. I would like to briefly highlight key points about 2018-19, the annual report year we are currently focusing on today, and note that the committee has the benefit of the report which details the performance of the office. I would then like to outline how our office is currently operating under our business continuity plan and key challenges we foresee over the coming months.

We reported record demand and strong performance across our services and functions in 2018-19. As we mark the 10th anniversary of the Right to Information Act and Information Privacy Act, demand for our services has never been higher and significantly exceeded that in 2009. Our community attitude survey in 2019 also showed that 87 per cent of Queenslanders surveyed thought having a right to access government information was quite or very important, and 80 per cent were aware they could access information from relevant government agencies. Pleasingly, government agencies have encouraged those surveyed to access information in the least formal way possible consistent with the push model in the Right to Information Act.

Our office has continued to focus our resources to be as effective and efficient as possible in an evolving environment to meet stakeholder needs and expectations and drive good practices. Our audit program targets strategic assurance engagement, such as the privacy awareness and education audit tabled in February 2019. Report recommendations for all agencies, including mandatory privacy and information security induction training, are consistent with the findings of the recent Crime and Corruption Commission Operation Impala report about misuse of personal information.

Our *10 years on* report was tabled in June 2019, the fourth in a series of self-assessment audits of all government agencies across Queensland. Key findings included the need for agencies to focus on push model strategies, such as proactive release and administrative access, and emerging areas particularly relevant to privacy and technology, including privacy impact assessment requirements which were of key concern showing the lowest overall result.

In 2018-19 we had our new laptop fleet across the office and signed a contract with a new IT services provider Datacom. We transitioned to the new ICT environment in November 2019 with Office 365. Our new IT environment has placed us well to work remotely when required including in the current COVID-19 event.

Our business continuity planning team has worked hard over the past several weeks to adapt our plans, systems and processes to enable our whole office to continue to deliver services remotely over this extended and unusual disaster event. Many staff across the office have been instrumental in ensuring we are agile and innovative in how we deliver all training, events and services in an online format, provide advice and assistance on current needs such as information sharing, and move all processes to electronic format.

Given we are able to work remotely and in the interests of our staff and stakeholders' health, safety and wellbeing, we are temporarily closing our physical office at 133 Mary Street, Brisbane, tomorrow on Tuesday, 31 March. We will continue to deliver all services during this time via email, internet and phone.

Our key concerns during this time for our ability to provide services and our performance include government agencies' ability to participate across the board due to a diversion of right-to-information or privacy officers and other relevant operational staff to critical services or substantial leave. Similarly, community members may also have difficulties participating. For example, we will be constrained in how far we can progress external review, privacy complaint and audit processes. Audit reports are also required to be tabled on parliamentary sitting days and are therefore uncertain.

We also expect a larger number of access applications to come to us on review because agencies have not met statutory time frames. We will need to process these, but it will be difficult to progress them in many cases if relevant agency personnel are not available. Unfortunately, we expect a backlog will occur in these conditions despite our best efforts. Like all organisations, we are also projected to experience a higher level of sick and carers leave.

Trust and transparency are critical at all times for government. The community generally understand that human rights, including rights to information and privacy, need to be balanced with other matters at times like these. However, it is important that actions taken are reasonable, necessary and proportionate and limited to the period of the crisis at hand. We will continue to progress all the work that we can during the COVID-19 period whilst understanding the reasonable constraints on all of our stakeholders. Once people are able to engage we will progress any matter that has been delayed. I note that, while COVID-19 will be very disruptive, not all of our work relies on others, so we will be able to progress other work at the same time.

Finally, I would like to take the opportunity to thank our wonderful team who have not only been responsible for our outstanding performance in 2018-19 but quietly risen to the recent challenges as a united team to ensure the best outcomes for our stakeholders and to ensure we build trust through transparency in the work that we do. My colleague Louisa Lynch would now like to make a brief statement, followed by Phil Green, if we may, Mr Chair.

CHAIR: Of course.

Ms Lynch: Good morning all. I will be brief and look forward to addressing any questions you have or taking them on notice if necessary. Firstly, OIC's external review service, which sees us undertake merit review of agency decisions about access to information under the Right to Information and Information Privacy Acts, continues to see an increase in demand and complexity in matters year on year. You may recall 2017-18 saw a 21 per cent increase. I can report an 11 per cent increase on that in 2018-19, with 687 new matters received. We are already close on the heels of that total this year, with 526 matters received at February's close. I expect to exceed last year's record high this year.

I am very pleased to report, though, that in our biggest year of demand OIC finalised just short of the number received, with a record 659 completed—only 28 less than that received. This represents a near 100 per cent result in the percentage of applications finalised to received—a significant measure of effectiveness and proof positive of the commitment and extraordinary effort of all staff involved in providing the external review service.

I put it on record for you that in 2019, OIC's anniversary year, demand for external review services was not only at an all-time high but also double the demand from 2008-09. Despite this, a five-year high 92 per cent informal resolution rate and a 96 per cent finalised to received rate was achieved with a small number of permanent staff on hand. Our collaborative, small team based approach incorporating an intake early assessment and resolution team works. It maximises opportunities for fast resolution of matters. Each matter is considered on its own merits every time. We are flexible and responsive.

In 2018-19 our intake team resolved 45 per cent of all new matters within 90 days. Of the 353 allocated to me or my other two teams, all but 15 per cent were resolved informally. Those matters not amenable to early or quick resolution take many months to undertake and are extremely demanding in terms of time and complexity. Amongst other things, the submission phase alone can take several months and is a legal necessity given rules of procedural fairness. Of course, though, agency or applicant delay at any phase of the review process also has an impact.

While we only had two matters older than 12 months at the end of 2018-19, it may well be that this number will increase for this current year given the impact of COVID-19 on the ability of applicants and agencies alike to participate in the external review process for those matters currently with us. We may also see a large increase in new applications because agencies, as Rachael alluded to, may be unable to process applications they receive within statutory time frames. In those matters, access would be deemed to have been refused under the legislation and an entitlement to external review arises. Also unknown, of course, is the impact COVID-19 will have on our own staffing levels and, in turn, our productivity in coming weeks and months. We will adapt as necessary.

Briefly, looking at trends, the majority of the increase in external review applications in the past few years has been in the department and local government sectors. The subject matter of all reviews is diverse, from matters relating to issues of great community interest to very personal matters for individuals alone. The profile of applicants making external review applications is largely consistent with previous years. Individuals comprised 77 per cent last year.

In conclusion, I want to emphasise three things: the demand for our external review service remains very high; the workload is being held in check through careful management of reviews and thoughtful management and support of our review team members; and the impact that COVID-19 has on agencies will have a knock-on effect on the external review service. Thank you, Mr Chair and committee members.

Mr Green: I will make a brief opening statement. It has been an amazing journey since our last annual report, and I am sure the committee believes that as well. It seems like an eternity is passing almost each week right now, let alone going back to our last annual report. As the Information Commissioner has noted, I am pleased that a lot of our hard work last year in moving our ICT fleets to portable laptops and moving our ICT services to Datacom has meant that we actually have been able to work remotely at very short notice using VPN, virtual private network, arrangements. Our fleet has been fantastic working in the remote situation. I think we are well placed to keep working, apart from the agency responses and the diversion of resources by agencies and local government—I think they will be facing challenges—and, likewise, our staff situation. However, we are really well placed and the technology seems to be working quite well. Hopefully, the committee's work can continue remotely as well. I think it is excellent that you have proceeded in this way.

In the privacy area, last financial year we had record demand as well. We had 98 privacy complaints. That still seems to be quite a small proportion of overall complaints. The CCC's Operation Impala highlighted over 1,300 matters of misuse of confidential information. Not many of those actually arrive on our desks as privacy complaints. I believe a number have had more serious repercussions, but there are also matters where agencies have worked within themselves to resolve privacy complaints. That is quite encouraging.

In that past year we have been moving from an emphasis on tick-box privacy complaints and sort of 'check the box' to privacy by design, trying to get involved in technology and legislative projects from an earlier stage so that privacy is built in. That has been a mantra for some years. I think it is a continuing challenge going into the future for some of our privacy work. We continue to do a lot of advice and assistance work—this year particularly COVID-19 and some of the challenges posed by the election have actually meant a lot of urgent advice in the past few weeks—and work nationally and across states and territories with our colleagues.

One of the things that Operation Impala highlighted and that we have mentioned previously about legislative changes to the Information Privacy Act is the introduction of mandatory data breach notifications. We have that on a voluntary basis at the moment. Last year the OIC saw 24 such

notifications. This year I believe we will see more of those. We are on trend to actually have an increase in that. The CCC in Operation Impala has endorsed that suggestion about legislative change to have a mandatory data breach regime in this state. New South Wales has announced that it will be progressing that. Victoria has that on a voluntary basis. Western Australia and the ACT are examining it. I think that is a really important factor in identifying privacy breaches and also in managing them in agency responses, so that they do not do more damage in the response. Also, if they tell us then we can guide them with resources and assistance and, hopefully, minimise the impacts of some of those privacy breaches.

Last year's Privacy Awareness Week was a fantastic success. We launched that on the Sunshine Coast which was a first, taking it out of Brisbane. A fantastic Queensland organisation called IDCARE hosted it with the Sunshine Coast university and local government. It was a really excellent opportunity. This year from our planning for PAW 2020 it was looking like we were even going to top that success. We are now moving to more of a virtual arrangement in May this year, with obvious reasoning behind that. We are still hoping to have the Australian Privacy Commissioner and the eSafety Commissioner online in virtual format. We have invited the Attorney-General to present online as well. As the Information Commissioner and the Right to Information Commissioner pointed out, we are looking at being agile in trying to deliver our services in innovative ways, particularly the training and resources that we have done. We always have tried to have some of those online. This is just an additional challenge to be creative and try to keep things as business as usual.

The emerging challenges and issues are much as they have been in the past. In 2019-20 the technology challenges and, as highlighted in the Solomon Lecture, the challenges of artificial intelligence, big data and data analytics are going to continue. Last year's Solomon Lecture had a whole-of-office theme and was delivered by Fiona McLeod SC. We still have that online. It was a fantastic opportunity to look forward to some of the challenges. Some of those are coming straight to us in our own backyard. There are Transport and Main Roads and QPS projects to do with distracted drivers, which you will probably see through the parliament in terms of legislation. I think those are the first instances of the deployment of artificial intelligence in the law enforcement context. It is really important that we get those settings right as a first project, so we look at the ethical and the wider human rights impacts of those technologies. Fiona gave us some very good flag posts along the way to look at how we can meet those challenges. This year's Privacy Awareness Week theme is 'Be smart about privacy'. I think we will have some great resources online to deal with some of that as well.

There are a couple of other big things for the office. The implementation of Operation Impala recommendations across government and through the legislative process will be important so that we do not lose momentum on that. The CCC came up with some excellent recommendations. We are interested in seeing what the government response will be to those. In particular, the Law Reform Commission inquiry into technology and surveillance, and then the further one on workplace surveillance have the potential to have repercussions across the board for our office, so we will be keen to be involved in the government response. There are recommendations where there will not be legislative changes or that will not necessarily have resourcing implications and we are moving ahead to address them into the future. There is plenty of work for us to do besides in the privacy complaint areas. I invite the committee to participate in PAW 2020 online. Hopefully some of the virtual activities will be very interesting. I look forward to questions and addressing any issues that the committee wish to direct my way.

Mr LISTER: Good morning and thanks very much to Ms Rangihaeata, Ms Lynch and Mr Green. I have a question probably best directed to Ms Lynch regarding RTI. If an agency wishes to contest a final decision by you that the release of information is in the public interest and must be done, I gather that its recourse would be to QCAT. If that is so, what do you do when a decision is appealed in QCAT? What is involved on your part and what costs might be involved?

Ms Lynch: That is correct: when a formal decision is reached, the parties have a right to appeal to QCAT on a question of law only under the legislation. Our role is really to stand to one side. The decision speaks for itself. We do not actively participate in terms of making formal submissions to QCAT. That is a matter for the agency and for the applicant alone. Our role is to assist QCAT in understanding our processes. Sometimes they call for information about, for example, how various provisions may work or processes on review, generally. That is our role. It is really an assistance role to the court and we stand to one side. In terms of cost, each party typically bears the costs themselves. We run those matters internally within my unit, so we bear our own costs in that regard.

Mrs McMAHON: Thank you, Commissioners, for coming in. My question is probably a little more topical in this COVID-19 environment. We have a lot of officers now working from home. We have a lot of people now moving to online. Can anyone comment on what might be the hidden impact from a

privacy point of view and an information point of view, with thousands of people now doing their business online, whether they be public sector agencies or in education, for example? We now have thousands of kids sitting at home with emails and that kind of thing. I was wondering if any of the commissioners might comment on where we stand or your understanding of the agencies that you normally deal with and their preparedness for the sudden move to the online environment?

Ms Rangihaeata: I might start and also ask Phil to comment. It has been a really rapid change in uptake and I think some agencies are better prepared than others. There are some particular rules and guidelines around the use of different types of emails. We all know that people are required to use official email. I know that that is quite challenging for some agencies that are not set up well to work from home, so there are some challenges there for some people. I think people need to be really careful through this period not to forget about the risks that are associated if they end up having to use personal email for any purpose and the principles that are behind that in terms of record keeping and other risks and so on. That is a matter that agencies really need to be mindful of.

In terms of privacy, I know that we have been very careful to ensure that all of our staff are very mindful of all of the key things they need to think about when working from home, because it is a very different environment. Many of us now have a very full house in which we are trying to work. We are dealing with confidential information so there are a number of ground rules for our staff. We actually required people to tick off a checklist as to what they would do in terms of working from home around security, confidentiality and so on which went to a lot of privacy issues, record keeping and so on.

The eSafety Commissioner has also compiled and released some great resources for both parents and teachers around dealing with safety online. We have linked to those and promoted those on our website. As Phil said, the eSafety Commissioner is one of our key speakers for this year's Privacy Awareness Week launch event. She has excellent resources in that regard. We are very much promoting those and ensuring that people in our schools in Queensland are well aware of those resources, as is Education Queensland I am sure. I think a lot of parents are now grappling with that, as you say, and are quite mindful that there are risks with kids having more time online. We are all trying to ensure that we are watching over what they are doing online, but it is a challenge when you are trying to work as well.

As Phil said, we have been providing a lot of advice through this period about information sharing, about new arrangements. We have been working with our colleagues, around privacy in particular, across Australia in that regard. We issued a statement late Friday from all privacy authorities around Australia around the key principles that need to be regarded at this time. We are also standing up a national COVID-19 privacy advisory committee across all of our jurisdictions, because we are providing advice on a national stage as well that will cut across our jurisdictions. There was one other point that I was going to make, but I have forgotten. I might ask Phil, if I may, to comment on other issues that he may be thinking about in relation to your question.

Mr Green: Sure. It is a very good question and I think it is going to be an evolving one as we go forward. As Rachael said, there is quite a differing level of maturity in terms of what sorts of fleets people have and what kinds of arrangements they have. For instance, when our staff are working from home the data in transmission is encrypted. It is encrypted on the laptops. We have tethers for our laptops in the office. We have reminded staff about keeping physical security. The privacy team is meeting this afternoon to see whether there is a bit of a gap in some of our resources. Because some people have asked us for advice and in terms of the checklist that Rachael mentioned before, we were thinking of doing that as a template for other agencies to use. There are others that do not have as good security.

One of the most mobile fleets of offices out there is QPS with their QLiTE capability. Those devices have very high security on them. The back end in terms of auditing might need to be boosted following recommendations from Operation Impala. Likewise, even for our databases we are looking at whether we should boost those sorts of issues. I believe quite a lot of agencies have virtual private networks and have pretty good security. We have done some hardening of the fleets for government for things like G20 and the Commonwealth Games where there was enhanced hacking threats. Particularly with people working remotely, I think loss of devices is an issue where you might need to wipe a device or at least have it locked down very heavily. In our own case we have two-factor verification that is in place so you have to get a code from your phone or some other source to log in remotely to the databases. That is a particularly important safeguard and control. The physical security of devices is another one, particularly with a lot out in the field.

Hopefully there is some pretty good advice on working remotely and there is probably some more work we can do, because I think it will be an issue for all government departments and particularly ones that have not done so much to have their fleets mobile. We just fortunately—and this is through

some good luck, I suppose—had seen the need for being mobile and business continuity and we started getting that in place the year before, so it has worked out quite well with the virtual private network and using Datacom. I know that the Department of the Premier and Cabinet uses Datacom as well and I believe ECQ for their elections because they have a very mobile fleet out there. They have done quite a lot of work with security as well with their staff leading up into this local government election. Hopefully we can learn from the experience and perhaps do some more work with resources. I hope that answers the question. There are going to be some emerging issues as we go along in terms of fleets that will not be able to go mobile or particularly people who have not implemented Microsoft Teams and Office 365. There are some very good tools which we are using right now that are quite well developed and quite secure.

Mrs McMAHON: Thank you.

CHAIR: Member for Mirani, do you have a question?

Mr ANDREW: Not at this stage, no, Mr Chair. My questions have been covered by the other questions that have been asked.

Ms McMILLAN: I have a question in relation to challenging behaviour. You made reference in your annual report to identifying challenging behaviour in applicants as being a significant contributor outside OIC's control that influences timeliness. Are you able to elaborate on this?

Ms Lynch: Yes, I am happy to answer that and the Information Commissioner may have a comment as well. Challenging behaviour of any participant in a review process but particularly applicants can cause a delay in the sense that we are writing and talking to people about very specific issues under the legislation in relation to the information they are trying to access. We find that people who are exhibiting very challenging behaviour will not focus on those issues and may send, for example, very lengthy and repetitive unsolicited emails, documents and calls which our staff have to deal with, and in the context of a load of matters that is not the only matter they have. They have that constant interruption in trying to manage that behaviour on two fronts—that is, you try to progress the review appropriately but also if you are looking after your staff it is demanding and very time consuming. Does that help answer your question?

Ms McMILLAN: Yes, absolutely. Thank you.

Mr McDONALD: In previous years staff turnover has been a concern. In your business as usual before COVID, was staff turnover still a concern? Going forward from here, do you foresee that it will be a concern?

Ms Rangihaeata: Our staff turnover was higher before we had the permanent additional funds for the four external review officers. We got those funds in 2017, if I recall, so that has helped us to stabilise our staffing. We have not had a very high turnover rate since that time. I am sorry that I do not have the figures right in front of me at the moment, but we have not really had a high turnover rate of our permanent establishment. We do still have some temporary staff particularly backfilling long-term leave and secondments—long-term leave like maternity leave and things like that—and part-time. We have a number of people returning part-time for long periods, so we have opportunities for higher duties or people to come in temporarily. In that sense we do have people coming into the office, but it is not so much people leaving. We have a very high retention rate of our people here and we are very fortunate to have a wonderful team who enjoys working at OIC so, no, I do not think we have a problem with retention. It is more that we had a real difficulty retaining our temporary staff to staff those four roles before we had the permanent funding.

Mr McDONALD: Thank you.

CHAIR: Information Commissioner, is there any part of that question you want to take on notice or are you happy?

Ms Rangihaeata: I can certainly provide the retention rate, if you like, by this afternoon.

CHAIR: Is that okay, member for Lockyer?

Mr McDONALD: Of course, Mr Chairman. Thank you.

Mrs McMAHON: I have a question that goes back to the QLRC's report on civil surveillance in relation to protection of privacy. I was wondering if anyone would make any comment on the issue of increased civil surveillance and what the impact might be on the office.

Ms Rangihaeata: Certainly. I may comment briefly on that and then let Phil also make a comment. We know that the increased civil surveillance throughout the community by both agencies and the private sector and the community itself is of significant concern to the community. With the event of drones and even people just using their own phones and so on and smart cameras that people

have around their homes, people are under increased surveillance and they are aware of that and there are gaps in the legislative framework to resolve issues at present. The current review looks at a range of those issues.

We understand that the QLRC was required to report to the Attorney-General on 28 February and that the report would be tabled within 14 sitting days. It will depend now, but it was to be some time in August. We raised a few issues in our submission for consideration. Probably the most concerning one for us was some recommendations around the expansion of our jurisdiction, particularly the significant change in the nature of our jurisdiction, and that that be considered carefully. Similar recommendations had been made in other Law Reform Commission reviews in other jurisdictions. However, none of those recommendations have been implemented in any other jurisdiction.

Essentially, it would change to more of a law enforcement jurisdiction and that is not the nature of our jurisdiction at present, so that would require quite a big change. It would also change our jurisdiction from looking at agencies to looking at the private sector and the community, and that is a significant expansion and change to who we regulate, if you like. It would really expand the scope of our jurisdiction. It would significantly expand our need for resources and the nature of the skills and capabilities of the people that we would need here to carry out the duties involved. We just wanted serious thought to be given to whether all of the issues that were to be considered were necessarily the right fit for here or whether we could perhaps expand our enquiry service to cover some of those things but whether the law enforcement aspects in particular really should sit with our office.

Ms McMILLAN: I just wondered if you could talk a little bit more about your priorities over the next 12 months, particularly in relation to the technological change. I know you mentioned data analytics and artificial intelligence, but what are your priorities within that scope over the next 12 months?

Ms Rangihaeata: Phil, you might be best placed to speak to that in more detail.

Mr Green: Yes. There are wider human rights implications for both of those things, particularly the discriminatory impacts of those things and getting it right in the Queensland context. The first project I think I mentioned was distracted drivers. That is a very limited artificial intelligence tool but one which I still think we need to pay close attention to to get it right to make sure there is adequate human oversight and whatnot and address some of the issues that have arisen in the New South Wales context. I think we are all going to be pushed to do more with less and squeezing efficiencies out of some of our processes. A lot of that will not necessarily involve personal information, but I think the one thing in the Law Reform Commission context is use of biometrics for facial recognition by companies like Clearview where they are not particularly well regulated and the technology is not well understood but there needs to be some transparency.

Rachael has talked about building trust through transparency. It is really important that people deploying technology explain how it is being used and are transparent about the data that goes into it and then how the decisions are made and what are the review mechanisms for the decision so people can understand how they are being processed. That is something that in Europe has been discussed quite a lot in the privacy law under general data protection regulation. It has not really even entered into the Australian debate yet, but the ACCC has looked at it in the consumer arena. The federal government are pushing ahead with data analytics because they understand that they are sitting on a lot of data and that we can perhaps deliver some better services and get better outcomes if we use the data well. It is just a question of making sure that people understand it, the processing is transparent and it is well communicated. You can probably look at some federal examples where it has not been well communicated or less than ideally communicated—for example, the My Health account, the census even and the processing of data through Centrelink, which has been badly called robodebt, where the oversight mechanisms have not been good.

Queensland is looking at that artificial intelligence for things like collection of revenue, and Treasury have had projects where they have been trying to use the data to do things more effectively. It is just a question of making sure that we look at it closely and we put safeguards on it. Scott McDougall as the Human Rights Commissioner will also have a good lens of it for the wider human implications, not that it can be scary. I think technology can be neutral, but we need to go ahead and implement it and use it whilst fully understanding it and putting the safeguards in place.

CHAIR: That brings this hearing to a conclusion. I understand there is one question that has been taken on notice and you volunteered to have the answer to that question to us by this afternoon, but you can have until Monday, 6 April if you wish. I want to thank everybody for their participation and thank you for your obvious hard work. That was outlined in your presentation as well as in answers to

questions and also outlined in your annual report. That concludes the hearing with the Information Commissioner. Thank you to the secretariat and to our Hansard reporters. A transcript of these proceedings will be available on the committee's parliamentary webpage in due course. I declare this hearing closed.

The committee adjourned at 10.48 am.