TRANSCRIPT

PANDEMIC DECLARATION ACCOUNTABILITY AND OVERSIGHT COMMITTEE

Review of Pandemic Orders

Melbourne—Tuesday, 29 March 2022

MEMBERS

Ms Suzanna Sheed (Chair)
Mr Jeff Bourman (Deputy Chair)
Mr Josh Bull
Ms Georgie Crozier
Mr Enver Erdogan
Ms Emma Kealy
Ms Harriet Shing
Ms Vicki Ward
Mr Kim Wells

WITNESSES

Mr Sven Bluemmel, Information Commissioner,

Ms Rachel Dixon, Privacy and Data Protection Deputy Commissioner, and

Ms Joanne Kummrow, Public Access Deputy Commissioner, Office of the Victorian Information Commissioner Victoria.

The CHAIR: Welcome. Thank you very much for attending today. I will just read out a few housekeeping matters. All evidence taken by this committee is protected by parliamentary privilege. Comments repeated outside this hearing, including on social media, may not be protected by this privilege.

All evidence given today is being recorded by Hansard. You will be provided with a proof version of the transcript to check. Verified transcripts, presentations and handouts will be placed on the committee's website as soon as possible.

I welcome our witnesses and would ask that perhaps you make a 5-minute opening statement to being with. Thank you.

Mr BLUEMMEL: Thank you very much, Chair, and thanks to you and your colleagues for the opportunity to be here today. I am joined by Privacy and Data Protection Deputy Commissioner Rachel Dixon on my left and Public Access Deputy Commissioner Joanne Kummrow on my right.

The Office of the Victorian Information Commissioner is the primary regulator for information privacy, information security and freedom of information in Victoria. We are independent. We do not report to executive government but of course directly to you, the Parliament. Our role in protecting privacy is also, importantly in this context, complemented by the office of the health complaints commissioner—that obviously is the privacy of Victorians' health information—as well as the Victorian Equal Opportunity and Human Rights Commission.

The committee of course today plays a very important role in reviewing the pandemic orders made by the minister under the *Public Health and Wellbeing Act*, and we understand that this extends to reporting to Parliament if the committee considers there are certain issues with a pandemic order, such as the order appearing to be made out of power or being incompatible with human rights. Now, our role at OVIC is obviously quite limited in that context, given the public health focus of pandemic orders, but we will of course assist the committee in any way today that we can.

The right to access government-held information and privacy are both essential features of a healthy democracy and essential to building and maintaining trust, and that cannot be overstated. Trust impacts the effectiveness of public policy and the efficiency of public services, and as we have seen over the last two years, trust is crucial to the success of public policies that depend on a behavioural response from the public. Of course the orders that you are looking at have a profound impact on the lives of all Victorians. To this end it is pleasing to see the requirement for the minister to table a statement of reasons for the making of pandemic orders in Parliament along with a copy of the advice on which they are based and a statement of human rights charter's considerations. We see that as a positive development for transparency.

Clearly trust is also essential in how a government handles our personal information as citizens, and the pandemic saw an increase in the collection and use of personal information in pandemic response. Often members of the community had no choice but to provide their personal information to access essential services, and if the public does not trust that the collection of personal information is necessary and proportionate or that their personal information will be protected, then the public will be less likely to follow the letter and the spirit of the law. This makes it particularly important. Under the *Privacy and Data Protection Act 2014*, organisations must collect only what they require, only what is necessary for their functions and activities. It has got to be kept for a specific purpose, and the practice of collection must end when the personal information is no longer needed. All of those topics are of course very germane to pandemic response. We have seen of course this minimisation of collection play out recently, and the information being collected now in fact under

the order is less than under previous iterations of the order, which again we see as appropriate and a promising development.

It is also important that people are told why their information is being collected, what it will be used for and how it will be secured. All of these things are essential, in our view, to building trust. Under the order, of course, it is collected for a particular purpose and agencies are not authorised under that order to use it for unrelated purposes, and of course that is of interest to us. But just in conclusion, for my opening statement, the last two years have really highlighted the importance of balancing the effectiveness of pandemic response initiatives with ongoing respect for privacy, transparency and human rights. And with careful consideration public policy does not have to be made at the expense of privacy rights, nor at the expense of transparency. It is possible to implement effective public health measures while respecting privacy and being transparent. A privacy-by-design and transparency-by-design approach to the development and implementation of all public policy helps to maintain the public's trust, particularly in uncertain times.

Thank you again for the opportunity to be here along with deputy commissioners Dixon and Kummrow. I look forward to answering your questions.

The CHAIR: Thank you. I will start with a couple of questions before we go to other members. We had Service Victoria this morning, and I think we learned in the course of their evidence that they are much more of an agency around forming the capability for capturing information rather than dealing with it. Their evidence was that they have set up the systems, the coding, all those things, for QR coding and vaccinations and the like, and that that is then transmitted to the Department of Health, which are really the repository of that information. I am just wondering what level of oversight you have over Service Victoria.

Mr BLUEMMEL: We have got a considerable level of oversight. Not only is Service Victoria bound of course by the *Privacy and Data Protection Act* itself but under its own legislation it provides us with an annual statement of its activities, which Deputy Commissioner Dixon can talk to in more detail if you wish. But in addition to that I think what is really important for us, to make sure that these things are done in a privacy-respectful way, is that we work closely with Service Victoria in things like initially conceiving of how information will be collected, used and disclosed.

The example you have just given there, that really it is the capability and Service Victoria do not generate a large repository of information that is then retained, is very much in keeping with the sort of advice we give to them. It is also required, of course, under law in most cases, but we work with them to make sure that collection is minimised, duplication of datasets is minimised—all of those things reduce privacy risks and reduce security risks.

The CHAIR: Are you aware of whether there have been any privacy breaches, or attacks even, on Service Victoria in their role? I mean, given that we are in a world where there is so much of that happening and governments have been very much under attack, it is obviously a way that people's privacy can really be seriously compromised. So I am just wondering what your experience or knowledge is in relation to Service Vic in particular.

Mr BLUEMMEL: Sure. There are two main ways we would find out about such things—two formal ways. The first one is that under the *Victorian Protective Data Security Framework*, which my office administers, agencies are required to inform us of data breaches. And the second way we would find out about something like that in a formal way is by us as the privacy regulator receiving a complaint or even an inquiry from an affected member of the public, for example, who considers that their privacy has been breached. Now, certainly in terms of the work in the pandemic response, with contact tracing, check-in, vaccination and so on, I am not aware that we have had any formal complaints in that regard. We have had a few queries around check-in in general, but none of them have actually gone to any sort of formal complaint. Often they were resolved quite informally. There may have been a misunderstanding. There may have been a lack of understanding of where data travels and what is collected.

Ms DIXON: If I may, within the scope of your remit—your current inquiry is into the current pandemic orders—I think there have been no complaints. Under the previous order there was one which was successfully conciliated. It was in relation to the collection notice. So it was not a breach per se. It was not that the data leaked out all over the place. It was that the full purposes of the information were perhaps not as clearly

articulated as they should be. That was successfully conciliated by our office, so no further action was required. Under our Act we conciliate matters; we do not have the power to make decisions. If it wants to be appealed, somebody can appeal to VCAT, but no appeal was made. So the complainant was perfectly happy because the collection notice was amended to be correct. So members of the public have the capacity to go and lodge a complaint about the information they might have been required to give during the pandemic, for instance? Health information, for instance.

Mr BLUEMMEL: There are a couple of things we need to distinguish there. What they can complain to our office about is that we have a role under the *Privacy and Data Protection Act* to ensure that agencies comply with the information privacy principles—the 10 principles in that Act about use, disclosure, collection of personal information and so on. Certainly those principles apply, including to the collection, use and disclosure of personal information in a pandemic response context, but an important thing to distinguish there also is that to the extent that it involves health information—things like vaccination and positivity status of COVID are considered—that will be health information and that then is under the jurisdiction of the health complaints commissioner. We work very closely with the health complaints commissioner as well. I might just ask Ms Dixon to talk, broadly speaking, about what the powers are that we actually have when someone does make a complaint to us, because we have different powers to VCAT.

Ms DIXON: I think—and again I am now referring not to the current orders because they are quite different to the previous ones—under the previous ones, for example, we did have several inquiries which were to do with private businesses of course collecting information under the previous pandemic orders, and of course we do not regulate that. That is a matter for the Office of the Australian Information Commissioner because those are private bodies. So we then refer those complaints on to the OAIC, provided they meet the threshold for OAIC complaints. You might be aware that in Australia businesses with a turnover of less than $3 million are not covered by the federal *Privacy Act*.

The other thing to follow on from Sven's thing: where we have had inquiries, and my understanding is we had 11 inquiries under the previous orders about the use of health information, in each of those cases of course there is nothing our office can do because we have no power whatsoever to deal with matters that involve health information. Anything that is subject to matters under the *Health Records Act* is explicitly excluded from the *Privacy and Data Protection Act*. So in that situation we refer on to the health complaints commissioner, and then people are free to take that complaint to the health complaints commissioner.

The CHAIR: So you do the referral?

Ms DIXON: It depends on the circumstances. In all of these cases, actually—sorry, I should clarify; there are possibly two or three that I am not completely sure of the way this was communicated—my understanding from the briefing that I got is that with the overwhelming majority of those complaints people said, 'Oh, well, okay', and did not take it further. But in some cases they may have taken those to the HCC. If we thought it was a serious matter, I would write to the health complaints commissioner, saying, 'I believe this merits your consideration'. But generally speaking we do not do that.

The CHAIR: Right. In the few seconds I have got left, I am just wondering: in the context of a pandemic did you have to really ramp up and resource yourself more fully, thinking that there may be a whole lot of issues for you as the Information Commissioner during what has gone on, really?

Mr BLUEMMEL: There was certainly some of that. It was not so much a matter of increasing our net resourcing. Clearly we would only be able to do that through the budget. For us, it was more an issue of internal prioritisation. We knew that these issues would almost certainly increase, because the pandemic response, whichever shape it would ultimately end up taking, would almost certainly involve a substantial collection, use and disclosure of personal information, whether for contact tracing, modelling—whatever the case might be. But we already had at the time a very substantial capability dealing with privacy generally, dealing with things like the impact of privacy on data analytics. All of those sorts of things—we have got very experienced staff in that regard. So it was simply a case of making sure that they were ready and available for the likely workload, which we did get. But what we did not get was a substantial increase in complaints to us in that regard. It was more the proactive work of us reaching out to the agencies involved in pandemic response to make sure that what they did was not only in accordance with the law but also genuinely respectful of individual rights.

The CHAIR: Thank you. I will go to Mr Bull now.

Mr J BULL: Thank you, Chair. And thank you, Commissioner and deputy commissioners, for being here with the committee and answering questions today and for the role you have played through the course of the pandemic but also the important role that you play across our state in independently reporting to the Parliament. Of course, as some of the Chair's questions have just alluded to, the way that the Victorian community have seen data and information through the course of the pandemic I think has changed. If we just look at check-in data and those sorts of things, we know that people would certainly have not expected to have been checking into places just three years ago. One thing that has emerged as an important tool for managing the spread of COVID has been of course the collection and use of these types of data. I just wanted you to be able to tell the committee: what type of engagement have you had with the Department of Health in relation to data collection and usage over the past two-and-a-bit years?

Mr BLUEMMEL: Yes, we have engaged with the department on a fair few occasions in this regard. Again I might ask Ms Dixon to take us through any more of that in greater specifics. But it has been pretty substantial because, as I said at the outset, we are really keen to make sure the government respects those principles of good privacy management: minimise collection to what is really required, keep it for as short as possible, do not duplicate it in many places, only duplicate it to the extent absolutely necessary, delete it once it is no longer required—all of those fundamental principles of privacy protection and indeed in many cases information security as well. We thought there would be a danger in a situation like this—that some of those principles would go by the wayside if we were not active as a regulator. So we were very, very careful to ensure that we engaged in that regard. That is why, as I said in my opening statement, it is pleasing to see that now, with the new orders, the amount of information collected is decreasing, which I think seems entirely appropriate to where we are in the pandemic. That is good privacy practice. The temptation to retain things for a long time just in case they might come in useful is something that we obviously advocate very strongly against.

All of that of course is in the context of what we term 'personal information' under the Act. Broader statistical information, genuinely statistical information from which individuals cannot be identified—that of course will continue to have various benefits for presumably planning future response and so on, and that does not need to come at the expense of invasions of privacy through the use of personal information. So that proportionality minimisation is really important. But for any further specific interactions with health, I might hand over to Ms Dixon.

Ms DIXON: During the course of the entire pandemic, so not just the course of these orders but the entire pandemic, we were involved in meetings—and I put this in the context of not just phone calls that my guidance team might have with the department from time to time but formal meetings that either I or one of my assistant commissioners was present with—12 times with the Department of Health. Several of those were multi-organisational meetings. There were quite a few, for example, I think we could probably say after the first few months of the pandemic where many agencies were gathered around the table to make sure about things. I should be very clear here, and I think Sven alluded to this before: our role in these is to provide guidance on what the Act provides for and what our views on privacy are, but we do not design things for the government. It is the government's role to develop the capability. All we do is administer the Act that Sven and I are both stewards of. So it is not appropriate for us to say, 'Well, you should definitely do it this way'. That is a matter for government, and we can just advise whether or not that will meet the requirements of the Act. So in those meetings quite often we were more the observer than the designer, if that makes sense. But they did consult with us very extensively. In addition to that, obviously our office issued guidance to agencies, including the Department of Health, which we published. That went on our website, it went out via social media and various other things, and that applied to members of the public as well as to those agencies. But we had 12 meetings with the Department of Health.

Mr J BULL: Thank you. That is very beneficial and also pleasing to hear that over the journey of those 12 meetings, whenever those issues were raised, albeit you were not the designer of the initiative or program that was being implemented, you were around the table providing that advice in relation to the Act. That is very pleasing to hear. In circumstances where there may have been a tension in terms of the advice that you as a commissioner and as deputy commissioners are providing within the course of those meetings, how do you resolve the tension around whatever the specific initiative or program may be? Is it a case of you are putting up an advice and then those conversations follow from there, or can you give us any examples of where that may have played out?

Ms DIXON: Usually what would happen would be the department—a department; it might be DPC, it might be the Department of Health; you know, there are various organisations—may suggest that they think that something is a way to resolve a particular issue. In the case of the pandemic DPC with their digital capability obviously were involved in trying to put together various systems for how the data would flow. They would put a hypothesis up. Various agencies, not just us, would give views on whether or not that was sufficient for what they believed the purposes were. We would advise them on the data minimisation and the various issues around collection. These meetings almost always involved Service Victoria as well, because obviously they were the ones coordinating a lot of this. And then the discussion would go from there. So I do not know that I would characterise it as tension. I would say that obviously the government agencies are aware of the requirements of the Act, so it is not like they are trying to resist what the Act says. That is not really a possibility. It was more 'Can we do this? If we do this this way, is that the right way?'. We will not say whether it is right or wrong, we will say whether it is a better approach or a worse approach. Ultimately members of the public have the right to make a complaint, but I would characterise it as a very open set of discussions open to solutions rather than there being a tension about 'We must have this by tomorrow and we're going to do it, and please don't stop us'. It was not done like that.

Mr J BULL: Thank you very much for clarifying that. That is good to hear. Considering the check-in process for individuals within communities that attend restaurants, cafes and local businesses, can you take us through what obligations businesses have to follow when collecting data if they were not using the Service Victoria app?

Ms DIXON: That is outside of our jurisdiction. As I said before, a private business is not regulated by us. We have absolutely no power to deal with any complaint against a private sector organisation unless they are operating under a state contract, which in this case was overwhelmingly not true. They were bound by the orders of the Chief Health Officer in the previous round and obviously now under the minister's direction, but again, because this is for the purposes of the health information it would be an OAIC matter. We did also throughout the pandemic—and in fact all of the privacy regulators in Australia did—have regular meetings. These meetings continue to go on even though there is a little less to discuss now than there might have been. But we had very frequent meetings with both the federal regulator and all the other states too to try and work out whether or not there were issues of common concern.

Mr J BULL: Were there issues of common concern across other states and other territories?

Ms DIXON: If I can characterise the state of privacy legislation in Australia, I would not start from here, but the fact that the federal Act has gaps is possibly an unfortunate thing that, if you were designing it from scratch, you might design differently. But it is a matter for the federal government. It is completely outside of our control, and it would be inappropriate to say, 'Well, the federal government must do X'. That is a matter for the federal regulator and the federal government.

The CHAIR: Thank you, Mr Bull. I will go now to Ms Crozier.

Ms CROZIER: Thank you very much, Chair. Thank you all for being with us this afternoon. Could I just follow on from the Chair's questions and remarks made around the security breaches. I think—correct me if I am wrong—you said Service Victoria, Chair. I am just wondering whether you had any complaints from the Department of Health around any security breaches or cyber attacks that may have occurred that you were notified about. Are you aware of anything that came from the Department of Health regarding data breaches?

Mr BLUEMMEL: Not in this context. I am not aware of any in this context, no.

Ms CROZIER: And I ask that because obviously in recent years there have been a series of breaches in the Department of Health, so that is why I do ask that. That is good to know. Obviously you have been playing a leading role in terms of information security for departments and agencies. Have all the departments and agencies complied to provide you information when requested, or have there been any breaches or any information that has not come through in a timely manner?

Mr BLUEMMEL: I will probably characterise it in two different contexts. The first context is when the Victorian protective data security framework was first legislated in 2017. One of the main requirements from that is that all agencies—all state and, to some slightly complicated extent, local government agencies—to the extent that they are bound by this part of the *Privacy and Data Protection Act*, which is almost all state

government agencies and some local government agencies in certain contexts, have to provide our office with a protective data security plan together with an attestation from the agency that the plan accurately reflects the agency's posture, work and work program. That is sort of more the proactive side of things. As a result of a change to the protective data security framework and the standards that sit beneath it, for the last two years those agencies that are covered have to inform our office of incidents, which includes data breaches. The reason I separate those two out is that is clearly more reactive than the proactive part. It is also immensely useful, because it gives us the intelligence about where the risks are, how the risks are changing, geopolitically of course—especially at the moment the risks are rapidly changing—but it also allows us to work with the agencies that might need a bit more help to understand what their obligations are and how they could discharge them. We cannot do the work for them of course.

The latter part, the incident response, or the incident notification scheme, is still relatively young, so I think we still have a fair bit of work to do to make sure that agencies are aware of their obligations and are in the habit of responding to us. We publish every six months a report of insights into what we can glean from those responses to help the sector with intelligence: what is going on, what things are changing, where are the risks, where are the same mistakes being made over again and so on. I think it is safe to say that we are pretty pleased with the scheme at the moment, but there is always room for improvement.

We certainly have not had I think it is safe to say, but please correct me if I am wrong, any sort of effective hostility to it or a considered reluctance to provide us with the information, certainly in terms of the proactive part of protective data security plans. Under the incident response it is a bit hard to say at the moment whether there are agencies out there who are just not sufficiently aware that they have to report those incidents to us. There is a lot of work for us to do in education there, and our information security team in this space, compared to the size of the sector, is very small, so they have a very large workload.

Ms DIXON: I would just put a caveat on that again that obviously health services are exempt from part 4 of the PDP Act. If a hospital, for example, suffers a breach, our office has no role. The Department of Premier and Cabinet maintain a cyber incident response service, and they would respond in a situation like that if they were notified by the hospital.

Ms CROZIER: Yes. I am aware of that, and I am aware of a number of incidents that have happened in hospitals. It is probably off the back of the QR coding, and I think people understandably were quite wary about where their information was going, how it was stored. We were trying to get that from Service Victoria this morning, and you mentioned that you had meetings with Service Victoria and the department around discussing these very issues. How many meetings did you have with Service Victoria and the department? You might need to take that on notice. Was it a regular—

Ms DIXON: No, I have a list.

Ms CROZIER: You are very well prepared.

Ms DIXON: The ones that were jointly with Service Victoria and the Department of Health would be only six formal meetings that involved both, but then, as I say, we have no role in the health information. This would purely be the personal information that is being collected, which is a different matter. All of the QR positivity things and things like that, while we would talk to Service Victoria about that—and obviously we do—we obviously cannot have any regulatory role.

Ms CROZIER: Thank you for that clarification. I would have thought that those discussions would have been happening at that level because of the sensitivity of the data being collected and the design that they were involved with, with the government, to get this sensitive material from Victorian citizens. Thank you for that clarification. That makes more sense to me now than perhaps before.

Could I ask: you also mentioned the work that you did with the health complaints commissioner, and through this my office has been getting many, many complaints and concerns from Victorian citizens about what has happened—their rights that have not been able to be fulfilled. I am just wondering in terms of that working relationship—and you might not be able to answer this; they are not here to answer what I am asking, but you did mention working closely with them—how close is that, and in what capacity would you be working with the health complaints commissioner about potential breaches of patient information during this time?

Mr BLUEMMEL: In most cases, if the matter is limited to a breach of health information, then that would really be almost entirely a matter for the health complaints commissioner; we would not have any sort of real role to play. Where we have that relationship with the commissioner and her office more directly is in terms of being able to coordinate approaches should they become necessary or should there be improvements to the law that might be able to be recommended. So, for example, in Victoria we have the scenario where we have the *Health Records Act* and the *Privacy and Data Protection Act* administered by different regulators. That is a fairly unusual situation in Australia. One of the changes, for example, to the *Public Health and Wellbeing Act* is that my office can now issue what we term a flexibility mechanism, which is a pandemic information directive which allows information to be shared in a pandemic context—both health and non-health personal information—where there is some strong justification for that. Now, my office—

Ms CROZIER: Has that happened?

Mr BLUEMMEL: No, it has not. The mechanism is relatively new and it is pleasing to say so far it has not been necessary. There are other flexibility mechanisms that were already in the *Privacy and Data Protection Act* where either Ms Dixon or I can issue a determination that says that in this particular case collecting, using or disclosing the information in a way that would not normally comply with the information privacy principles, the benefit of that outweighs the harm to privacy effectively of non-compliance. They are incredibly rare. We do that very rarely, but the pandemic has highlighted that there may be situations where that is required in a health context. The problem was that the health complaints commissioner does not have an equivalent power, and in any event a determination like that would need to cover in most cases both health and non-health information.

Ms CROZIER: So that should be rectified, then? The health complaints—

Mr BLUEMMEL: That part has been rectified. As a result of that I can now, under the *Public Health and Wellbeing Act*, make such a determination that covers health and non-health personal information. There is a carefully prescribed process to make sure that in doing so I consult with the health complaints commissioner, and the health complaints commissioner can respond in writing and so on. That change was one that resulted from the discussions that we had. Of course it was a matter for Parliament to pass the legislation, but it was, I think, assisted by the discussions that we had with the health complaints commissioner. So that mechanism is now in place. We have not had to use it. Hopefully it will be an extremely rare occurrence.

Ms CROZIER: Am I out of time, Chair?

The CHAIR: You are, yes. I was listening with great interest.

Ms CROZIER: Thank you.

The CHAIR: Right. We will go to Ms Ward.

Ms WARD: Thank you, and thanks for being here and thanks for all of your work throughout this pandemic. There have been some really interesting discussions you never thought that you would have, so thank you, and thank you for your diligence. Just following through with some of the conversations that we have already had, with the privacy framework that you are talking about, such as the data collection Act and the advice that you give or the suggestions that you have been giving as to whether it is a better approach or a worse approach, do your conversations or suggestions come solely from the various acts or do you consider the health needs advice as well before you offer your suggestions? There is that tension that we have seen throughout this pandemic of individual privacy versus community rights, so how do you manage or how do you strive to get that balance right? Because it is difficult.

Mr BLUEMMEL: It certainly is difficult, and we have to bear in mind that none of us are appointed by the Governor to give public health advice. We are not the experts in that space. But of course I think as a mature regulator we realise that our role does not exist in a vacuum. So clearly while we are never going to give public health advice to anyone, including the Department of Health—

Ms WARD: But you recognise that health need exists.

Mr BLUEMMEL: Precisely. What we will do in a case like that often is where there is expressed by the appropriate authorities or experts a public health measure that is proposed, where we can I think have the most impact is by helping to steer them in a direction where that outcome can be achieved in a way that either has as little as possible or ideally no negative impact on privacy. Some fairly straightforward examples are like the Service Victoria data collection. It is passed from Service Victoria to the Department of Health, and it is deleted after a fairly short period of time in Service Victoria. That is good from a privacy perspective, and that does not in any way weaken the efficacy of the public health outcome from contact tracing, vaccination certificates or anything else. Had that been designed differently so that these datasets exist in many different locations and are duplicated, then the privacy and security risk increases with no net increase in the public health outcomes. So it is things like that where we can be cognisant of the public health outcomes—very much so—but also provide the expertise that we can, to say, 'Here's how you can do it in a better way'.

Ms WARD: So you were part of that conversation around the 28-day data dump, that cycle?

Mr BLUEMMEL: Yes, we were. And also in discussions about the legislative restrictions on the use of contact-tracing data. That was a very important one to us. In fact in a case like that while on the surface it might look like there is tension between respect for privacy and public health efficacy, in the end I think on some closer analysis respecting privacy will often get you better outcomes in efficacy for public health, because people will be more likely to trust the system, the collection and the systems behind it and will therefore be more likely to engage with it in a constructive manner, rather than be more likely to try to put in fake data or not check in, because if you do not trust the system, you are more likely to do those things.

Ms WARD: Yes. Sure. So with what you are saying today, though, it does seem like a very robust approach across the agencies to preserve people's privacy as much as possible.

Mr BLUEMMEL: Broadly speaking, yes. It is an ongoing effort for us, as you can imagine. For example, and this is a hypothetical, if government had decided instead to collect this information and keep it as personally identifiable information from here on in because it might be useful, we would have some grave concerns about that. Our view is always to minimise collection, use and disclosure, and as the pandemic evolves, as it has, information that may have been necessary 12 months ago is no longer proportionate to collect, so we would always encourage agencies constantly to keep asking those questions and be diligent.

Ms WARD: Thank you. One of the key outcomes that came from the Finkel review was the need to enhance data-sharing arrangements between jurisdictions. What advice did you have in relation to data sharing between jurisdictions particularly around the pandemic?

Ms DIXON: Around the actual health information?

Ms WARD: Yes.

Ms DIXON: Apart from the discussions, as I mentioned before, with the various national and state privacy regulators, very little because those discussions were going on between health departments—that was a matter for those jurisdictions. But we did discuss it obviously many times at the various regulatory meetings that we have, and as I say they were quite frequent during COVID. We had a standing COVID-19 data discussion going on there. So, yes, it was considered. We did not communicate that as a group back to those, but obviously the OAIC with the federal remit had a good coordinating role in helping to disseminate some of that information back.

Ms WARD: Thank you. Have I still got time, Suzanna?

The CHAIR: Yes, you do.

Ms WARD: Great. Thank you. Can you also elaborate a bit more, expand a bit, on the interaction between COVID-19 obligations and our privacy legislation? You have alluded to some of the acts. Can we tease that out a little bit more?

Mr BLUEMMEL: Sure. Broadly speaking, the information privacy principles—10 principles in the *Privacy and Data Protection Act*—are principles with which agencies have to comply when collecting, using and disclosing personal information. That fundamental aspect has not changed, so basically everything that

agencies do has to comply with those principles. Now, those principles do of course interact with other laws. For example, an agency is only allowed to collect personal information to the extent it is necessary for one or more of its functions. It is only allowed to use and disclose it for the primary purpose of collection, in certain circumstances for a secondary purpose, subject to certain protections, but importantly also where the use and disclosure is authorised by or under law. Therefore if you have either primary legislation, like the *Public Health and Wellbeing Act*, or orders made under such legislation that expressly authorise the collection, use or disclosure of personal information, then that effectively makes that compliant with the relevant privacy principle. That is broadly how they interact.

What we then do is we are usually consulted where an agency or a minister puts up a proposal for legislation that would have such an effect. There is no obligation to do so, but generally it is done, which is pleasing, and we try to remind agencies that that is a good thing. In addition to that legislative framework that might now have been amended by other legislation, there are still good and bad practices within that scheme—like I said, the duplication and so on. So that notwithstanding, we then work with agencies to say, 'Yes, this is now authorised by or under the law; however, there are ways to do it well in a privacy-respectful manner and there are ways to do it poorly. Please let us help you do it well'.

The CHAIR: Thank you. I will go now to Ms Kealy.

Ms KEALY: Thank you very much for your time today. Ms Dixon, can I go back to I believe it was one of the comments you made earlier in your opening comments around having 12 meetings with the department. Sometimes these were multi-agency meetings, and some of that feedback was around whether they were meeting the requirements of the Act. Were there any instances during those meetings that were flagged with you which would indicate that those departments were not acting in compliance with the Act?

Ms DIXON: No. If there were, I would have said so.

Ms KEALY: Okay. We have to be sure to be sure in this setting.

Ms DIXON: Bear in mind that I was present at most of those meetings but not quite all of them, so my assistant commissioner of policy would have been involved or my head of assurance would have been involved, but if I was not there I was briefed after the meeting. I would have of course also talked to Sven about it, and we would have worked out an alternate strategy for leveraging anything that had happened. But we did not have any cause and there was no circumstance in which people were trying to do the wrong thing. I have to say one of the credits I think to the Victorian community in the pandemic was that people were very focused on trying to do the right thing. Nobody wanted to just do the quick thing. It was all, 'How can we do the thing that will last and will not destroy the public trust', to Sven's point. Nobody would push back and say, 'Well, we have to do it anyway'. They would not do that.

Ms KEALY: Thank you. This is quite a specific question. I will ask whether the commission has been asked by the government, and perhaps it is then a question from me if you have not been asked by the government. We have had numerous opportunities to ask the government, 'Who are the people who have been appointed to the independent medical exemption review panel?'. This was appointed by the Department of Health. Would there be any reason that you can see that that information would be withheld—the people that have been appointed to that committee?

Mr BLUEMMEL: Look, it is not something that we have looked at, frankly, so it would be a bit difficult for us to express an opinion on that specific one at the moment.

Ms KEALY: I realise I am putting you in a position. I am happy to take it on notice. We are giving questions on notice if that is of assistance.

Mr BLUEMMEL: Sure. It may even be difficult to take on notice if the matter has not come before us—for example, as an FOI review. Ms Kummrow and I together administer the *Freedom of Information Act*, so we are in a position to independently review agency FOI decisions, for example, but if it has not come to us in that regard then I think it is probably inappropriate for us to speculate. It is not a current matter that we are dealing with, as far as I am aware, but I will check with Ms Kummrow. Are you aware of anything in that regard?

Ms KUMMROW: I am not aware of a matter coming on review, or a complaint for that matter, under the FOI Act.

Mr BLUEMMEL: We can check whether there is anything sort of specific that my office has had to make an FOI review decision on. Because we make a substantial number of FOI review decisions every year—the most in Australia. So—

Ms KEALY: I think most of them come from Georgie.

Mr BLUEMMEL: I assure you they do not. But what I think I can say meaningfully—and not talking about the specifics, but it may be relevant to your question—is that in our FOI jurisdiction both Deputy Commissioner Kummrow and I take a very pro-disclosure view when it comes to decisions of government, particularly senior levels in government as opposed to more junior levels. There is no hard and fast rule as to where that line is drawn. It depends very much on the circumstances, but our view that we always use as guidance is that the FOI Act is intended to be a pro-disclosure act. It contains exemptions, but where in doubt, where there is a genuine case to be made both for and against the exemption and the case is finely balanced, we would always err on the side of disclosure, because that is clearly Parliament's intention from the Act. So that is probably as far as I can go without knowing the specific matter and the specific matter being before us.

Ms KEALY: In relation to the orders and how they impact on particularly government employees' requirement to work from home, it has taken a level of known risk away in that people are working from home. We know that they are working on a VPN system or alternative remote system. That information may be more widely available if they share their home with other residents, which may or may not be family. What advice have you provided to the government in relation to working from home, specifically around orders and how that may impact the number of people who are working from home and your comments earlier that any time that there is a risk it should be minimised and utilised for as short a period as possible?

Ms DIXON: When the pandemic first began, our office I think put quite a considerable amount of effort into trying to reach out to government agencies. We run a series of regular information security sessions. Obviously our newsletter goes out to a lot of people. We developed some specific guidance, both on the how to minimise privacy issues but also particularly around the information security, because we are conscious that, as you say, a lot of the controls that would exist in a workplace may not exist. So we produced some animated kind of guides to people that they could get some quick ready reference from. There is some material on our website that I believe is still there, so you can access that. And then, again, we regularly reinforced with the information security leads in various departments through our information security community that, you know, they needed to brief their workers on the kinds of risks around things like, for example, if you have got somebody else in the room who can hear the discussion, then you probably should be using headphones—those sorts of tips.

But obviously our role in that situation is mostly to issue guidance. If there was a complaint or a breach around those things, then we would have action to take after that. We have not actually seen terribly many of those. We are aware of some, which I would not like to talk about in great detail because one of them is still under investigation. There were a couple of breaches, more on the contract service provider side of things than the public service per se. And I think part of that reflects the fact that, you know, those contract service providers were unfamiliar with some of those things because they had not had to deal with them before. So all our office can do is to issue the guidance and say, 'Here's how you should do it'.

Ms KEALY: To minimise the risk, but you cannot guarantee there are no breaches, can you?

Ms DIXON: There is no such thing as perfect security. You can only try better.

Ms KEALY: Yes. Just referring to the *Incident Insights Report* from 1 July to 31 December last year, I note that there were 161 notifications regarding the department of justice. Is there a key trend in relation to that? And is there an underlying understanding that may be because of the remote court that was put in place over the COVID pandemic and restrictions?

Mr BLUEMMEL: I think most of that would be reflected by the fact that the department deals with large numbers of prisoners. I would think that with mail to and fro in prisons, all of those sorts of things, there is lots of scope for a breach to occur. But in addition to that, Ms Dixon might have something further.

Ms DIXON: I would caution you. We had a briefing actually this morning. We had an information security network meeting, which was well attended. We usually get about 150 or so attendees, which for a virtual meeting is—

Ms KEALY: Significant.

Ms DIXON: pretty good. One of the things of course we present is the incident notifications, and we look for trends. But as we have consistently said—bearing in mind this standard, which is standard 9 of the VPDSS, was only introduced two years ago and there has been a ramp-up period as awareness has increased—it is very hard to look at this year on year and say that things are getting better or worse yet. Some of it may be that people are just becoming more aware of their reporting obligations and therefore are reporting more to us than they were, and also there is occasionally a small delay. So if you look month on month, for example, it is impossible, because in fact the thing that you are looking at might have actually occurred a little while ago or it might have occurred yesterday. We did issue that caution at this morning's meeting: 'Here are the latest stats', but if you are looking at that in comparison to last year, it is very hard to work out whether that is because there have been more breaches because more bad stuff is happening or because more people are reporting to us.

Ms KEALY: In that briefing you issued this morning have you identified any trends at this point in time that could be specifically related to the pandemic?

Ms DIXON: The overwhelming issue with information security is human error. It is the overwhelming, number one cause of breaches. People send the wrong email to the wrong person; Microsoft Outlook autocomplete is the bane of my existence. That is, I think, overwhelmingly we would have to say the number one cause of breaches. Then there is human error in terms of somebody actually just left something on the train, which does not happen that often, but it happens often enough. But human beings are fallible. We just again have to try and train people to say, 'If you're carrying material home, here's how you should secure it. Please don't use an unencrypted USB key. Please don't'. And these are exactly the kinds of messages that our information security, which is only six people for thousands of Victorian government bodies—

Ms KEALY: That sounds like a pitch to the budget to me.

Ms DIXON: I shall leave that alone.

Ms KEALY: Thank you very much.

The CHAIR: Thank you. Just a couple more questions. With Service Victoria having a policy of deleting that information that they collect within 28 days, does the Department of Health have a similar policy or do you advise them in relation to how long they should keep those sorts of records?

Mr BLUEMMEL: I think the 28 days specifically does not apply to the Department of Health. And in terms of how long it should be kept for, again it would be difficult, if not impossible, for us to advise the department on how long it does need to be kept, because it does relate to the department's health functions. What we do, however, of course is to constantly reinforce that issue of 'Keep as little as possible for as short a period of time as possible'. It is often said that the data is an asset and is valuable—and yes, it can be—but it is also a liability. Certainly in the public sector once you hold information, you are responsible for privacy and for security, and you have to do that well. So therefore keeping something when you have no good reason to keep it is not only a breach of the Act but is actually exposing you to greater risk.

The CHAIR: So your advice is to keep the overall statistics but get rid of the identifying information generally.

Mr BLUEMMEL: Broadly speaking, yes. There are some caveats there because even things that look like aggregated or de-identified data can often be re-identified with appropriate techniques or, dare I say, inappropriate techniques, depending on one's motivation. A couple of years ago we issued an investigation report into the re-identification of a large public transport dataset, for example. That was all published and tabled in Parliament. What that investigation really showed was that even with the best of intentions and an attempt to de-identify a large complex dataset for future aggregate planning purposes you have to be careful, because almost certainly something that has been de-identified can often be re-identified. The difference is to truly statistical information that was never identified in the first place, where you have this many number of

cases in this area, for example. As long as the area itself is not too small, that would fit into the category of not being personal information and therefore the privacy Act would not apply to it, or at least the information privacy principles would not apply to it.

The CHAIR: So with Service Victoria deleting at 28 days, I mean, is that backed up somewhere else, that information? Is it truly, absolutely deleted or is it in a cloud somewhere?

Ms DIXON: Service Victoria have consulted us quite extensively on their RDA, which is the policy that governs the retention and destruction of data. I believe at certain times they might have had some concerns that this was not being dealt with properly. They certainly took pains to address it immediately. So I have no concerns about that. At a certain point we might have gotten sick of hearing about their RDA! They are very, very responsive to the issues around whether or not information is truly retained in their platform. Because they run a multi-tenanted platform, that can be a tricky thing because it is a question of which bit of which agency. There are encrypted backups that are kept for the purposes of restoring data, but of course after 28 days that is not necessary anymore. They do not need to restore that old data. So, no, they have been extremely attentive to that particular issue.

The CHAIR: Yes. Okay. So perhaps just a more philosophical question: in the course of the early days of the pandemic, newspapers like the *New York Times* would publish page after page of people who had died from COVID-19 before there was any vaccine being widely taken out—so an incredible not taking notice of perhaps individuals' privacy, because it is hard to see that they could have consented in any way to that occurring. Here we have not done that sort of thing unless someone has gone to a newspaper or wanted to tell their story. Is there a vast difference between jurisdictions, in a sense, as to what might be considered private and what is not? Because we similarly have lost thousands of people, and every week we are losing hundreds in Australia from COVID, even with a highly vaccinated community, but we have no sense of who they are or whether they are vaccinated or unvaccinated. So some of this information now seems to be more unavailable, and I just wonder whether that is part of a role that you might take in terms of what information should be made available and what is not.

Mr BLUEMMEL: In short, that is not something we would get into unless of course we saw something that was being done by an agency we regulate that was inconsistent with the information privacy principles. But on your broader philosophical question of the variation between jurisdictions, there is substantial variation across the world, certainly—well, even in Australia. Both Western Australia and South Australia do not have state privacy legislation. They have other mechanisms to try and safeguard personal information, but it is not legislation. Internationally there are quite big differences. Europe has stronger privacy legislation than the average. The US is often considered to be fairly low in privacy regulation, but I do not think that is actually even true anymore because it is just more fragmented over there. Some states have strong privacy laws. There are even federal privacy laws for some sectors—for example, to do with children or, I think, the health sector as well. So it is a global patchwork, and that actually causes all sorts of friction with certain international trade because many privacy laws, including our own, provide that you cannot ship personal information outside the jurisdiction, including electronically, unless it is subject to certain safeguards. One of those safeguards is that the receiving jurisdiction has privacy laws as strong as yours. That in itself is often a very difficult question to answer. So, yes, it is a patchwork and it is a bit of a drag on trade. But broadly speaking, of course, our role is to administer the Act we are given.

The CHAIR: Thank you. Another question?

Ms CROZIER: Yes. Could I just get some clarification from Ms Dixon firstly on the RDA—the retention and destruction. You said Service Victoria are very keen to have that information destroyed after 28 days. They said that it was then stored in the department. Does that automatically mean that that information stored in the department is destroyed at the same time?

Ms DIXON: I could not answer that. That would be a matter for looking at Service Victoria's API and the practices of that individual department. So, as I say, the problem for Service Victoria there is that they are a multitenanted service. They have many agencies that are onboarded to them, and so each of those agencies are responsible. To Sven's earlier point, bear in mind that the department may have a legal reason for being able to retain that data because it is necessary for one or more of their purposes. So you could see how, for example—and I will talk in the abstract here, not about COVID data but about other data—if you were looking at fishing

licence data, while Service Victoria may not retain the transactions around individuals applying for fishing licences, the agency that issues fishing licences is going to want to have some retention of that for the probity of fishing regulation, and that is a permitted purpose under their legislation. I think it is very important to distinguish between what the *Service Victoria Act* allows Service Victoria to do versus what the various acts that relate to each of those bodies allow, and you really have to then refer to: well, which body and which act, and what is the permitted purpose, and how is that data being treated for that purpose? It is utterly contextual, and obviously Parliament passes new legislation all the time or new regulations to allow agencies to do all sorts of things, so there is no global map in Victoria of what every agency must do. I do not think anybody has the resources to do that.

Ms CROZIER: No. Thank you for that clarification again. So to a follow-up question then—you possibly will not know the answer to this: are you aware of the number of organisations that have requested access to this data that the department has that has come through the Service Vic app? For instance, the police—

Ms DIXON: Once it is in the department, no, we would not. Unless there was a complaint made we would not have an awareness of all the various uses, because again—I will just take a random kind of example—there may be, for example, a law enforcement provision that says that the law enforcement agencies can get access to fishing data. That would be either in the fishing regulations or legislation, or it may actually be in Victoria Police's enabling legislation, depending on how things work. So, again, it is completely contextual, and I would need a specific example of a specific agency retaining data and then sharing it to offer any kind of view. But even then, we may not have been consulted in that, because if it is within their Act it is not a breach of the IPPs.

Ms CROZIER: Thank you.

The CHAIR: Thanks. I will just go to Josh, to be fair across the spectrum, on a further question. We just have got a few minutes left now.

Mr J BULL: I will keep it brief. Thank you, Chair. I was just reflecting, Deputy Commissioner, on sharing the same surname as another member of Parliament and often receiving his emails, and he receives mine—Tim. Your point was very well made. Look, I think it is fair to say there is a sliding scale of community views about data sharing of information—information that is provided to government and its agencies. Some in the community will be keen to share quite a lot, others will share very little. I just wanted to ask broadly: what do you think undermines people's faith and trust in data collection and sharing, and how do messages from certain groups or individuals within the community change that, do you think?

Mr BLUEMMEL: I am happy to start off, but for us the importance of trust, as I said in my opening statement, is I think so crucial to our democracy. In terms of privacy, what I would say is that, yes, there is the legislative requirement to comply with the information privacy principles, and that is very necessary. In addition to that I think what has a really positive impact is when there is clarity and respect. By that I mean that a person who obtains a government service or interacts with a public authority can be really clear about what is going on—'What will happen to my information? Why do you need it? How are you going to protect it?'. Now, not everyone on every occasion will want to delve into the full detail of that, but they should be able to if they wish, and it should be expressed clearly without jargon. Anybody should be able to comprehend that and be genuinely informed about why this is being done and what is going to happen to it.

The second part of that, which I think is highly complementary but seems quite different, is the importance of transparency, and this is where the jurisdiction that Deputy Commissioner Kummrow and I exercise comes into it. Being transparent about not just what is happening proactively but being transparent when there is a request; being transparent about, dare I say, modelling of the pandemic going forward; being transparent with all of that, especially when it is not always good news—I think that builds trust. And of course in our FOI jurisdiction, where I see an agency do something where we really think, 'Yes, this is a mature, positive thing to do' is when an agency releases information that is a bit inconvenient, a bit embarrassing, a bit politically sensitive. When that happens and the agency says, 'Well, yes, we'd rather not, but we've gotta do it and it's the right thing to do for our democracy', then that is where I see trust being built. I want that to happen a lot more. It is really, really important. So when you combine those two, the transparency, both proactively and on request, with the respect for individuals, for their intellect, for their ability to be free, self-determining individuals—you put those two together, you build trust. You do the opposite, you erode trust.

Mr J BULL: Absolutely. It empowers the community as well, which is [Zoom dropout]. Thanks, Chair.

The CHAIR: I think on that note you could have one quick one, and then time is up.

Ms CROZIER: Okay, thank you. I was very interested in that last statement from the commissioner. I totally concur with what you said about transparency and respect and building up trust in our democracy, so thank you for those comments. I wanted to just go back to an earlier comment that you made. You said earlier that risks are rapidly changing, especially geopolitical risks. What is the latest on those threats for Victoria, do you believe?

Mr BLUEMMEL: The threat has always been there. There have always been state actors and their proxies who attack all over the world, including in Victoria. They may not target Victoria as a state—

Ms CROZIER: We have had incidents of that in recent years.

Mr BLUEMMEL: Yes, and it is certainly not just one or two countries either. So it has always been there. It is certainly not a new thing, but what can happen with the geopolitical environment at the moment—of course what we are seeing in Europe—simply means that that situation is even more dynamic. It may not even be a risk that has increased because of some sort of central directive from the highest levels of a foreign government. It may simply be people who are sympathetic to that foreign government, wherever they may be in the world, using cyber attacks to sow doubt, misinformation, disinformation, all of those sorts of things. They are just heightened in times of this sort of tension. But we have been in sort of heightened tension in that regard for quite a while, so the message that we really send to the Victorian public sector is that there is unfortunately never a time to relax about these sorts of things.

The CHAIR: And they are probably getting worse all the time.

Mr BLUEMMEL: They are probably getting worse. They are getting more sophisticated. Of course these days, with connectivity, you can massively leverage yourself as a bad actor and with relatively little effort launch attacks in very broad geographical and virtual spaces. That is just the environment we live in. I cannot see it ever becoming simpler.

The CHAIR: I would like to thank all three of you for attending today. It has certainly been interesting hearing about your role as regulators in the space of information and about your relationship with government. It has been very informative for us. You will receive a copy of the transcript of the hearing within the next week for review, including any questions that may have been put on notice—if there were any; I am not so sure. But thank you again very much for attending today.

Witnesses withdrew.