T R A N S C R I P T

INTEGRITY AND OVERSIGHT COMMITTEE

Performance of the Victorian Integrity Agencies 2022/23

Melbourne – Monday 25 November 2024

MEMBERS

Dr Tim Read – Chair
Hon Kim Wells – Deputy Chair
Ryan Batchelor
Jade Benham
Paul Mercurio
Rachel Payne
Dylan Wight
Belinda Wilson

WITNESSES

Sean Morrison, Information Commissioner,

Rachel Dixon, Privacy and Data Protection Deputy Commissioner, and

Penny Eastman, Public Access Deputy Commissioner, Office of the Victorian Information Commissioner.

The CHAIR: I declare open this public hearing for the Integrity and Oversight Committees Inquiry into the Performance of the Victorian Integrity Agencies 2022/23. I would like to welcome the public gallery and any members of the public watching the live broadcast, and I acknowledge my colleagues participating today. I will just go from left to right: Rachel Payne, Jade Benham, Deputy Chair Kim Wells – I am Tim Read – Ryan Batchelor, Belinda Wilson, Dylan Wight and Paul Mercurio.

On behalf of the Integrity and Oversight Committee I acknowledge the First Peoples, the traditional owners of the land, which has served as a significant meeting place for the First Peoples of Victoria. I acknowledge and pay respect to the elders of First Nations in Victoria past and present and welcome any elders and members of communities who may visit or participate in the public hearings today.

To the witnesses: there are some formal things I have to cover, so please bear with me. Evidence taken by this committee is generally protected by parliamentary privilege. You are protected against any action for what you say here today, but if you repeat the same things anywhere else, including on social media, those comments will not be protected by this privilege. Any deliberately false evidence or misleading of the Committee may be considered a contempt of Parliament.

All evidence given today is being recorded by Hansard, and you will be provided with a proof version to check once that is available. Verified transcripts will go onto the Committee's website. Broadcasting or recording of this hearing by anyone other than Hansard is not permitted.

I welcome from the Office of the Victorian Information Commissioner Sean Morrison, the Information Commissioner; Rachel Dixon, the Privacy and Data Protection Deputy Commissioner; and Penny Eastman, the Public Access Deputy Commissioner. Thank you all for coming in to give evidence at this hearing. Have you got some brief opening comments?

Sean MORRISON: Yes, I do, Chair. They are brief.

The CHAIR: Wonderful. If you could start with those, and then we will follow up with questions.

Sean MORRISON: Thank you. Good afternoon. I would also like to begin by acknowledging the traditional owners of the land, the Wurundjeri Woi Wurrung people, and paying respect to elders past and present.

In my brief opening remarks I would like to speak broadly about OVIC's [Office of the Victorian Information Commissioner] role, impact and the significance of the work we do as an integrity agency. But first I would like to thank the Committee for its recent and very thorough report into the operation of the *Freedom of Information Act* in Victoria. This report recognises that Victoria's freedom of information requires modernisation, and OVIC supports the findings of that report, which closely align with the recommendations we made in our submissions to the Committee. We hope that the report acts as a catalyst for legislative change not only in relation to access to information but also in relation to Victoria's privacy and information security regimes.

OVIC operates, as many regulators do, in a challenging environment, with demands for our services continually increasing. For example, in comparison to the 2022/23 financial year, in the 2023/24 financial year freedom of information reviews received by OVIC increased by 7.3 per cent, FOI complaints by 19.4 per cent and privacy complaints by 25 per cent. To further highlight this point, this financial year we have seen an increase of 40 per cent in FOI requests received by OVIC and a 12 per cent increase in information security incidents reported to OVIC when compared to the previous reporting period. Regardless of this increased demand, OVIC was able to finalise more FOI reviews and privacy and FOI complaints in the 2023/24 financial year than in the previous reporting period. These outcomes are mostly due to the professionalism of OVIC

employees and the assistance of agency staff working with OVIC when we are performing our regulatory functions.

Apart from service demand increases, the current information environment also poses a challenge for OVIC and public sector agencies. The emergence and adoption of generative AI [artificial intelligence] and increased threat-actor activity are just two important issues that require OVIC's guidance and regulatory focus, both of which are resource-intensive. In order to meet these challenges, OVIC is undertaking a review of its processes, and we have recently updated our Strategic Plan, with our vision being a public sector culture that supports access to information and ensures its proper use and security. To bring this vision into reality, we will need to create regulatory certainty, enhance agency accountability, continue to champion information rights and advocate for best practices. Through this co-regulatory approach, we expect to improve outcomes and awareness of information rights in the public sector and the broader Victorian community. Information rights literacy is particularly relevant, with human error still the leading cause of information security incidents reported to OVIC.

To perform our legislative functions and adapt to changes in the information rights environment, OVIC requires independence. Being independent is critical to the way OVIC operates and the outcomes we achieve, whether through our regulatory actions, education activities or our monitoring and compliance role.

Once again, I would like to thank the Committee for their diligent work with the report, and I would also like to thank you for your time. I welcome any questions.

The CHAIR: Great. Let us go to Rachel Payne for the first question.

Rachel PAYNE: Thank you. And thank you for presenting before us today. My question is related to cookies or web bugs and website analytics. Does OVIC have any concerns over the use of cookies and website analytics on its website or on other government websites? And does their current use comply with privacy legislation and best practice?

Sean MORRISON: I will throw to Ms Dixon.

Rachel PAYNE: Thank you.

Rachel DIXON: Thank you for the question. We have done a lot of work on this. One of the things that we did quite early – some years ago – was move to Matomo, which we actually host, so the information is information that is held by OVIC. But we de-identify all of the IP [Internet Protocol] addresses, and people have the option to opt out essentially and delete cookies and things like that automatically. We do not place a cookie if you have chosen to opt out.

We had a fairly notable case at VCAT [Victorian Civil and Administrative Tribunal] where somebody tried to basically say that because we were recording IP addresses in the server logs, we were therefore capturing their personal information. VCAT found that IP addresses in fact are not personal information in that particular case. In terms of cookies, yes. I am aware that you might have somebody here who has worked in digital media and has some exposure to this.

The data economy is a huge enterprise, and the companies that are collecting this information have multiple reasons for wanting it. Some of that is outside of our jurisdiction, because a lot of those are commercial entities that are governed by the federal *Privacy Act* [*1988* (Cth)]. Government bodies, though, should be conscious where they are collecting information through the use of cookies and particularly things like, for example, Google Fonts and things like that, which are tremendously useful but nevertheless send information to Google. We have raised previously that that is not great practice. I am aware that many people still do it. Most government agencies still use Google Analytics, and they do that for the purposes of improving their websites and various other things. It is probably something I would prefer people not to do, but it is not for us to say, 'Look, you must use this other system.' It is just that that particular issue is of concern to us.

Rachel PAYNE: Are any legislative reforms needed in this area?

Rachel DIXON: The problem I think in that space is that, because of outsourcing and other arrangements, it would be almost impossible to have a Victorian law that prohibited something like that. I think if you had a national law that would then easily bind the contractors, bearing in mind that a lot of the contractors have other

commercial clients. So just saying, 'Well, Victoria's not going to let you do this thing if you're a contractor to the Victorian government' would be tremendously difficult to administer, so I am not sure that it is a practical solution at the State level. But I think we have seen over the last 20 years, ever since the birth of Google AdWords actually, that Google – I am not punishing Google here – moved their model from organising all the world's information to organising all the information about people watching ads, which is a different mission statement. And there does need to be reform. I think the federal *Privacy Act* reforms that were proposed in that area had some suggestions, possibly, but it is not my jurisdiction, so it is not for me to say.

Rachel PAYNE: I appreciate that. Thank you.

The CHAIR: Great. Let us go to Jade Benham.

Jade BENHAM: Thank you, Chair. I think it would be interesting if Australia moved to try to legislate against Google in the first instance. It would be very interesting. But with regard to cyberattacks and cybersecurity and that information that OVIC holds, what sorts of initiatives has OVIC put in place to mitigate or prevent – I know that preventing cyberattacks is the ultimate – or lower the risk of cyberattacks and security breaches?

Sean MORRISON: Look, I will answer that question first and then throw to Rachel. I think that the Protective Data Security Framework and the work we do working for co-regulatory approaches – we work with organisations. We are not on the ground in those organisations, so we provide a framework that is a risk-based framework and we expect agencies to work with that, and we have a lot of agencies calling us and seeking guidance. The first thing we do is through co-regulation we provide that expertise and guidance to lift the literacy of information security. What we would like to see is legislative change to have all organisations subject to this information-security scheme, because we are only dealing with a small subset of the public sector. There are other agencies that we would like to be subject to this framework at a minimum standard. I think the first two things for us are that it is through that education but then it is also through legislative change. Rachel.

Rachel DIXON: One of the things that we initiated at OVIC – we do not collect the actual full SRPAs [Security Risk Profile Assessments]. We get the attestation from every body head, but we do not get the full documentation, we get an abstract, if you like, of what the status of the agency is. We then choose a set of those organisations. We meet with them, and we work through their PDSP in detail, but that means we do not become a honey pot for all the vulnerabilities in the Victorian government. That would not be terribly helpful.

We do maintain an active security program in our own office. We will be doing it again shortly, but, for example, we do red-teaming exercises where we do data breach responses and things like that. They are tremendously useful. I recommend that every agency do them. We regularly review our Microsoft secure score. We are in the 90s for that. If Microsoft would stop changing things, that would be very helpful, but it is an ongoing thing. And because we are concerned about security of physical information and personnel as well, we maintain a secure office that is actually not accessible by anybody outside the building. If they do break in, then we are alerted.

Jade BENHAM: And that is where your own servers are?

Rachel DIXON: No. Actually, we have most of our servers in the cloud. We moved to the cloud in 2022. We did that because I had some concerns about where they were on level 6 of 121 Exhibition [Street]– it did not have redundant power. It was not a tier 1 centre, it was just an office building. I did not like that. I have a background in hosting, so we moved into a cloud-based system for almost everything. We have some backup services on premises still. Because they are just for backups, it did not make sense to pull them down.

Jade BENHAM: Okay. Just one more, Chair.

The CHAIR: Go ahead.

Jade BENHAM: With the agencies that you would like to bring along – and you were speaking about legislative change – are you able to expand on that at all?

Sean MORRISON: Hospitals are not included, for example, so that is one – and some courts and tribunals. Rachel, would you have any?

Rachel DIXON: We have recently seen several breaches that have involved tribunals and courts. Interestingly, the language in the Victorian Act is – if you changed one word, for example, to mirror what is in some of the other States' Acts, it would greatly assist the coverage of those bodies. In other States, they are regulated much more carefully. Obviously, we cannot interfere with any judicial functions; that is not the point of the exercise. But, yes, there are. And courts of course have all this very sensitive information and a lot of personal information. When the hospitals were being 'ransomwared', for example, which I think was back in about 2019 or thereabouts – I liaise very closely with the government chief cybersecurity officer; we meet at least monthly, sometimes more often than that. We have an MOU for exchange of information, and we regularly then meet to discuss breaches that have happened. We are not the 24-hour service. CIRS are the 24-hour service. We do not interfere until there is sort of a resolution, and then we might look at,'Well, was this preventable? Should we take some further action to put on a compliance notice or something to make sure it does not happen again?' But, by and large, it is better to let the people who are good at restoring systems do the restoration and cleaning than it is for a regulator to just stumble in and ask all the same questions. They would be dealing with it twice. So, we do not do that. To Sean's point about where we can collaborate, we do try to do that, because it is much more efficient.

Jade BENHAM: Great. Thank you.

The CHAIR: Great. Kim Wells.

Kim WELLS: Thanks. OVIC made a number of recommendations to VicPol [Victoria Police] to assist in implementing their information security and privacy. What progress have they made, and is it at the benchmark that you would expect?

Rachel DIXON: If I can take that one, I think the last time I appeared I spoke about the fact that we had some very old recommendations that had not been implemented by VicPol and that one of the problems with that was we did not put a time. The then Commissioner, and this is way back in the days when it was CPDP [Commissioner for Privacy and Data Protection], did not put a timeframe on when those things should be done. Of course, now, some of them are so old that they relate to systems or processes that do not exist. So, we have been winnowing through those gradually. We have got them down. I think we have got 13 outstanding from 2012, and we currently think we might be able to resolve 8 in this calendar year. We have three from an investigation that we ran in 2022, where we made specific recommendations to Victoria Police about their privacy practices. They will be closed soon. They relate to things like training and handling of material and things like that.

Kim WELLS: So, you would be blaming the police, not the police minister at the time.

Rachel DIXON: It is not my job to criticise the minister.

The CHAIR: We will pass immediately to Paul Mercurio.

Paul MERCURIO: Very quickly. Sean, in your opening statement you talked about the proper use of information. During the freedom of information inquiry I was very interested, concerned and frightened about the rise of AI and its use and what it may be. I am just wondering: what initiatives, if any, is OVIC thinking of undertaking in relation to the use of things like AI and ChatGPT, et cetera?

Sean MORRISON: Earlier this year, we released guidance on what we thought was the proper use of, or should we say the dangers of using, ChatGPT in the public sector. That is a resource that has been heavily used by the public sector. We produced guidance on the use of Microsoft Copilot as well in the public sector. That was late last year, I believe.

Rachel DIXON: I have both of those with me if anybody is interested.

Sean MORRISON: Yes, before my time. Those two resources – we were the first regulator out of the gate to issue those, and they have been leaned on by other regulators across Australia and incorporated into legal

firms' materials. They exist unchallenged, so we have set those foundational pieces. We also work with CIRS at DGS [Department of Government Services] to comment on whole-of-government guidance. We are working in the background on that, lifting that literacy around AI and the use of the appropriate tools.

We have also done an investigation into the use of ChatGPT with the Department of Families, Fairness and Housing. That is on our website; we are able to provide it to the Committee. It found basically that certain IPPs [Information Privacy Principles] – IPP 3 and IPP 4 – were not adhered to. It is one of the situations where we are trying to ensure that there is no use of AI in high-risk environments, like in child protection. That ended up with a compliance notice. We have also commented on federal regimes, and we are trying to nudge the needle slightly against the AI hype.

Really, I think we have front-footed it quite well. There is more to come; there are more resources. We have one out for consultation now on the use of AI. We have gone out to everyone and said, 'What do you want to hear about AI? What is it that OVIC is not doing, or how do we fill the gap?' That is, I think, a broad summary of what we are doing.

Paul MERCURIO: Does OVIC use AI currently?

Sean MORRISON: No, not really. One caveat, though.

Paul MERCURIO: A bit more complicated?

Sean MORRISON: Yes.

Rachel DIXON: Caveat: we do have a cybersecurity tool. Obviously, most agencies will have one that looks for phishing or other kinds – that is actually algorithmic. Likewise, network intrusion detection is a thing. I will say just very briefly that when we talk about AI there are different kinds of AI. There are very specific tools that do certain things very well because that is the sole domain that they work in; they are not trying to be all things to all people.

The general-purpose tools that you are seeing that are coming to market, like Copilot, exist in a range of things. Because context is absolutely critical to understanding the risk that AI poses in general circumstances, those general-purpose tools, we would say, are not sufficiently reliable to be trusted. And this is consistent with guidance – it is fine. The Department of Government Services are producing some guidance; they have taken a lot of our comments on board. Nobody expects that you should be able to deploy AI without having to read everything it writes, so that is our current consistent guidance. I do have a presentation that I presented to the Victorian government AI summit which I am happy to share with you. I can give it to you electronically, but I also have printed copies here, together with the actual speech notes and all of the underpinning research, because there is a lot of stuff here that talks about the issue of context.

We will not deploy Microsoft Copilot in our environment. We were forced to use a tool recently to do some recording of a presentation we made, and I subsequently discovered that in order to do that Microsoft made it mandatory that we turn on Copilot. So, we will be using a screen-recording tool to record presentations in the future. We will not be using Copilot.

Sean MORRISON: Just on that point, sorry, we do have an internal policy that is about to go on our website – we publish most of our policies – which basically says that staff cannot use AI, subject to my discretion where our policy team needs to research or there is a specific use case. So, that will be our approach going forward. And in our attestations for the security framework we asked organisations what their use of AI was, so we are starting to get some 'intel' as well about the use of it.

The CHAIR: I think our members might be interested to see that presentation that Deputy Commissioner Dixon mentioned.

Sean MORRISON: Absolutely, yes.

The CHAIR: If you would not mind emailing it.

Rachel DIXON: I can send it electronically as well, if that is more useful.

The CHAIR: I think electronically would be useful. Thank you very much. Let us go now to Belinda Wilson.

Belinda WILSON: Thank you. Thanks for joining us. The question of funding and money is always a great question, and no-one is ever going to say it is always enough. But does OVIC consider that they receive sufficient funds to do investigations into regulatory compliance in all areas?

Sean MORRISON: Could I reframe that question, and then you might ask me it again. I think the question for me is: Do we have enough funding to be an effective and competent regulator? I think we do, and I think the obligation is on me and on the Deputy Commissioners, but more on me, to ensure that whatever our funding envelope is, we pivot or we move in the way we do our processes or we change our regulatory focus to make sure we have the trust of the public sector and the trust of the public and we are an effective regulator. I think some of those statistics I provided before, and our annual report, show that we are hitting most of our metrics and our performance has improved during these challenging times. I am happy to elaborate further if you need me to.

Belinda WILSON: No, no, no. That sounds great. I guess I can also ask you: How are the FOI requests being managed? Are they being managed in a more timely manner?

Sean MORRISON: At the moment our timeliness is within our performance metric, and with Penny being recently appointed, we are going through a process change. We are looking at, end to end, how we can improve timeliness. I am happy to say to the Committee that I would like timeliness to improve, and that is on me and my performance. It is not an impact of budget. I think it is an impact of how we do things. Timeliness could be better, but it definitely is sufficient.

Belinda WILSON: Thank you.

The CHAIR: Thank you. Can we move to Ryan now?

Ryan BATCHELOR: Sure. Just a quick follow-up to Paul's question: you mentioned, Commissioner, the use of AI in high-risk environments in one particular area. What other environments across the public sector, do you think, are high-risk for the use of AI in decisions?

Sean MORRISON: Rachel, you can elaborate as well – I know you will. I think it is where you have information that is quite sensitive. That might go to things like taking personal information and drilling down into that subset of information, information that is quite sensitive – biometric information, for example. To me, it is the environment it is used in – as in the damage, the harm, that can come from the outcome. It is not just that you are using personal information in there. It could be, 'Is this a critical decision that could take away someone's freedom or incarcerate them or have a court order used against them? Where is the human in the loop?'

I think the other factors are that you are putting that information into a model that you do not control, so eventually this data lake is being built up of people's personal information and sensitive information that could be weaponised or used in another environment. I think what makes a high-risk environment is not just the currency of the information but it is the outcome and the potential to cause harm. Someone looking at it just from a data lens [perspective] might think this is quite a simple process, but they are not thinking about the outcomes and the potential for harm.

Rachel DIXON: There are things I would prefer it not be used for that have been authorised to be used. You will note that the education ministers nationally made a statement allowing teachers to use ChatGPT, for example. I would prefer that in the context of – now, I am sympathetic to the workload that teachers have. I know what it is like to have to write reports on all your students. But it would be inappropriate, because it is deeply personal information, to use ChatGPT to write a report card. The reason for that is that that information on the student's performance is travelling to California where it is held by OpenAI, and it never comes back. I am not being a conspiracy theorist, but should OpenAI have 10 years of educational prowess or failings on all Victorian students? I think that is probably an undesirable outcome, quite apart from breaching the privacy of the individuals whose reports are being read. As I said, the education ministers have all collectively across the country said teachers can use AI, that it will help their jobs. I am sympathetic to the goal; I think it is an inappropriate use of the technology.

Sean obviously mentioned child protection; it is just a doozy. But, also, if you are doing internally hosted models, where the data is not travelling, obviously the risk is slightly less. But there is the risk of incorrect information being stored if you are using an AI, and that is a breach of the *Privacy Act* as well.

I would not like to see this used in Human Resources [HR]. There is a lot of evidence that commercially available HR tools have fairly large degrees of bias against certain ethnicities in them, so the government as best practice should really try and steer away from those. That includes in the contract service providers they are using to do some of those services. I am aware that at least one of those contract service providers uses an algorithmic tool to assess candidates before providing a short list to their clients. So that is something to watch because you would not know. How would you know if the short list was biased? You do not have the ability to compel the algorithm.

It is interesting that in the competition space there is a notable case that the ACCC [Australian Competition and Consumer Commission] ran a couple of years back where, because in competition the powers of the regulator are much greater, the ACCC was able to compel the provision of an algorithm that recommended hotels and flights. They got the algorithm and all the data, and they ran it in their own environment and were able to show that it did not do what the company Trivago said it did. There is no corresponding power for any Victorian regulator to do something like that, nor actually, functionally, are there the skills or the facilities to do it. But it is an interesting way of looking at how we prioritise regulation in certain areas and not in others. It is such a fast-moving field as well that it is very difficult to say we should regulate this in this way or we need a new Act to do 'x'. I actually think that the tool – the legislation – that Victoria already has is a pretty reasonable ruler to run over most AI projects. So that is an answer to a question you did not ask.

Ryan BATCHELOR: I always like those.

The CHAIR: Did you want to ask another question or are you good for now?

Ryan BATCHELOR: I am good for now. If we have got time, I will come back.

The CHAIR: All right. Let us go to Dylan Wight.

Dylan WIGHT: No worries. Thank you, Chair, and thank you, everyone, for appearing. OVIC is developing an evaluation and assessment framework for its education and prevention program. I am just wondering where that is up to and how much progress has been made.

Sean MORRISON: We are still working through that process. Given that we have just done our Strategic Plan, we are looking at our education model. By the time we next appear before the Committee it will be firmed up and delivered, but, given our funding envelope, I am a new Commissioner, I have a new take on where we want to go, we are looking at our Regulatory Action Plan – all of these things – education is just one of the things that we are developing. It has sort of been reset since I was appointed, to be honest.

Dylan WIGHT: I guess just for the benefit of the Committee, Hansard and anyone watching maybe you could just go through exactly – not exactly, but broadly – what it might look like, what it may cover.

Sean MORRISON: I think I mentioned the co-regulatory approach before. Neither OVIC nor any regulator has the resources or the time to deal with every single potential alleged breach or every FOI request or every security incident, so it is about trying to lift the digital literacy and the literacy of information principles with the agencies we regulate. That is, we have FOI [Freedom of Information] guidelines and privacy practice notes. We are trying to get better engagement with them because they show everyone the standard that OVIC expects everyone to work to.

In our Strategic Plan one of the first things I mentioned was creating regulatory certainty. If everyone knows when OVIC will investigate, when they will not, what the threshold of risk is, what the expectation is – we do not think it is out there, given I referred to the fact that human error is still the biggest cause of information security incidents. We do not see the training being delivered by agencies that is needed, so we need to step into that void.

That is the first plank of it: looking at our regulatory model in that there is this tension between when we say to people, 'Please report incidents to us,' but then, on the one hand, we might investigate those incidents. So, it is about looking at the balance of when that is right, because we want people to come to us with clean hands and

say, 'We've had this incident. Can you work with us?' We want that remediation and mitigation to take place straightaway. We do not want these things to be happening in the background and we find out versus where we see abhorrent conduct when we investigate. They are the things we are working through now, that tension, but really we want this open dialogue with agencies and for them to know exactly how we are going to act in certain situations and what the expectations are on them.

Dylan WIGHT: Okay. Beautiful. Thank you.

Sean MORRISON: Sorry, that was a longwinded answer.

The CHAIR: Thank you very much. In the 3 or 4 minutes we have got left, just briefly, I have got to ask about lessons you have learned about oversight, particularly for outsourced government operations, and whether this is from the FOI perspective or the information security and privacy perspective.

Sean MORRISON: Just quickly from my point of view, we have got some new guidance that is going out for consultation on contracted service providers. The expectation there is that when agencies are contracting with a provider, they pass on all of the requirements to those agencies, whether that be access to information, privacy or information security. We do not believe that is happening now, and that is one of the considerations. So, from my point of view, we need to pass on those obligations and make sure that we bind contractors and subcontractors so that, if there is a breach, we have the jurisdiction, but, also, there is a right of recourse.

The CHAIR: Thank you. We have got a minute and half left. Jade Benham.

Jade BENHAM: Further to that, if you do not believe that contractors and subcontractors adhere to all of those measures, is that a huge concern?

Sean MORRISON: Yes.

Jade BENHAM: I would imagine.

Rachel DIXON: We have an abbreviated investigation report on a contract to a provider that was breached last year. It was abbreviated because the company went into administration, and since our powers to investigate are based on whether or not we intend to issue a compliance notice, it seemed fruitless to continue going in that direction. But that was an organisation that was contractually required by several government agencies to delete the data they were collecting within a matter of months, and they still had not seven, eight, nine, 10 years later. The volume, the exposure from the breach, was much greater. You can read that report on our website. I would be happy to send a copy to the Committee if you would like.

There are also a couple of other breaches that we are aware of that we did not do investigations on because CIRS did their work and we did not see a role for us. Again, the volume of information that was exfiltrated was much higher than it should have been. Deletion costs money. This is the point: when you contract with a contract service provider, it costs the contract service provider money to delete data. They have to actually get somebody to go in and clean the data out of a database without the database collapsing, so you have got to do some testing afterwards. Nobody is going to do that unless somebody is monitoring whether they are doing it, and agencies typically say, 'It's in the contract; they must do it.' In the case of the breach I was mentioning, they were contractually obliged to do it; it was just that nobody had checked that they were ever doing it.

Jade BENHAM: Which was my next question – who checks and enforces that data is be deleted?

Rachel DIXON: The government agencies should, but, again, it is a question of resources on both ends. It is always the first thing that fails.

Jade BENHAM: That is a concern. Thank you, Chair.

The CHAIR: All right. Thank you very much.

Given the time, I think we will suspend the hearing now, but not before we have thanked Deputy Commissioners Dixon and Eastman and Commissioner Morrison for appearing before us this afternoon and answering all our questions. Thank you all very much.

We will take a break and be back in 5 or 10 minutes.

Witnesses withdrew.