



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND
SECURITY

Review of the mandatory data retention regime

FRIDAY, 28 FEBRUARY 2020

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

To search the parliamentary database, go to:

<http://parlinfo.aph.gov.au>

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Friday, 28 February 2020

Members in attendance: Senators Fawcett, Keneally, McAllister and Mr Byrne, Mr Hastie, Mr Leaser, Mr Tim Wilson.

Terms of Reference for the Inquiry:

To inquire into and report on:

Section 187N of the Telecommunications (Interception and Access) Act 1979 provides for the review and requires the Committee to report by 13 April 2020.

The Committee has resolved to focus on the following aspects of the legislation:

- the continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill;
- the appropriateness of the dataset and retention period;
- costs, including ongoing costs borne by service providers for compliance with the regime;
- any potential improvements to oversight, including in relation to journalist information warrants;
- any regulations and determinations made under the regime;
- the number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security;
- security requirements in relation to data stored under the regime, including in relation to data stored offshore;
- any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the Telecommunications Act 1997; and
- developments in international jurisdictions since the passage of the Bill.

WITNESSES

BURGESS, Mr Mike, Director-General, Australian Security Intelligence Organisation	24
CARLESS, Mr Maurice, Assistant Commissioner, Intelligence and Covert Services Command, Queensland Police Service	32
FITZGERALD, Mr Michael, Commander, Forensic Evidence and Technical Services Command, New South Wales Police Force	32
HANSFORD, Mr Hamish, First Assistant Secretary, National Security and Law Enforcement Policy Division, Department of Home Affairs	1
KATHAGE, Mr Tristan, Assistant Secretary, Telecommunications Market Policy Branch, Department of Infrastructure, Transport, Regional Development and Communications.....	1
KENT, Mr Karl, Deputy Commissioner, Specialist and Support Operations, Australian Federal Police	44
KERSHAW, Mr Reece, Commissioner, Australian Federal Police	44
McNEILL, Ms Jennifer, First Assistant Secretary, Communications and Infrastructure Division, Department of Infrastructure, Transport, Regional Development and Communications.....	1
PHELAN, Mr Michael, Chief Executive Officer, Australian Criminal Intelligence Commission	32
VICKERY, Mr Peter, Deputy Director-General, Enterprise Service Delivery, Australian Security Intelligence Organisation	24
WARNES, Mr Andrew, Assistant Secretary, National Security Policy Branch, Department of Home Affairs	1

HANSFORD, Mr Hamish, First Assistant Secretary, National Security and Law Enforcement Policy Division, Department of Home Affairs

KATHAGE, Mr Tristan, Assistant Secretary, Telecommunications Market Policy Branch, Department of Infrastructure, Transport, Regional Development and Communications

McNEILL, Ms Jennifer, First Assistant Secretary, Communications and Infrastructure Division, Department of Infrastructure, Transport, Regional Development and Communications

WARNES, Mr Andrew, Assistant Secretary, National Security Policy Branch, Department of Home Affairs

Committee met at 08:33

CHAIR (Mr Hastie): I declare open this public hearing of the Parliamentary Joint Committee on Intelligence and Security for its review of the mandatory data retention regime. These are public proceedings, although the committee may agree to a request to have evidence heard in camera or may determine that certain evidence should be heard in camera. I remind all witnesses that, in giving evidence to the committee, they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated as a contempt. It is also a contempt to give false or misleading evidence to a committee. In accordance with the committee's resolutions of 4 July 2019 this hearing will be broadcast on the parliament's website, and the proof and official transcripts of proceedings will be published on the parliament's website.

I welcome representatives from the Department of Home Affairs and associated agencies to give evidence. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of parliament and therefore has the same standing as proceedings of the respective houses. Giving false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence today will be recorded by Hansard and attracts parliamentary privilege. Do you have an opening statement?

Mr Hansford: Thank you for the opportunity to make some introductory framing remarks. The corpus of evidence provided to the committee outlined in submissions and public hearings to this review from Home Affairs, Commonwealth agencies, state law enforcement, anticorruption agencies and, indeed, the Uniting Church, documents the criticality of telecommunications data. Put bluntly, the use of telecommunications data by agencies protects Australians. The use of telecommunications data is integral to gathering information to investigate threats to Australia's security, including terrorism, espionage and foreign interference, cybercrime, illicit drugs, illicit firearms, child exploitation, corruption by officials, and serious criminal investigations such as murder, rape, sexual assault and kidnapping.

In 2015 the criticality of the investigative tool was recognised by this committee and then the parliament with the passage of legislation to require communications providers to retain a prescribed set of communications data for two years.

The mandatory data retention regime did not give agencies new powers. Agencies have had the ability to access telecommunications data under Commonwealth legislation since at least 1975. Instead, the obligations in the regime have provided certainty that certain telecommunications data is protected and available for a minimum of two years. Submissions and the public hearings that this committee has had to date also reiterate the intended operation of safeguards and oversight arrangements, which are designed to protect the privacy of innocent Australians and press freedoms and to ensure that telecommunications data is accessed and used appropriately. These protections include requiring retained data to be encrypted and protected from unlawful intrusion; clarifying that the Australian Privacy Principles apply to retained data; requiring agencies to obtain a journalist information warrant when seeking to identify a journalist source; and empowering the Commonwealth Ombudsman and IGIS for ASIO to comprehensively oversee how agencies access and use telecommunications data.

Some have expressed reservations about the two-year data retention period. Their argument has been that the majority of data is accessed within the first three months or the first year. Let me provide some context to counter this argument with some new information that has been tabled in the Australian parliament from the annual report of the Telecommunications (Interception and Access) Act in the 2018-19 report. That says that 85.5 per cent in 2018-19 had data retained for zero to three months before authorised disclosure. However, authorisations for point-in-time information, without a so-called identifiable age, include subscriber information and information that is currently held in the integrated public number database. This is an industry-wide database managed by Telstra containing all listed and unlisted public telephone numbers—a comprehensive White Pages, if you will.

Access to this data is often recorded as zero-date data. So while it is true to say that the majority of telecommunications data is accessed in the zero to three-month range, it's also true that the majority of this data is likely to be subscriber checks. This is backed up by the fact that 73.7 per cent of data retention requested information, including IPND checks, in 2018-19 were for subscriber data as opposed to traffic data. This confirms the evidence provided to this committee from agencies that basic subscriber checks are those basic checks that are undertaken at the start of an investigation and predominate in the data retention regime.

Requests for older data are likely to seek more traffic data and disproportionately relate to investigations into more serious and complex criminal activity and matters of national security. Our supplementary submission to this committee identifies a number of case studies that go to the practical difference that telecommunications data retained for up to two years has made to investigations. Any reduction in the retention period, therefore, may result in agencies being confronted by situations where they are unable to obtain vital information for an investigation because the relevant telecommunications data has not been kept.

At this point I should like to make a correction to our supplementary submission at paragraph 15, page 6, where it says:

The Australian Criminal Intelligence Commission has estimated that almost 100 per cent of their investigations targeting serious and organised criminal activity requires access to telecommunications data older than 12 months.

This should read:

The Australian Criminal Intelligence Commission estimates that almost all of their investigations targeting serious criminal activity requires access to telecommunications data older than twelve months.

Certain submitters have also called for access to telecommunications data to be judicially authorised and subject to a serious offence threshold. Requiring agencies to obtain a warrant to access telecommunications data would impose a disproportionate burden on agencies and issuing authorities and would cripple timely access to data. Furthermore, it is unlikely that introducing a warrant regime would provide a level of additional protection that would outweigh the investigative bottleneck that would likely result. The thresholds and safeguards that govern access to telecommunications data under the TIA Act are already substantial and include the Inspector-General of Intelligence and Security for ASIO and Ombudsman oversight. Introducing a serious offence threshold would also impede agencies from undertaking a variety of important investigations that nonetheless do not meet the threshold of 'serious'. Furthermore, limiting access to telecommunications data to only certain criminal offences may place Australia in breach of its international legal obligations, including under the Convention on Cybercrime.

There have also been many concerns over a perceived loophole that enables access to telecommunications data outside of the TIA Act, specifically under section 280 of the Telecommunications Act 1997. My colleagues from the department next to me are here today to answer any questions that the committee may have about the intent and practical operation of that section of the Telecommunications Act.

In conclusion, almost five years after the passage of this legislation, telecommunications data remains a vital investigatory tool for Australian law enforcement, anticorruption and intelligence agencies. Retaining consistent and reliable access to this data is and will remain of critical importance to our agencies. The data retention regime remains a necessary, reasonable and proportionate response to the Australian threat environment. Thank you.

CHAIR: Thanks very much, Mr Hansford. Mr Kathage?

Mr Kathage: I would like to thank the committee for the opportunity to appear today on behalf of the Department of Infrastructure, Transport, Regional Development and Communications. Of interest to the committee, the department provides advice to government on the operation of part 13 of the Telecommunications Act, which aims to protect the disclosure and use of telecommunications information except in authorised circumstances, and part 14 of the act, which facilitates appropriate access and assistance from telecommunications companies in certain circumstances.

The department appreciates concerns from the committee and raised in some submissions on the purpose and operation of section 280 of the Telecommunications Act and its use in accessing telecommunications data. One of the points raised in some submissions is the purpose and operation of section 280. I would like to note that under no circumstances is it possible for enforcement agencies or non-enforcement agencies to rely solely upon section 280 to obtain access to telecommunications data. Section 280 is located within part 13 of the Telecommunications Act, which is primarily concerned with the protection of communications. Specifically, sections 276, 277 and 278 require carriers and carriage service providers to protect the confidentiality of communications, information related to communications and other personal information.

However, acknowledging there may be legitimate circumstances requiring the disclosure of this protected information, part 13 includes a number of exceptions to this prohibition. Section 280 specifies two mutually exclusive circumstances where it is appropriate and lawful for carriers and carriage service providers to disclose protected information they hold, despite the prohibitions against disclosure. Under section 280, telecommunications providers are not prohibited from disclosing protected information to an enforcement agency if it is required or authorised under warrant or if it is required or authorised by or under law.

It is important to note that section 280 itself does not authorise the disclosure of any protected information to enforcement agencies or non-enforcement agencies. Further, section 280 itself does not provide any legislative authority for enforcement agencies or non-enforcement agencies to compel carriers or carriage service providers to disclose any protected information, including telecommunications data. The authority to disclose telecommunications data and other protected information is provided by existing laws passed by the Commonwealth parliament or state and territory legislative bodies which set their own thresholds and safeguards. It is important to note that coercive powers to produce by these bodies exist regardless of the operation of section 280. However, section 280 provides a mechanism for assurance to carriers and carriage service providers that they are not contravening the prohibitions on disclosure outlined in sections 276, 277 and 278.

CHAIR: Thank you very much. From the top, and for the benefit of the Australian community, can you give us a sense of how 280 and 313 operate from federal agencies right down to local government? How do organisations or agencies go about accessing information?

Mr Kathage: I might choose to answer the question from the perspective of telecommunications companies. As I mentioned in the opening statement, section 276 prohibits the disclosure of information by carriers or carriage service providers. An agency can use a notice-to-produce power in combination with section 280 to request that a carrier or carriage service provider disclose protective information. Notice-to-produce powers exist in a number of forms, principally at the state level; state legislative bodies provide powers to some agencies to request information. It also exists, as you noted, in section 313(3), which allows officials of the Commonwealth, states and territories to seek assistance from carriers and carriage service providers in certain circumstances.

CHAIR: For example, protecting the public revenue?

Mr Kathage: That's correct.

CHAIR: Tribunal offences—

Mr BYRNE: Ballot forms, parking fines, council fees—

CHAIR: Yes.

Senator KENEALLY: I think we're interested to understand the range of reasons that some of these other agencies, beyond the 20 who access metadata for the serious purposes you outlined earlier, are accessing it.

Mr TIM WILSON: And, just to add to that, the attitude of the AFP to the—

Mr Kathage: Sorry, I didn't hear the last part.

Mr TIM WILSON: The attitude around the acceptability of that and whether you believe that's justifiable, considering the severity and seriousness of the matters you're trying to access metadata for, for serious crimes versus the triviality of a parking fine.

Ms McNeill: Perhaps we can start with the purposes for which assistance can be sought from carriers and carriage service providers. If we go to the terms of the legislation, the purposes are specified in section 313(3) and (4):

(c) enforcing the criminal law and laws imposing pecuniary penalties—

There is some stretch in that—

(ca) assisting the enforcement of the criminal laws in force in a foreign country—

so assisting in the investigation and prosecution of the crimes specified in those two subparagraphs, and—

(d) protecting the public revenue.

It is relevant to note that these are quite longstanding provisions and that they predated the data retention arrangements. So there's nothing new in this, and it's entirely appropriate for there to be a mechanism by which the cooperation of carriers and carriage service providers can be secured. That's the purpose of the sections.

Senator KENEALLY: Mr Wilson and I both expressed an interest—and I accept your point—in understanding, for example, why a veterinary association or the Victorian Institute of Teaching needs to access this data. Because we have instituted a scheme to set certain types of data for certain periods of time, we have essentially made it a lot easier for those types of bodies to access quite a significant set of data. So we're seeking

to understand what types of offences or what types of activities they are investigating, and, as Mr Wilson said, your view of the appropriateness of that?

Mr Warnes: Maybe I can assist. I point you to the fact that state parliaments get to pass a lot of these laws. There are underpinning powers here that enable those bodies you've mentioned, like state veterinary associations and other things—the parliament has enabled notices to produce to enable those bodies to get that information. Absent section 280 and the operation that section 280 has under Commonwealth law, those bodies wouldn't be able to access that information because they wouldn't be able to overcome the disclosure provisions in the Telecommunications Act. You can point to some that look trivial on their face and ask why the teachers association has them, but when you look behind some of those—and we've only got some anecdotal examples, because they're not in the Commonwealth—they go to really serious matters of teachers behaving inappropriately to students, for example, and being able to access the phone records of those teachers to try and make out those cases to make sure that those people can be potentially removed and that further action can be taken. Similarly, with bodies like the RSPCA, who have statutory duties around animal welfare under legislation in various states, there are some really important things. With telecommunications data, generally, low intrusive data allows you to do those initial investigations.

Senator FAWCETT: Mr Warnes, I think you started to answer what we're after. It's very easy to just say 'parking fines' and everyone goes, 'Why should we allow access to data for that?' What would be useful, if you have those kinds of examples of bad behaviour by teachers that puts students at risk, would be to give us some examples of that but also an understanding of why that's not being pursued by the state police. If there's criminal type behaviour going on—grooming or inappropriate conduct, et cetera—surely a state education authority would refer that to the police for prosecution?

Mr Warnes: They may well, but if they have administrative processes they're able to follow those processes too. The two may go hand in hand.

Mr BYRNE: Some of us have been sitting here for a while and know the history of all of this. I just want to get the facts clear. Are you arguing that these agencies should have the power to access metadata?

Mr Warnes: Those state parliaments have that process. I'm arguing that if you don't have section 280 you create an issue where state parliaments have rightfully, in their own legislative purview, legislated for access to data, and that without section 280 you won't be able to give effect to that state parliament intent. So you will have an issue there. I'm not arguing for individual councils and bodies; that's a state matter.

Mr BYRNE: You just did!

Mr Warnes: No, I am saying that state parliaments have the ability to legislate. If you remove section 280, you remove that ability for access that state parliaments have given.

Senator KENEALLY: Mr Warnes, isn't the issue—as you rightly said, Ms McNeill, some of this goes back quite some time—that that reflects a time when the types of data you could get were far more limited in their scope and the information that they revealed? Getting access to landline records is quite a different thing to getting access to metadata. That's what we're trying to understand. Because the scope of the data and the information that it reveals has shifted quite significantly, because the retention period has been made mandatory, we are seeking to understand whether or not the regulations and the privacy protections continue to be fit for purpose under section 280. I think Senator Fawcett's point, requesting some examples and asking why certain matters aren't being pursued by the police rather than by an institute of teachers, is the type of information we are seeking.

Senator FAWCETT: If I can clarify: the intent of the committee when it recommended the government pass these laws last time around was based on the arguments Mr Hansford put forward in his opening statement—that this is about organised crime, exploitation of children and terrorism. These are the kinds of things that we believed were an appropriate balance between the individual's right to freedom and the mandatory dataset. I understand, from your submissions, that the data that other agencies can gather is not necessarily that two-year dataset that's specifically drawn aside. I understand the point you made, Ms McNeill—that this has been a longstanding provision—but it is still the function of this committee, looking at federal law, to say: is the access by other levels of government, which enables people like the RSPCA or whoever, appropriate? Or should we be wrapping some constraints around section 280 of the Telecommunications Act such that there are thresholds of criminality that—for example, if the teachers registration board want to take action against someone who they suspect of bad behaviour, it needs to be the kind of thing that they can refer to the police so the police then take that action. They're the kinds of things we're seeking to understand. Just saying 'teachers registration board'

doesn't give us an example of what they access. It may well be that we need to go to some of the state authorities to get that information from them firsthand.

Mr Kathage: If it would assist the committee, I would like to put a counterfactual forward. Imagine the scenario if section 280 wasn't in operation; as Ms McNeill noted, it has been in operation since at least 1991. From the perspective of a carrier or carriage service provider, if they are approached with a notice to produce from the state body, and they didn't have an authorisation under section 280, they would be in an invidious position in needing to decide which offence they would need to commit in terms of disclosure or nondisclosure.

Senator FAWCETT: The point we're trying to make is: we understand that section 280 is an enabling provision, even for the TIA and everything we want it to do. But if we limited section 280—so if you are approached by a state or territory or other body, you can only release for these kinds of thresholds—that gives them quite clear guidance as to what they can and can't do. Perhaps it's also an issue for COAG. These are the sorts of things. We shouldn't just accept that, because it has been this way for 30 years, it should continue.

Senator KENEALLY: To build on Senator Fawcett's point: 30 years ago, in 1991, we didn't have the internet in the form we have it today and we didn't have the capacity to have the types of data we can access today. These are the questions we're pursuing.

Ms McNeill: I will just make an observation in response to that. You referred to landlines and the sort of data that was traditionally available with landlines. We're increasingly in a world where people don't have landlines at all. So there does have to be some data point available to investigatory authorities. I'm not advocating a particular dataset; it's just an observation.

Senator KENEALLY: With due respect, Ms McNeill, I think you're making our point: the technology has changed but the regulations and the laws haven't.

Mr Warnes: I think this point was expressly looked at in 2015 and there was a decision then to retain, for the same reasons we're talking about now; I don't think our arguments have changed in the intervening period since 2014-15. This was looked at and recognised by the committee, and a decision was made, as I understand it, to leave section 280.

Senator KENEALLY: This is a review. That's our job.

Mr Warnes: Absolutely, but I'm saying from our point—

Mr DREYFUS: Chair?

CHAIR: Mr Dreyfus.

Mr DREYFUS: I want to state for the record that Mr Warnes's characterisation of what occurred in the hearings conducted by this committee in 2015 is completely wrong. The outcome was that this committee's view was that there should be a very restricted group of agencies—namely law enforcement agencies, the ones listed. That was the primary conclusion of this committee. There were other conclusions that this committee drew. One of them is noted in a footnote in the Department of Home Affairs' submission—that is, that there was considerable evidence taken by this committee about what was the appropriateness or otherwise of civil litigants being able to access telecommunications data. The firm recommendation of this committee was that civil litigants should not be able to access telecommunications data. That recommendation was made—it's recommendation 23 of the 2015 report—and it was given effect in the legislation that ultimately passed the parliament. Far from your suggestion being that the committee was unconcerned about section 280, Mr Warnes, the committee was deeply concerned about section 280.

While we're on it, Ms McNeill, I want to ask you something. You referred to section 313(3), which is a set of categories about assistance that is to be given by telecommunications providers to a range of Commonwealth, state and territory agencies. That's true, but section 280—which is the authorisation that's primarily relied on by this disparate group of other state agencies, ranging from local councils to the Victorian Institute of Education—contains no such limitation, does it? It is completely unconstrained, other than the requirement that the disclosure is required or authorised by or under law.

Ms McNeill: That's correct, but there does have to be that authorising provision under law—

Mr DREYFUS: But beyond that, beyond being required to identify a provision in a state or territory act, there is no other filter, no other prerequisite and no other limitation on what access can be required by any agency. The Communications Alliance has identified 87—this is a question for any of you—but it could be a lot more, couldn't it? There's no public reporting requirement to identify which agencies, other than the 20 that we're having to deal with under the Telecommunications (Interception and Access) Act, are accessing telecommunications data.

Ms McNeill: There are at least two propositions wrapped up in that, if I may take each of them in turn. The first one was a question about the extent to which section 280 contains any in-built constraints or whether it is simply a requirement that there be authorisation under law. There is of course the in-built requirement that was put into the legislation as a result of the committee's deliberations, which I think you've referred to, where there are constraints about civil proceedings—

Mr DREYFUS: No, there's a bar. It's a prohibition, Ms McNeill. Don't call it a constraint; it's a bar.

Ms McNeill: It's a very effective constraint, then. The second point I think you were making went to whether there is transparency about the sorts of state agencies and requests that might be made under state law but which section 280 means the telco providers can and should comply with. There is no centralised public reporting of anything like that; you're right.

Mr DREYFUS: Whether it be centralised or otherwise, there's no reporting. Is that right?

Ms McNeill: I don't know if there is reporting in state transparency mechanisms and annual reports. I don't know that for sure. I do know that—

Mr DREYFUS: Not at the Commonwealth level.

Ms McNeill: At the Commonwealth level the only reporting, I think, is the reporting that the Australian Communications and Media Authority does around the use of section 313 by Commonwealth agencies. I think that appears in the ACMA's annual report. That's the only reporting I'm aware of.

Mr Kathage: There is a report that the ACMA produces under section 105.

Mr DREYFUS: You've reproduced that data in your second supplementary submission. What that data tells us about is the number of requests made under 280, as far as ACMA knows, and the number of telecommunications providers—the other end of the transaction—who have provided data. But ACMA don't report anything at all about who—which state and territory agencies—have made requests in the first place.

Mr Kathage: That's correct.

Mr DREYFUS: To be clear for all of you, the committee is interested in this because the Communications Alliance has drawn to our attention, based on the survey of their members—namely, telecommunications service providers; they have some 600 or so members. They surveyed them and asked which agencies have asked them for information under the Telecommunications Act. That's how they got to their list of 87 agencies. This is my question to all of you: does anybody know how many authorisations for telecommunications information have been made in reliance on section 280 and some other law, this year or last year or the year before?

Ms McNeill: We will take that on notice, I'm afraid.

Mr DREYFUS: Thank you. Last question: do you know whether those other laws used in conjunction with section 280 have been used appropriately?

Ms McNeill: No.

CHAIR: So there's no central database where you track this stuff? That's what I was going to follow up with, Mr Dreyfus.

Ms McNeill: No, there's no central database.

Mr TIM WILSON: I want to go to page 16 of your submission, where there's a graph on the percentage of authorisations by age of data. Obviously age of data is a critical topic that is raised by other witnesses throughout this hearing process. Essentially it says that between zero and three months and up to six months, most of the data that is requested is requested. Is that a fair reflection of the graph? Unfortunately I've only got it in black and white, and I can't differentiate between the different ones in black and white. It's based on a number of agencies. I'm wondering: when it gets to the period over 24 months—could you firstly outline which are the two peak ones at the end? Or do you not have a colour version either?

Mr Hansford: We've got it in colour. I think the very top one is ICAC in New South Wales, and the one underneath it is the—it's the yellow one—

Mr Kathage: Our colour differentiation might not be great.

Mr Hansford: It's either the ACCC or QLD Police.

Mr TIM WILSON: Can we perhaps get the underlying data for that chart so that we can have clarity, because it's so confused. I'm not saying it's a misrepresentation or anything, but it's very difficult to read because of the dataset. The other question is: when it comes to the over-24-month period, is there a nature or particular type of crime that leads to it being taken back that far? Presumably up to six months would include all sorts of different crimes and points of investigation and allegations, whereas when you get back to data points, if there is some sort

of reflection we can draw from the need to maintain data for a 24-month period because of severity or seriousness, it would help us in terms of, let's say, the public understanding.

Mr Hansford: Sure. I tried to explain in my opening statement that, in the zero to three month mark, the majority of those are straight subscriber checks. Some agencies actually have the integrated public number database within their agency. So they don't necessarily go straight to the provider. It's almost like a big *White Pages*. You would naturally see, at the start of an investigation, a spike in people checking a name and a number and then either discounting it and doing nothing else or starting an investigation. When you start to move down the graph, towards 21 to 24 months and above, we've outlined in our submission that there are a range of different crime types where over 24 months is particularly important. Espionage and foreign interference was one we've highlighted. The corruption of a Commonwealth or state and territory official that might not be reported for some time and then the compilation of material to—

Mr TIM WILSON: Reported for some time or not become obvious?

Mr Hansford: It might not be reported and then you might do a subscriber check and identify an individual. It may take some time to work out. Because of the sophistication, potentially, of a law enforcement person who knows law enforcement methods, in order to counter their tradecraft, you might need to work for some time or go back to data that's been held for over 24 months. It might be a particularly complex fraud investigation which involves a lot of different component parts and communications. It might be a rape from a state jurisdiction that's historic.

Mr TIM WILSON: I'm not arguing that there aren't plenty of examples. I'm just wondering if there's any underlying trend about the particular types that are emerging.

Mr Warnes: I know that graph is a little tricky to read, especially because it's in black and white, but if you read it and if my colour differentiation is any good, the top two big peaks after those 24 months—I'm reasonably confident, and I will correct it on notice if I'm wrong—are ICAC New South Wales and the Law Enforcement Corruption Commission. I think that gives you an idea, with those two agencies having a big peak at the back end, that corruption is a particular subset of crime that might not become apparent for a while and then you might need to do initial investigations sometime after the actual offending.

Mr BYRNE: I have a long history with this right from the start when there were 2.5 lines in a submission from the Attorney-General's Department's office that spoke of data retention to the committee when I was chair. The issue for the committee was that we fleshed out exactly what data retention. So our committee effectively created the subset of the data that you've been talking about and created the framework for the then enabling legislation to be enacted by the government.

One of the things that has struck me, listening to your presentations today, was what I was told and why the agencies were given the powers in the first place. That was that they only wanted a set number of organisations—I think we agreed upon 21—that could access this really important data. Our committee, in its various iterations, was told in 2012, 2013, 2015 and 2016 that they would be doing everything within their power to limit the number of organisations that could access this metadata. So for me to hear you effectively say that you're not quite sure how many organisations can access this metadata and then casually say that it's a jurisdictional issue goes against the guarantee that we were given to put the scheme in the first place. So if you were me and you were listening to what I've just listened to, which was a cavalier disregard for people accessing intrusive information which this parliament had to fight years for, how do you think I would feel about that?

Mr Hansford: I think that there are two issues. The first that you've rightfully outlined is that this committee did deliberate long and hard, and I accept the fact that it took a long time to come to a decision about the types of data that were retained for data retention purposes and the limitation for the 21 agencies contained in the TIA Act. Our evidence to you is that the comprehensive reporting of the 21 agencies outlined in the annual report and other oversight mechanisms—the clear governance arrangements for those 21 agencies in terms of the retained data and access to the retained data is highly governed and highly reported and highly transparent. That relates to the agencies and the retained data. What we're talking about in the telecommunications act is about data access and not related to the data retention regime. It's a general access power, as opposed to all of the safeguards that this committee recommended and the parliament eventually legislated for, which are outlined in the TIA Act. The concern that you have is in relation to access to data rather than the data retention regime and the 21 agencies, and I think there is a big distinct difference.

Mr BYRNE: I would disagree with you, particularly given the reports and the discussions that we've had with interested stakeholders that have conducted surveys of the company of what was precisely sought, which was, basically, from our understanding, metadata. So I disagree with you. The fact that there's been a report on that—I

come back to the point that the agencies were basically saying to me in 2012 that it was bad that the RSPCA could get access to the data. It didn't suit their purposes because it undermined faith in the scheme. The police were telling me the same thing. We heard from different heads of the organisations. We were told that it didn't matter about the nuance of what you've put forward, but people's capacity to access metadata or information in the way you described, if this scheme was given to the agencies, would be stopped. What you've just said today, basically says it hasn't been stopped. Worse than that, you've known about it and you've done nothing about it. You didn't come to the committee and say, 'This is a problem.' We had to find out via third parties, and then to hear you justify it—I don't need a lecture about schools pursuing principles. Your organisation has got responsibility for coordinating access to this. To hear you say, 'Well, it's a state problem'—there's a thing called COAG that you could use. You use it when there are national emergencies. This undermines faith in the scheme. If you think that it's okay that the RSPCA accesses it or councils or teachers, and then you defend them—your role is to make sure that the agencies—

Mr Hansford: Mr Byrne—

Mr BYRNE: I haven't finished. You listen and I talk. This is the way this goes. When I ask you questions, you respond. That's what you do. That's what we're here for as a committee. What I'm saying to you, as someone who was involved right at the start of this, is that this is unacceptable, and your job should have been to come to this committee to point it out and to find some legislative way we could fix this. As I said, underpinning this scheme, underpinning the reason why we gave the agencies, the agencies that you allegedly represent, the powers was that we would protect access to intrusive data—you want to call it metadata, whatever it is—and prevent the very thing that you've just casually described as happening from happening. That's why I'm so annoyed about it.

Mr Hansford: I don't think Mr Warnes's testimony was either cavalier or defending the existing regime. He was merely pointing out how it operates. I think the evidence that we've given and the concern that you're trying to articulate and we're trying to respond to is that the data retention regime put a mandatory obligation on carriage service providers and carriers to retain data—

Mr BYRNE: You're not answering my question.

Mr Hansford: What we're saying is the agencies that can access data under the data retention regime—

Mr BYRNE: You are not answering my question. Pass it on. I'm finished. That's it.

Mr Hansford: Sorry, what was your question?

Mr BYRNE: I said we were given a guarantee when the agencies were given metadata that this sort of—it doesn't matter about the state jurisdictions—thing wouldn't occur. I literally took evidence. I had discussions with agency heads about this matter. I was told this would be plugged. It has not been plugged. It doesn't matter about you handballing it over to the state agencies. They could access it; it was access to telecommunications data. You take it on notice. I'm finished. You've basically not answered the question. You've indicated to me that you're not seriously wanting to address the issue. I'm extremely annoyed about the issue, and I will pursue it in another forum. I pass this on. Park it. I don't want to hear any more from you.

Mr Hansford: Mr Byrne—

Mr BYRNE: Park it and we can pass it on. Listen to me: park it and pass it onto other committee members. I'm done with you on this. Move on. That's it. I'm done.

Mr Hansford: Um—

Mr BYRNE: Don't talk. Keep going.

CHAIR: Thank you, Deputy Chair. Is there a way around this, potentially: for all data requests to go through state police bodies?

Mr Hansford: Chair, our evidence is that the 21 agencies who have a regime under the TIA Act access information that has been mandatorily held by carriers for two years and that the governance around access to that data is highly governed and is transparent and outlined in the report. Mr Dreyfus raised the point that section 280 was raised in the last committee hearing and the last consideration of the issue, but that legislative—

Mr DREYFUS: No, no—it's been raised for years.

Mr Hansford: For years, indeed. And that piece of legislation—and 280 and 313—was not changed in 2015. So, on the face of the legislation, under court orders, for coroners and for a whole range of people, that legislative provision was retained by the parliament.

Mr DREYFUS: And we're trying to get at how it's being used.

Mr Hansford: Indeed.

Mr DREYFUS: If I can paraphrase Mr Byrne's questions, what we're trying to get at—and we're seeking the assistance of the department of communications and the Department of Home Affairs—is to try to see: what are these very extensive uses, under section 280, of telecommunications data? You're not in a position at present to reassure us in the least about whether there are safeguards or checking, or what it's being used for. It appears you simply don't know, and you've taken it on notice, and you're going to come back to us about those uses of section 280, which will go a long way beyond, I hope, what ACMA presently tells us—that being the thousands of requests that are made under section 280 and the number of telecommunications providers who give information. What we're looking for is the other end of the process.

Mr Hansford: I think we've got some numbers under 280 that we can give you and are outlined in our submission. But the point I was trying to make is: not to conflate the two regimes in two separate pieces of legislation and treat them as a problem in its entirety. There are two different issues. The policy issue that you have identified is in the Telecommunications Act and section 280, as distinct from the data retention regime in chapter 4 of the TIA Act. I just want to try to make that distinction and identify what concern the committee particularly has, and, from our understanding, it was sections 280 and 313.

Mr DREYFUS: Well, if I can state it, it's that there are, according to the Communications Alliance, some 87 government agencies—state and territory and some federal—in addition to the 20 agencies formally listed in the Telecommunications (Interception and Access) Act, that are accessing telecommunications data. You don't need to tell me anything about there being two separate sets of legal process here. I fully understand that.

Mr Hansford: But just to be clear: the 87 agencies are not accessing telecommunications data under the TIA Act.

Mr DREYFUS: You don't know that. Let's be clear about that, too, Mr Hansford. You have no idea. You are pointing to a provision in the Telecommunications (Interception and Access) Act which says that it's only the 20-odd agencies that are to have access to the data that is retained—

Mr Hansford: Under that regime.

Mr DREYFUS: only for the purposes of compliance with the mandatory data retention regime. But, because you don't appear to have much information available—and that's not necessarily a criticism; there are no laws around this—

Mr Hansford: Understood.

Mr DREYFUS: You're not actually able to tell us, and anything you can provide—you don't have to do it now, but anything you can provide—

Mr Hansford: We can give you the statistics that we've got.

Mr DREYFUS: Sure, but we'll come to that in a tick. It would be helpful because then we might be able to interrogate whether that provision, which you correctly point to—namely, that the mandatory data retention regime is confined to those 20 agencies—is being adhered to, because the Communications Alliance gave a little bit of evidence about this, and it should be obvious to all of you that there's a difficulty here. There's no supervision and no reporting, and no accountability mechanism at all about this section 280 process. We are reliant on, potentially, quite small communication service providers doing the checking and making sure that there is a lawful request and also reliant, it seems—because there are no scrutiny or accountability mechanisms here—on those communication service providers adhering to the prohibition that is contained in the Telecommunications (Interception and Access) Act on their mandatory data retention, retained data, not being revealed. Some of the communication service providers who are subject to the mandatory data retention regime don't keep the data separately. Some do. We know they do because Telstra set up a huge separate facility in Clayton Victoria to comply with its requirements, but other smaller communications providers don't necessarily keep it separate. I'm trying to flesh out for you what the committee's inquiry is about.

Mr Hansford: I think we're on the same page.

Mr Kathage: If I might add, I suppose, as you've noted, the numbers of disclosures that occur under section 280 there are reported by the ACMA. As Mr Hansford mentioned, those disclosures in 2018-19 were 8,432. I note the committee's concerns that that's just the numbers that are reported, not necessarily the reasons for those disclosures. I suppose I would make two points.

The first point is that the ACMA is responsible for the enforcement of section 276. It is the case that some investigations can occur, to the extent that section 280 is being used properly, including that the authorising law that is being relied on, be that section 313(3) or laws at the state level, are appropriately used.

I suppose the other point I would make is that there has been a concern expressed by the committee of the merits of state based authorising laws, and it would be open to the committee to talk to those agencies that use those authorising provisions.

CHAIR: To go to Mr Dreyfus' point about accountability and oversight, we're looking at practical ways to enhance the integrity of the regime. With the advances in technology and databasing on the government side, would it be onerous to have some form of central database to collect information on who has accessed data under the metadata regime?

Mr Kathage: I suppose, absolutely, enhancements to the reporting that is done by the ACMA could be contemplated. In a sense, it depends on the information that is held by carriers and carriage service providers in receiving requests, but that is something that could be looked at, yes.

CHAIR: What about from Home Affairs? Do you have a view on that?

Mr Hansford: I think we have pretty comprehensive reporting for the 21 agencies. The outstanding policy issue that Mr Dreyfus has articulated is for the access to telecommunications data under the Telecommunications Act. The question is really for our colleagues in the Department of Infrastructure, Transport, Regional Development and Communications to work with us about how those two regimes might operate together.

Senator McALLISTER: I want to move on to a different matter, so it's a little dependent on other committee members feeling that we've, at least for the time being, exhausted this conversation about access. In your submission, at page 13, paragraph 54, you make a very limited case for expanding the datasets that are kept. In the context of this morning's conversation about some of the shortcomings, certainly from my perspective about the access arrangements for existing datasets, I wanted to talk to you about the case for expanding them.

As the digital world expands and we move into a kind of 'internet of things' environment, telecommunications' networks will be used to enable substantially larger numbers of devices in an individual's home or workplace. There appears to be, at least from some of the submitters, a lack of clarity about the extent to which the existing regime applies to these new devices. Optus' submission is particularly useful, in this regard. They make the point that, whilst the administrative guidance that's been developed to support implementation has been really useful, there's going to have to be active management about the extent to which the regime applies to watches, refrigerators or phones. They also make the point that, should the department seek to expand the regime to include data of that kind, a positive case for the value to law enforcement and the proportionality of such an expansion, relative to the burdens on privacy it suggests, would need to be made. Are you doing that work, because it's not really apparent at paragraphs 54 and 55?

Mr Hansford: I think Senator Keneally made the point that in 1979 the T(IA) Act was looking at an individual and an individual communication. On the face of the legislation, that still holds true today. When you look at, as you rightly said, particularly the 5G environment and the internet of things, that's a whole area where data will be produced and might be available to telecommunications providers. We have outlined in our submission that the current regime is suiting the current purposes for law enforcement and other agencies, but we do recognise that there is a broader issue around things like machine-to-machine communications—a fridge talking to a watch and those types of things. The government has commissioned a comprehensive review of the national security intelligence legal framework by Mr Richardson, and that review has a terms of reference to look at the T(IA) Act and to look at how that's really supporting the national intelligence community effort. That is one mechanism that the government is looking at to comprehensively review the regime.

Also, we continue to do a lot of policy work and work with agencies, particularly through our national consultative committee processes, to see what the key operational impediments and issues that agencies are finding are and what policy solutions we might develop. Our evidence that's outlined both in this hearing and in our submission is that the current regime, the current data, is really suiting law enforcement efforts at this point in time, but we do recognise that there is an emerging issue and that is something that we will have to grapple with.

Senator McALLISTER: It's not really an emerging issue, is it? From your perspective, it's an emerging opportunity.

Mr Hansford: That's true.

Senator McALLISTER: What I'm asking you is whether your submission is, over the course of this inquiry, seeking to make the case to expand the regime to include these additional kinds of datasets—machine-to-machine communications et cetera—or not.

Mr Warnes: No, the submission is not making that case. It just flags that agencies have noted some extra data that could be retained would be useful if it were guaranteed to be there. Of course, that doesn't mean that they

can't access it if providers are actually retaining it themselves. That's a really important distinction—that they can access things that are being retained by providers. So we're not making the case to expand the dataset, no.

Senator McALLISTER: Are you involved in any work with any other agency of government that's seeking to engage with the privacy implications of the scenario that you've just outlined? It's an additional and new dataset which potentially provides a great deal of information about pattern of life for individuals. Your evidence just now is that it's able to be accessed by law enforcement or, indeed, a whole range of other organisations under the existing regime, should it be retained by the telecommunications provider. Is there any part of government that is seeking to deal with the privacy implications of that scenario?

Mr Warnes: We think that the privacy provisions are already considered under the existing legislative framework as set out—that it has to be bounded by 'reasonably necessary', for example, for the enforcement of the criminal law. If companies are able to exploit that data to target advertising and do their own sorts of work with it and retain it for those purposes, our submission would be that it's reasonable for law enforcement to access it where it's necessary for the enforcement of the criminal law.

Senator McALLISTER: So there's no work going on? Your evidence is that you're satisfied with the existing protections that are in place and there's no work going on in government to engage with this set of issues from a law enforcement and intelligence perspective?

Mr Hansford: I think our submission to you was that we continually look at reforms and we're continually looking at it. Is there a specific piece of work?

Well, yes. I've outlined to you that the *Comprehensive review of the legal framework governing the National Intelligence Community* looked at that. We're looking at the issues that Mr Richardson identified and our policy team is looking at the very issue of machine-to-machine communication and how we might design a regime that would capture that. Nothing's been put to the government yet.

Senator McALLISTER: I see. When is that work going to conclude? That's being done in your division, Mr Hansford?

Mr Hansford: We look after the Telecommunications (Interception and Access) Act. The government has outlined—and I'll just check on the government's public statements on this—that they have received the comprehensive review and will develop a government response.

Senator McALLISTER: I'm trying to understand whether you're doing a separate and additional piece of work to the work being done by Mr Richardson?

Mr Hansford: There are two issues: the review and then our day-to-day policy work. My submission to you is we are looking at things like machine-to-machine communication, how we look at electronic surveillance in the future and what are the key impediments that law enforcement have identified. Outside of this review, we've been working on those very issues and we continue to do so.

Senator McALLISTER: Is there a specific project underway in this regard in the department at the moment?

Mr Hansford: I wouldn't categorise it as a project, but we are looking at it. It goes back as far as the 2013 inquiry in the parliament that said that the T(IA) Act needs fundamental reform. Multiple reviews have looked at it. We are looking at how we might be able to do that in a proportional way to deal with all of the issues that law enforcement are dealing with. Separately, there is a particular project that the department is working on—and that's the 2020 Cyber Security Strategy—which recognises a whole range of different cybersecurity threats, including cybercrime and how that might be dealt with in the future. The particular point there is that the last cybersecurity act was only four years ago and we're already reviewing it. So multiple pieces of policy work are being developed in the Department of Home Affairs from different lenses. But my evidence to you is we are looking at machine-to-machine communication. We are looking at what a future regime might look like and, as this committee has found out, it's pretty complex work.

Senator McALLISTER: Indeed. Is there a time frame for the conclusion of this policy work that you've commenced?

Mr Hansford: There's no specific time frame. We are involved in a range of different bodies of work but, as I said to you, the government is considering a review and may well make some comments about any reforms later this year.

Senator KENEALLY: May I quickly follow up on that because I think that Senator McAllister's questions about the work that is being done are relevant. I think, Mr Warnes, you may have mentioned the capacity for companies to use this data in terms of advertising, targeting consumers et cetera. Therefore, if I can paraphrase your testimony, similar data should be available for law enforcement agencies. I just note that last year the ACCC

did the Digital Platforms Inquiry that looked specifically at the question of data retention and privacy in the context of advertising and targeting of consumers as well as people being able to control their data on online platforms. Has that review been taken into account in the work that you are constantly reviewing, Mr Hansford, in terms of the data retention laws and the privacy issues that have been raised by the internet of things?

Mr Hansford: Indeed. I think the whole digital environment is one that is emerging. It's one that lots of parts of government are looking at—from the ACCC to task forces within the Department of the Prime Minister and Cabinet. Our cybersecurity team is looking at it from a lawful access perspective. We're looking at a lot of different parts and using a lot of evidence to try to build a robust policy base.

Senator KENEALLY: The Information and Privacy Commissioner, as well, has had a few things to say in this area.

Mr Hansford: We consistently look at the Information and Privacy Commissioner, the IGIS and the Ombudsman—all of their findings on access to the metadata regime or the data retention regime where they identify issues and where agencies self-report—and all of that goes into forming an evidence base.

Senator KENEALLY: I think Senator McAllister was able to clarify that you're not recommending that we should consider putting a requirement on companies to retain this data at this time, but you seem to be considering what to do about this question. Communication providers gave evidence before us at our last hearing that they're unclear as to whether or not they're meant to retain this data. So your clarity today that you're not specifically recommending that is helpful.

Mr Warnes: If it's not within the five datasets, that's correct.

Senator KENEALLY: Are you looking to actually bring forward a recommendation to government that would provide that clarity at some point in the future?

Mr Hansford: I think our evidence, on the current legislation, is that we can do further work on guidance to make it clearer, if there are particular concerns from communications companies and telecommunications companies. We can do that body of work. As to the broader issues, we're still considering them.

Senator KENEALLY: I'm asking if there is a time frame or a process underway that we can come back and talk to you about later, to understand when we might get this information and when you might be bringing policy proposals forward.

Mr Hansford: Without wanting to reveal the contents of the comprehensive review, I think the process that I can outline to you, that the government is considering, is that the comprehensive review raised a range of different issues and a number of recommendations in this area, and the government will be looking to provide a response to that review later in the year.

Senator FAWCETT: Mr Hansford, can I come back to both your opening statement and also your second supplementary submission, where you talk about the fact that the graph that shows the age of demands obscures the fact that those demands that are beyond 12 months are often for the most complex cases, and you're making a case there for retaining the minimum two years of that dataset. Noting that the minimum dataset that this committee agreed to when we first put this legislation through is only a subset of what the providers keep, and many of those providers keep a range of information for much longer, up to seven years or more, are there any of those inquiries that deal with those more serious matters, where investigations have been frustrated, either by an inability to access data more than two years old or by particular datasets that a company has kept but not for as long as two years? That is, are there grounds, given that these are the most serious crimes, to consider specific extensions in some areas—either expanding the dataset or expanding the time?

Mr Hansford: You'll speak to law enforcement later this afternoon, and I think their evidence is that any data that can assist in an investigation is helpful. But you're right. In our supplementary submission we outline, particularly, the changing nature of some of the crime types, and we point to counterespionage and the work that ASIO and the AFP do—foreign interference and long-term terrorism investigations which have really difficult and complex characteristics. I think that the environment is becoming much more complex and obviously if data were retained after 24 months and could be of use in an investigation that would be a positive thing. But the balance that we've put forward in our submission is that the two-year period is helpful for law enforcement and the intelligence community.

We have also outlined in our first submission, I think, that there are a range of international examples where there's varying degrees of data retention. In the case of Italy, I think, it's six years. You look at the particular environment with the organised crime threat in Italy, and the Italian government and the Italian police obviously find it of benefit to have the data retention period for six years, given the complex world they live in, particularly with some organised crime groups like the 'Ndrangheta, who are incredibly secretive. The evidence that this

committee took in 2015 and the types of case studies we've outlined to you and the complexity of the case studies puts a case for two years, and outlines that that is actually providing a lot of useful information. But, equally, you're right: there is information used after 24 months.

Mr Warnes: Perhaps to add to Mr Hansford's answer, there was one case study outlined in our submission where the AFP received a referral from a foreign law enforcement agency, where the alleged offender was using an onion router to obscure their identity to access child exploitation material. That ended up being just outside the two-year threshold for the retained data, and that data wasn't there and the AFP wasn't able to pursue that matter. When you're looking at the balance that Mr Hansford has talked about, any shift in that balance the other way, if you have less data retained for two years, is going to increase the number of cases where you see this type of outcome, because it's really important initial investigatory material that will stop an investigation—and the AFP can give much better evidence than I can on investigative techniques.

Senator FAWCETT: That's the point I'm trying to get at. You have given us a number of worked examples, most of which demonstrate why the data has been useful beyond 12 months, but the cases where an investigation has not proceeded are useful—and, if there are any further of those you could provide, that would be great. As a related question, in 2015, when we were looking at the original passage of the data retention, there was a fair bit of evidence around the range of voluntary data retention. Some of the classic telcos were seven years plus, because it was just how their billings systems worked. There was a lot of evidence that emerging providers, who are using over the internet type protocols for phone calls as well as internet access, didn't retain data, because their billing systems were different. And there was concern that, by mandating a two-year limit, we would see a change of behaviour and that a lot of companies that had been keeping data for long term would actually start culling and reducing that. Have you seen any evidence of companies deliberately reducing data down to two years, or are many of those telcos still doing what they've done for decades and retaining data for more than five or seven years?

Mr Warnes: I haven't seen any evidence. I think you'd have to ask the telecommunications companies—probably better than the department—about their practices. There are some sporadic examples of companies still having some data available in the three- to four-year period, for some cases, which we've drawn out in our submissions, but there are also cases, like the one I just gave you, where companies don't have that data after two years. That case in particular that I referred to was only a few months after the two-year period—about five months—so it was about 2½ years and that data was gone. It gives you some indication by way of anecdote, but I don't have detailed information to respond to your question on that.

Senator FAWCETT: Some of the concerns raised by people who are concerned about intrusions on privacy and civil liberties go to the amount of data, the time it's retained, the threshold for access and whether or not a warrant is approved or required. If there is a case for data to be retained longer so those more serious crimes can be dealt with, would the cost implications for industry to increase the time be minor if they are already retaining data for their own purposes longer anyway? From an agency perspective, if we were going beyond two years, would the requirement for a warrant in that small number of cases, but more serious cases, be an unreasonable burden for you? It would only be for those cases beyond two years in that more serious category. It is so we get the balance of keeping data available but also putting thresholds there to satisfy the balancing around privacy.

Mr Hansford: That's certainly something we could look at, and if the committee were minded to recommend, beyond the 24-month period, a warranted regime, it's something we'd look at closely. But, noting the fact that, if companies already keep telecommunications data for longer than 24 months, it's not subject to a warrant already. I do note the speech provided by Mr Phelan of the ACIC, who is appearing later today, that, particularly if a warranted regime were put over the entire data retention regime, they may as well pack up and go home; I think those were his words. I think that's particularly relevant with things like looking at child exploitation on the dark web, and Mr Warnes used the example of the onion router, the virtual private network and masking of information; that makes it much more complicated for any law enforcement agency to investigate those types of crimes. Is there a case for beyond 24 months? Obviously on the face of it there is, but whether or not that's a policy response that might be implemented we will have to look at in detail.

Senator FAWCETT: Sure. Speaking from myself, there is no appetite to warrant the up to 24 months because I accept that it's a very legitimate use. Many of the public don't differentiate in their minds the difference between the mandated data and the volumes of data which are kept on a voluntary basis for much longer periods. I don't think most of the public recognise there is a difference there. If we try and give more mandated protection for data there has to be an equivalent balancing. I think that's where potentially, for longer periods were that to be an approach, there would have to be a balance and that may look at warrants or other thresholds for access to that.

Mr LEESER: I want to have a sense of the legislative history of how we got to the two years. Looking at your submission you quote from this committee and two years was a compromised position when the 2014 bill was being considered. What was the initial position of the government when the bill was introduced, in terms of the period of time which the data should be retained?

Mr Hansford: I'll have to refresh my memory on the precise events of 2014 and 2015, and we might take some of that on notice. The criticality of the information in the first two years was the evidence of the Attorney-General's Department at the time, and law enforcement intelligence committees—that was particularly critical to ongoing investigations and the environment that they found at the time. We've included in our submission, as I said before, a number of international jurisdictions. We continue to look at what the balance of international law is and what are other countries doing. It does range from, I think Germany is—

Mr LEESER: We had an example of the outlier at six years—

Mr Hansford: Six years is definitely the outlier. Germany is a very short period. The evidence that was provided both in our current submission and back in 2015, as I understand it, is that two years is an appropriate balance. But the longer the period the more information would be retained and the more it would assist investigations, self-evidently.

Mr LEESER: I suppose what I was wanting you to do was to give us a sense of what that period was, to reflect on the rationale that the agencies, that the government, asked for a longer period initially, to look at the a affliction of time and your experience with the regime. All the data you have given us here indicates that in most instances it's data that has been retained, it's data that has been recently collected, that is the one that is most used. But there's a bit of the submissions that it is slightly, if I may put it this way, schizophrenic, in that having said that you also note there are some agencies, including ASIO, that are saying there are these longer investigations that require, potentially, the consideration of data to be retained.

I take the point Senator Fawcett made about whether there's a need to look at warranted periods after the two year period. In paragraph 78 of your submission you've come what I might describe as a fence-sitting position which is, 'We'd need to have a bit more discussion about some of the privacy implications if we were going to extend.' What I would really like to know is what do you, as a department, what do the agencies, want us to do? We can make the decisions about the balancing. Given the nature of what you've seen and the way in which you and other agencies have been looking at the way in which data has been retained, and the usefulness of having data retained over a longer period, effectively, I wonder if you might reflect on whether—after this period that the data retention regime has been going—any of the initial concerns that you had asking for a longer period were warranted? And, indeed, whether we should be considering a longer period at this point?

Mr Hansford: Sure. In relation to Senator Fawcett's question, we took on notice that we would look at particular examples where over 24 months was useful. We'll ask agencies, and you're hearing from agencies later this afternoon, so you might be minded to ask them as well what would be useful to their investigations and intelligence work. Our submission takes up the history from 2015 and starts from and accepts the premise that this committee and the parliament recommended two years, and nothing has substantially changed in the environment to warrant an extension of the regime, except for the fact that a lot of the environment is becoming more complex and technology is increasing, but the fundamental policy position articulated in our submission hasn't changed. We will take on notice the starting position in 2015. I do note that in 2015 there was a particularly helpful table in ASIO's submission which outlined the types of data that were kept. The longest period was, I think, seven years, as I think Mr Dreyfus previously said, from one particular provider. So, self-evidently, that goes to evidence that's saying there is some use in keeping data for seven years, but that has not been reflected in our submission.

Mr LEESER: The problem that you were getting at with the legislation, as I understand it from reading your submission, is that there were some providers that just weren't keeping any data, and then, as the table on page 10 of the submission shows, there were some that were keeping it for longer than seven years. In asking the question, I don't want to indicate that I'm in favour of increasing the retention period; I just want to hear from the agencies what their view is in relation to that question.

Mr Hansford: Sure.

Ms McNeill: I will just observe that I know that you've said that it's the role of the committee to balance the different interests of entities in this space. One of those interests, obviously, will be the interests of industry, who previously have been quite concerned about the costs, including the costs of changing regimes very frequently.

Senator KENEALLY: I think Mr Leeser has pursued the questions I wished to ask, and I thank him for his questioning, which brought some clarity to what I would concur was a rather fence-sitting proposition being put before us.

Mr DREYFUS: I want to ask about the historical data authorisations and how the power is being used. In 2018-19 there were 291,353 authorisations by enforcement agencies for the release of telecommunications data in the enforcement of a criminal law. That was under section 186(1)(a) of the TIA Act. Have I got that right?

Mr Hansford: On the assumption you're using the figures in the annual report—

Mr DREYFUS: Yes.

Mr Hansford: we can confirm the annual report is correct.

Mr DREYFUS: Based on that number, how many individuals and how many individual corporations did those approximately 290,000 authorisations relate to?

Mr Hansford: We don't break down the data to individuals.

Mr DREYFUS: The purpose of asking is: did law enforcement agencies in Australia access the telecommunications data of 290,000 Australians in 2018-19, or was it 200,000 or 100,000 or 1,000? It could have been 1,000 but accessed 290 times each.

Mr Hansford: Yes, correct.

Mr DREYFUS: Are you saying you don't know?

Mr Warnes: It's not broken down in that way. You are correct in saying that multiple data authorisations can be for the individual. I would be very confident in saying it was not 290,000. The journalist information warrant scheme gives you some indication of how that works, with I think it was six warrants for about 80 authorisations of data. So that shows you how that works, but we don't have that detail.

Mr DREYFUS: Is there any way you can give us any idea of what ratio we might usefully apply to the approximately 290,000 authorisations used in the criminal law?

Mr Hansford: I think we could work with the 21 agencies, or a component of the 21 agencies, to give you an understanding of generally in an investigation how many authorisations are issued. We're not going to get the specific number of individuals that have—

Mr DREYFUS: I'm sure. It'll be an average.

Mr Hansford: But we might give you a sense that, for every serious criminal investigation, we do on average 50 authorisations, for instance, or two, or one. We might be able to give you a more anecdotal response rather than a specific number.

Mr DREYFUS: If you could, and if you could take that on notice.

Mr Hansford: Sure.

Mr DREYFUS: You note in your primary submission, at paragraph 30, that section 180F of the TIA Act requires an authorised officer in an enforcement agency to have regard to, among other things, the gravity of the conduct in relation to which the authorisation is sought before seeking access to retain telecommunications data. In the annual report, which I imagine you've got there, the department sets out the categories of offences for which authorisations have been made. As is apparent to anyone reading it, the categories are very broad. In many cases, they don't provide an indication of the gravity of the conduct. The best example of that category would be the category called 'miscellaneous', which could mean anything at all. Can you provide a breakdown of the offence provisions that those 190,000-plus authorisations relate to? I'll flesh that out. For example, 10,000 authorisations were made in relation to alleged breaches of section 250-something of the New South Wales Crimes Act 1900, or 30,000 authorisations were made in relation to alleged breaches of section 122.4 of the Commonwealth Criminal Code—that's unauthorised disclosure by a current or former Commonwealth officer. That's precise, but the other ones are just very general descriptions. Are you able to provide the committee with more information about the offence provisions for the general categories?

Mr Hansford: We will try to do that but I think we are reliant on how all of those 21 agencies collect information and report to us. But we will double-check whether or not we have any further broken-down information per category of offence and what offence that might relate to if it is possible to do so.

Mr DREYFUS: That would be helpful, because, as you've all acknowledged, the role of this committee is to look at the balance that is involved here between the seriousness of the offences and the utility of the information as against all of the other privacy and community considerations that arise. What conduct is captured by the category 'miscellaneous'?

Mr Warnes: I would have to take that on notice.

Mr DREYFUS: That's alright. If you could do that too. I will move to a separate topic, and that is the topic of warrants. A lot of submitters have argued to this committee that judicial warrants should be required for access to

telecommunications data. This is something that you deal with in the second of your supplementary submissions, and in paragraph 16 of your primary submission you point to the fact that law enforcement use the data to rule out innocent parties from suspicion without having to resort to more privacy-intrusive and costly investigative measures. This may be something you need to take on notice, but how many of the 291,353 authorisations by law enforcement agencies for the release of data for the enforcement of the criminal law in 2018-19 related to innocent parties who were ultimately ruled out from suspicion? If you can't say exactly, can you tell me approximately how many?

Mr Warnes: I suspect that will be very difficult information to get. The evidence in our submission was based on conversations we'd had with agencies about more generally how they would use in their investigations that type of authorisation. I'm happy to take it on notice and see if I'm able to.

Mr DREYFUS: I'm certain that you will not be able to provide precision on this. But if you could make some inquiry of other agencies about what proportion we're talking about and how often.

Mr Warnes: Happy to.

Mr DREYFUS: It's a perfectly legitimate use of data. I'm not suggesting otherwise.

Mr Warnes: No—I'm more concerned about our ability to be able to get it than about the data.

Mr DREYFUS: Do your best.

Mr Hansford: You get some indication when you look table 40 on page 71 of the annual report, and you look at the subscriber data versus the traffic data. I don't want to cast aspersions on a direct link but you can anecdotally get some information about where there's been a subscriber check and then potentially additional traffic data that has been requested. You get a sense about the proportion of information that's been accessed. I'm not concluding, though, that that would be directly innocent people—but you get a sense. But as Mr Warnes said we will take it on notice.

Mr DREYFUS: How many of the authorisations in total do you think might have led on to the use of more privacy-intrusive and costly investigative measures being deployed? What I'm getting to is: can you quantify the link that you have sought to draw in your submissions between these two types of investigations?

Mr Hansford: Well, I think we can point you to the information that has been accessed by agencies under the data retention regime, and then the numbers of, for instance, telecommunications interception warrants and stored communication warrants or other powers, which are documented in the annual report. But if you're asking us to do a specific analysis of the information that's sought under the data request, or under the data retention regime, and then whether or not a further power has been used, I'm not sure that would be possible to undertake.

Mr DREYFUS: Do what you can. You've taken it on notice.

Mr Hansford: We will do what we can, certainly.

Mr DREYFUS: It goes to the strength of the argument that you're putting. If you can't back it up with any data, it raises a question about whether the department knows exactly, or roughly, how the powers are being exercised, or is it simply—I'll put it nicely—just extrapolating from a small number of anecdotal reports from agencies. I'm sure—just to take this point—that there are occasions on which telecommunications data is used to rule out innocent persons—of course. That is what one would expect of our enforcement agencies—

Mr Hansford: And we've given some examples—

Mr DREYFUS: That's right. But I'm trying to get to whether or not you can quantify it at all, even by way of estimate, because it would add to the strength of the argument that is being put here.

Mr Hansford: Understood.

Mr DREYFUS: You've argued at paragraph 99 of the second supplementary submission that: Warrant applications are resource intensive, and can take days, if not weeks, to prepare, review and issue. You also say, at paragraph 94:

... the regime already contains a number of rigorous conditions that must be satisfied before these agencies can seek access to telecommunications data for their investigations and operations. When these thresholds are applied in succession, it ensures that agencies exercise their power to access telecommunications data appropriately, and only when necessary.

How resource intensive is the process of working through those thresholds that you're talking about there? How much time do authorised officers spend on each request for an authorisation?

Mr Hansford: I think the best way to get the answer to that is to ask some of the agencies that work on this day-to-day. I can't give you a precise time, because it would depend on the matter.

Mr DREYFUS: So, the department doesn't know, and you think we should best ask the agencies?

Mr Hansford: The department does not have data on the amount of time it takes per application process. We can give you a sense of the quantum of applications, the types of crime, but I don't have that data.

Mr DREYFUS: I accept that—and we should ask the agencies. The power to make an authorisation for an individual's telecommunications data is exercised by an authorised officer under this legislation. Are you able to say nationally how many people are authorised officers for the purposes of section 178 of the Telecommunications (Interception and Access) Act?

Mr Hansford: No. We will take it on notice, in that we will ask each of the agencies how many designated officers they have, and if they keep that list. We will try to compile it and come back.

Mr DREYFUS: Thank you. You also say, at paragraph 83 in the second supplementary submission, that access to telecommunications data under the TIA Act is: 'subject to stringent decision making criteria'. You also point to the fact, at paragraph 87, that 'telecommunications data can only be accessed if it is "reasonably necessary" for a relevant purpose'. That assessment would be made on a case-by-case basis by an authorised officer. Is that right?

Mr Hansford: Yes.

Mr DREYFUS: How much knowledge or involvement would an officer who authorises the release of telecommunications data have of a particular investigation? What does an internal approval process look like?

Mr Hansford: I think it would depend on the agency. When you ask some of the agencies—in my sector, maybe ask the AFP later this afternoon—what the characteristic of the authorising officer is—I know you've already had evidence from ACLEI about their authorisation regime and a couple of officers who are intimately involved in the investigatory process and their authorisation of requests. I think it would vary per agency. But the evidence that I think has so far been given to this committee is that it is an experienced officer of sufficiently high level in agencies making that decision, independent from the investigation.

Mr DREYFUS: Is the process something like an investigating officer goes to an authorised officer and says, 'Can you approve this?' That's the start of it, isn't it? The investigating officer goes to the authorised officer and says, 'Can you approve this authorisation for telecommunications data?'

Mr Hansford: Yes, and they would document why and the reasons and how this links to the legislation.

Mr DREYFUS: Again, I imagine you will say we should ask the agencies how much time an authorised officer then typically would take to consider a request like that.

Mr Hansford: Yes.

Mr DREYFUS: How much information would an authorised officer be required to look at?

Mr Hansford: Again, I think it would depend on the agency, but I understand that agencies have forms that give you a sense of how the agency has complied with the legislation, through their internal governance mechanisms.

Mr DREYFUS: So, the forms would give us some indication?

Mr Hansford: Indeed.

Mr DREYFUS: But there's no prescribed process. It's just a requirement that it be an authorised officer making the authorisation?

Mr Hansford: Yes.

Mr DREYFUS: Are there uniform national guidelines or policies that set out—by way of example, the matter you have referred to—when it will be reasonably necessary to authorise the release of telecommunications data?

Mr Hansford: No, but we do run a national consultative mechanism where we discuss the implementation of the TIA Act—how it's working in operation and what are some of the key issues. But in answer to your question about whether there is a national guideline, the answer is no.

Mr DREYFUS: I think it's probably fair to say that in the absence of some uniform guidance, some kind of checking process by any other person, let alone a judge, it would be a highly subjective criterion—that is, what is reasonably necessary?

Mr Hansford: It would depend on the individual investigation and the individual agency's remit. I might also point out the role of the ombudsman, in particular, and their commentary about the individual processes and whether or not agencies have complied with both the law—and they do make comments on the government's arrangements as well. The point of our evidence is that the act stands. There is no uniform national guidance but

we do have a national consultative process. Agencies have their individual governance arrangements, including forms, and then the ombudsman, or the IGIS in the case of ASIO, looks over the regime. I think that is, from start to finish, how we envisage the implementation.

Mr DREYFUS: Is there any way of determining whether or not the criteria, and particularly this reasonably necessary criterion, are applied consistently by authorised officers across Australia?

Mr Hansford: Short of the ombudsman's role, there is no particular mechanism to determine consistency across Australia, except, of course, where the courts have made decisions based on a whole investigation.

Mr DREYFUS: That's a good example. If I could go to another matter, which is the matter of pecuniary penalties—a number of submitters have expressed concern to the committee that section 179 allows authorisations for telecommunications data to be made available for the purpose of enforcing a law, imposing a pecuniary penalty or for the protection of public revenue. You've defended that position at paragraph 98 of your first submission, and you've emphasised the actions taken by ASIC and the ACCC, the Australian Competition and Consumer Commission, in investigating insider trading offences, for example. How many times did the ACCC authorise the use of metadata in 2018-19?

Mr TIM WILSON: I point out, just for clarity, I've already asked for that data, if they don't have it at present.

Mr Hansford: In 2018-19, the ACCC asked 108 times for data, as I understand—at table 39. And then, to break that down even further, eight of those requests were for zero to three months and 17 were for three to six months et cetera. The information I think is on table 39, which gives a breakdown, as well as the breakdown at a higher level on page 71, table 40—subscriber data 60, 48 traffic data for the ACCC in 2018-19.

Mr DREYFUS: I'm trying to get at the ones where the ACCC has authorised data for the purposes of imposing a pecuniary penalty.

Mr Hansford: The closest we get in terms of offences is table 35, which—99 cartel offences and one fraud. But if the particular question is imposition of a pecuniary penalty, we will talk to the ACCC and see if they have further information. Because what I don't know is whether or not any of the cartel offences relate to the imposition also of a pecuniary penalty and whether or not it's just not the straight offence—what the fraud offence relates to, the balance of the 100 offences that have been outlined, its relationship, then, to table 40 on page 71 and the relationship to 108. I wouldn't want to say that the difference is eight because I just don't know the categories.

Mr DREYFUS: What about ASIC? Can we tell, from the table, how many times ASIC has used these powers for the purpose of enforcing a law or imposing a pecuniary penalty?

Mr Hansford: Sorry—table 37 is offences against which authorisations were made for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue. Actually, I can answer the previous question. For the ACCC, the pecuniary penalty was eight. Eight in 2018-19 and for ASIC—

Mr DREYFUS: This is my fault too, I'm afraid. So this is table 37 of the annual report?

Mr Hansford: Table 37—yes. It has a category: 'pecuniary penalties'. So there were eight for the ACCC, four for the AFP, none for ASIC, 19 for Home Affairs, 59 for New South Wales police, 25 for TASPOL and three for WAPOL, WA police. So, according to this table, there were offences relating to a pecuniary penalty 118 times.

Mr DREYFUS: So just on this point about ASIC and the ACCC, it's fair to say that ASIC and the ACCC account for a tiny fraction of the total number of authorisations.

Mr Warnes: Yes.

Mr Hansford: Yes.

Mr DREYFUS: At paragraph 98 of your submission, you've also noted that police agencies use the provisions to prove traffic infringements. Can you point me to the table we would look at in the annual report as to how many times powers have been used by police agencies for traffic infringements?

Mr Hansford: In table 37, the last column there is 'traffic'. The answer to the question is one for Northern Territory and 38 times for New South Wales police, with a total of 39 for the 2018-19 period.

Mr DREYFUS: And for some police forces not at all?

Mr Hansford: Two in the 2018-19 period.

Mr DREYFUS: Just to go back then, could I ask you a couple more questions about prospective data authorisations, a different type of authorisation. Under section 180, an authorised officer of a criminal law enforcement agency can authorise the disclosure of prospective telecommunications data—that's into the future, obviously, not historical—if they're satisfied that it's reasonably necessary for the investigation of a serious

offence or an offence under a Commonwealth, state or territory law that's punishable by imprisonment for at least three years. Have I got that right?

Mr Hansford: Yes.

Mr DREYFUS: And in 2018-19, the last available year, there were 27,824 prospective data authorisations made?

Mr Hansford: Yes.

Mr DREYFUS: As I said, a prospective data authorisation gives an agency access to data that comes into existence in the future, during the period of time that the authorisation is enforced for.

Mr Hansford: Indeed, and because it's prospective it's a higher threshold.

Mr DREYFUS: Just at a practical level, when an authorisation is in force does it mean that a provider will release new data to an agency every day or every week, or is it only upon request? How does it work in practice?

Mr Hansford: I think that would depend on the investigation. I will check with some of our agencies as to how it's operationalised, but I think it would be an agreement with the telecommunications provider. That might be, for a particularly intense investigation, when something has changed, or it might be a particular agreed date, noting that law enforcement agencies routinely pay for prospective data authorisations.

Mr DREYFUS: Yes, so could you let us know about that. You don't need to obtain a warrant to make one of these prospective data authorisations?

Mr Hansford: No.

Mr DREYFUS: Again, as with the previous questions about individuals, is there any way of judging or estimating how many individuals those 27,824 prospective data authorisations relate to?

Mr Hansford: No, I think the biggest breakdown we've got is in table 33, which gives you the number, the days in force, the actual days in force and then how many were discounted.

Mr DREYFUS: Is it more likely, given that these are prospective, that each would relate to an individual? Perhaps that's something you could take on notice and ask for some more information on.

Mr Hansford: Because of the higher threshold and the fact that the other information includes subscriber checks, particularly in the first zero to three months, or zero days as some agencies define it, I think it is more likely that this would relate to individuals, but I wouldn't want to give you the answer that there are 27,824 individuals. As before, we'll take it on notice to try and give you a sense about whether or not prospective data authorisations are more likely to relate to an individual, comparative to the other requests for telecommunications data.

Mr DREYFUS: Thank you. Do you know how many of the individuals in respect of whom any prospective data authorisation was made were ultimately charged with committing a criminal offence?

Mr Hansford: No.

Mr DREYFUS: Or how many of these individuals were ultimately ruled out from suspicion?

Mr Hansford: No.

Mr DREYFUS: There's one question that is probably within the department's direct knowledge. That table 33 tells us that the Department of Home Affairs itself used a prospective data authorisation 225 times in 2018-19. What were those powers used for, in those 225 cases?

Mr Hansford: I'll have to check what the powers were used for, but for the Australian Border Force, which is for all intents and purposes part of the Department of Home Affairs, it would likely be in relation to enforcement of the Customs Act. I will check if we've got any more information about the breakdown, but I routinely speak to ADF officers and it's the enforcement of the Customs Act.

Mr DREYFUS: Yes, if you could let us know. All the questions are directed to getting a feel for how this scheme works in practice. Lastly, I'll just turn to something that intersects with our press freedom inquiry, because there's quite a lot of intersection, as you would appreciate, between the press freedom inquiry and this inquiry. As you know on 13 December 2019 this committee announced publicly that it had effectively put its press freedom inquiry on hold while we waited for a further submission from the Department of Home Affairs and the Australian Federal Police, which your department said was coming, Mr Hansford.

Mr Hansford: Yes.

Mr DREYFUS: Yesterday the committee received the long awaited supplementary submission on press freedom. I have it here. It runs to six pages, although it's actually only about 3½ pages of text. It makes only one

very modest suggestion for further consideration. I wonder if you could tell me, why did it take almost three months for the department and the Australian Federal Police to lodge a submission which runs to 3½ pages of text?

Mr Hansford: The balance of evidence before the press freedom inquiry from some individual organisations was promoting the concept of a contested warrant. It took us some time to work with the Australian Federal Police to explore what a contested warrant would look like. You pointed us, I think, in your questions at the press freedom inquiry to the design of the UK regime. We looked in depth at the UK regime. We also worked with the AFP about—if the committee was minded to make a recommendation about a notice to produce regime, which is outlined in the submission, as opposed to a contested warrant regime—what that would look like, the impact it may have on the Australian Federal Police, what the policy considerations are. Obviously there was a range of discussions and it took a lot of deliberation to come up with a potential option for the committee to consider. That is why it took some time to develop.

Mr DREYFUS: When did you complete the submission?

Mr Hansford: Well, the submission was tabled yesterday.

Mr DREYFUS: No. When did you complete it? I know it was delivered to the committee and made public by you yesterday, but when did you complete it?

Mr Hansford: We've been reiterating the draft for some time. I formally signed off on a submission to the minister and he signed it on the same day.

Mr DREYFUS: What prompts my question is that on page 4 of the press freedom submission, which is actually the second page of text, you wrote:

The Australian Federal Police Commissioner has also commissioned Mr John Lawler AM, APM to undertake an independent review of the conduct of sensitive investigations in the Australian Federal Police—

and then I will emphasise this—

(expected to report in January 2020), to further strengthen policy and practice regarding such investigations.

That language 'expected to report in January 2020' suggests that this submission was actually completed before January 2020. Have you been sitting on this submission for at least two months?

Mr Hansford: No, I think we've been reiterating the submission and looking at it for a number of months, having lots of conversations with a whole range of people. That sentence in there is an oversight on our behalf and we should have made it more contemporary.

Mr DREYFUS: So you care so much for press freedom and the committee's inquiry on press freedom that you can't even be bothered taking out a sentence which was obviously written in December 2019, or maybe November 2019 for all I know. You also can't be bothered telling this committee anything about John Lawler's report which was made public on 14 February and given to the commissioner, as I understand it on 17 January. Is that reflective of the department and the government's attitude towards press freedom or this committee?

Mr Hansford: I think the balance of the joint submission between the AFP and Home Affairs is to articulate the notice to produce scheme and how that might operationalise.

Mr DREYFUS: That's the one modest suggestion you make.

Mr Hansford: In addition to that, the Australian Federal Police commissioner has provided the committee with a copy of the Lawler review in its entirety and has made that public and made comments on it. So those are the two pieces of evidence I would like to give you.

Mr DREYFUS: Who made the decision to delay providing a submission to this committee on press freedom?

Mr Hansford: I think we've been iterating the submission for some time on the issues and making sure that a whole range of parties are consulted in the process, from Attorney-General's to the Federal Police to ourselves, to make sure that the suggestion would be both helpful to the committee and something that was practical.

Mr DREYFUS: Who's been involved in this iterating since last December?

Mr Hansford: I'll have to take that on notice.

Mr DREYFUS: It's your area, Mr Hansford.

Mr Hansford: Yes, I've given you—

Mr DREYFUS: Why do you have to take on notice telling me now who was involved? Which departments and which ministers were involved in taking three months to give us 3½ pages of further text when the whole

committee has delayed the conclusion of its inquiry awaiting these 3½ pages of text? Who was involved, Mr Hansford?

Mr Hansford: The Department of Home Affairs and the Australian Federal Police co-wrote the draft. They consulted with a range of different individuals.

Mr DREYFUS: Who were they?

Mr Hansford: Particularly the Attorney-General's Department.

Mr DREYFUS: And?

Mr Hansford: I'll have to refresh my memory on the range of people we consulted, and I'll provide it to you on notice.

Mr DREYFUS: Was the minister's office involved?

Mr Hansford: The minister noted the submission.

Mr DREYFUS: The minister's office was involved. Is that a yes?

Senator KENEALLY: Were they part of the iterating?

Mr Hansford: We've had discussions with the minister's office.

Mr DREYFUS: And the Attorney-General?

Mr Hansford: I haven't had any discussions with the Attorney, but I'll take it on notice to try and get you a precise answer as to who was consulted.

CHAIR: Mr Dreyfus, in the interests of time, I think that, on this line of questioning, we'll get another opportunity in the hearings on press freedom.

Mr DREYFUS: You've taken it on notice. I'm looking for you to explain why it is there's been a delay of nearly three months in the provision of 3½ pages of further text with one very modest suggestion being offered up to this committee, given the significance that the department put—which, indeed, the committee accepted it should have—on the making of a further submission.

Senator KENEALLY: I'd like to turn to a matter related to Mr Dreyfus's line of questioning but more specifically in relation to the CLOUD Act. It is my understanding that the United States CLOUD Act requires that jurisdictions with which they form agreements must have in place an independent authorisation for requests for data that would go to the US under the CLOUD Act agreement. Could you advise this committee as to the current metadata process—the very laws that we are reviewing right now—and whether or not, in your view, that process conforms under the CLOUD Act or whether we would need to consider any changes to the access to metadata under the T(IA) Act in order to conform with the CLOUD Act?

Mr Warnes: Thank you, Senator Keneally. It's a good question. I can't go into too much detail, because there are current negotiations on foot with the United States. What I can tell the committee is that you're absolutely correct: orders sent under the CLOUD Act need to be judicially authorised. However, that is in relation to content, mainly. Subscriber data is generally dealt with differently and at a different level. I'd point you to the United Kingdom agreement, which essentially carves out subscriber data. I'm not saying that's what the Australian agreement will do, but you can see that another jurisdiction that has dealt with this has carved out this sort of subscriber data to deal with that separately. Any orders for content that go under the CLOUD Act do need to be independently authorised.

Senator KENEALLY: I appreciate that answer, Mr Warnes. We've had some evidence before this review, particularly that of the Ombudsman, that some of the information that is provided under metadata access can communicate content. This may be an issue that gets ventilated under the negotiation. I am curious as to whether the department has turned its mind to that evidence from the Ombudsman and how that might be dealt with under a possible CLOUD Act agreement—if that introduces any further consideration.

Mr Warnes: We certainly took note of that evidence from the Ombudsman, Senator. But what I would say in relation to your question is that the data authorisation regime does not allow content to be accessed. Those authorisations that sit—and I won't bore you with the subsections—in the TIA Act in relation to metadata don't allow for content to be passed. It is for data or metadata, not for content.

Senator KENEALLY: Are you suggesting the Ombudsman's evidence is not accurate or—

Mr Warnes: No. What I'm suggesting is it depends on how that came about. So, if an agency hypothetically asked for a data authorisation and got back content, that is an issue, but that's not an issue with the regime; that is an issue about what has been provided in response to a request.

Senator KENEALLY: My understanding of the Ombudsman's evidence is that some data can inadvertently reveal content. Some of the data that providers are required to retain can, nonetheless, inadvertently reveal content.

Mr Warnes: Providers are not required to obtain, for example, any web browsing history. There can be a little bit of trickiness with IP addresses, for example. Google, the web site, has an IP address. So, if you reveal a Google search in the IP address associated with that, that could be content because you could be showing what someone was browsing. That's very clearly out of the regime. But, if you want to know the IP address of my phone, for example, when I'm communicating with someone, that is not content; that's just the location of my phone on the network—the address of the phone. That is data. An IP address can be both but not under the regime, if that makes sense.

Senator KENEALLY: It does. That is a very helpful answer. Thank you, Mr Warnes.

Mr Warnes: Not a problem.

CHAIR: Before we wrap up, there are no submissions from local government associations who might use 280. Is there a reason why? And is it possible for you to solicit some submissions from interested organisations, if indeed they see this as a necessary part of their work?

Ms McNeill: We will take that on notice, if we may.

CHAIR: Sure.

Mr DREYFUS: This is about web browsing history. The Commonwealth Ombudsman has told the committee that carriers have provided agencies with the web browsing histories of individuals and that's despite the fact that 187A(4) makes it very clear that service providers are not required to retain information about a person's web browsing history. Are you able to explain to the committee why and how such information has been provided to agencies? Is it that the legislation doesn't require the information to be retained, but that doesn't prohibit disclosure of the information either? I'm just trying to get at how this happened.

Mr Warnes: I'm not familiar with the circumstances. I think you would have to ask the Ombudsman about exactly how it happened, in terms of their investigation. What I can tell you from the legislation—

Mr DREYFUS: I suppose I am trying to get to how, theoretically, it might have happened and am asking you to speculate. One of the things this committee may choose to do is make a recommendation about how the legislation ought to be amended to make sure this doesn't happen. I can't speak for the other members of the committee, but our position certainly was, in 2015, that web browsing histories ought not be provided.

Mr Warnes: My answer to the committee is that it shouldn't be disclosed, as far as I'm aware, as content. It's very clearly ruled, both what's required to be retained and what can be authorised under the authorisation provisions. Any content should be sought under a stored communications warrant. That's what a stored communications warrant is for. Web browsing history has been clearly set down by parliament as content. There's another mechanism to get content, and that is a judicially authorised mechanism that, as you know, Mr Dreyfus, has a serious offence threshold.

Mr DREYFUS: Last question—three questions maybe—what do enforcement agencies do when the carriers do provide web browsing information? Do they use it, do they delete it and can you find out for us?

Mr Warnes: I think you would have to ask the enforcement agencies. I'm happy to take it on notice.

Mr DREYFUS: If you could—it is not so much the specifics. Obviously if you could tell us how many times this has happened that would be of interest but it is more, 'Is there a process?' The agencies know they're not meant to get it. I'm not doubting their bona fides at all; I am just trying to find out what happens. Should there be a process? Should there be a provision in the legislation?

Mr Warnes: I'm happy to take it on notice. Normally in a general sense when information is sought under the TIA Act, whether it is no longer authorised or incorrectly authorised—a range of things can mean data has been got that shouldn't have been—it is usually quarantined and not used. If it needs to be sought it can be re-sought under the appropriate authority. That is generally what will happen but I'm take on notice and ask the agencies.

Mr DREYFUS: I have no more questions. I was critical before about the press freedom submission and I've been critical in the past about the quality of submissions from the Department of Home Affairs but I want to be complimentary about the three submissions on this occasion for this inquiry into the data retention scheme. The submissions have been actually excellent and full and I hope it continues. Thank you very much.

Mr Warnes: Thank you, Mr Dreyfus. We'll pass that back to the teams. They'll appreciate that.

CHAIR: That ended nicely. Thank you very much for your attendance here today. You'll get a copy of the transcript so you can make corrections. If you could get answers to questions on notice to the secretariat by 20 March, 5 pm, that would be appreciated. We'll suspend for 15 minutes.

Proceedings suspended from 10:36 to 10:51

BURGESS, Mr Mike, Director-General, Australian Security Intelligence Organisation**VICKERY, Mr Peter, Deputy Director-General, Enterprise Service Delivery, Australian Security Intelligence Organisation**

CHAIR: I now welcome representatives of the Australian Security Intelligence Organisation to give evidence. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. Director-General, I now invite you to make an opening statement before we proceed to discussion.

Mr Burgess: Thank you for the opportunity to appear before the committee today. I'm on the public record this week outlining the threats to security we face, so in summary: the threat of terrorism at home remains probable, and the espionage and foreign interference threat is unprecedented. The threats we face drive what ASIO do, and the environment in which we operate influences what we do.

Since the early nineties, communication technologies have helped drive significant change to our lifestyles and our economy. Technology and connectivity are now more vital than ever. Services built on these technologies are nothing short of crucial, and it's not an exaggeration to say that a mature 5G network will be the nervous system of our economy, connecting and enabling its vital systems—the health system, energy system, finance system and so on. While these changes are undeniably positive, they also have a profound impact on organisations such as ASIO. This is a problem we continue to deal with.

The practical experience of this is that access to communications, the kind of access that existed until the late nineties in terms of both historical data and real-time communications afforded by interception, has diminished in the 21st century. Information about communications exists or is accessible only for some services at some times and in some places. Intelligence and law enforcement agencies have referred to this as going dark, and one response by government was the introduction of the mandatory data retention regime. This regime was intended to ensure that agencies had access to at least a minimum set of retained data for a minimum period in an environment where business models were and remain on the cusp of moving entirely to billing by bandwidth and volume, keeping no record of individual communications at a transactional level.

The kind of information that can be retained by carriers and carriage service providers is necessarily limited. For example, carriers and carriage service providers keep no record of the communication applications running on the top of the internet services they offer such as WhatsApp or Skype. All they retain is a record of providing the internet access service and no record of communications. Leaving mobile networks altogether, the records retained when devices access wi-fi are often less complete again. Agencies piece together fragments of records of communications to glean the insights that are of value in progressing our investigations, such as a time, a location, the details of a service, a partial network of contacts, an IP address, the subscriber's details—effectively, the traces of communications that carriers and carriage service providers have visibility of.

I understand the impression that, with so much data being transmitted and collected around the world, the retention of data is somehow more intrusive now than in the past. In aggregate, across all private sector collection, this is true. However, the degree of intrusiveness is simply not present in the datasets provided by carriers and carriage service providers, be it from slightly broader available datasets they keep on their business systems or the more basic datasets they retain under the data retention legislation. And yet this limited fragmented information provided to us through the data retention regime is critical to the majority of our investigations. Records of communications may be the only intelligence that we have available to identify terrorist networks and conspiracies or to identify hostile foreign intelligence services seeking to do harm to Australia's interests. To develop further investigative leads we need access to retain data.

Let me give you an example of how retained data has helped ASIO, as noted in our unclassified supplementary submission to the committee. We received information about a visiting scientist undertaking clandestine intelligence activity on behalf of a foreign government. For over 10 years the scientist had access to Australian government clearance holders, people with access to Australian government secrets. Thanks to retained data, we managed to identify some of the scientist's contacts for some of the time they were in Australia. From that information we were then able to investigate the harm the scientist caused to Australia, specifically their access to classified material over the previous 10 years. This is just one example of many, noting that retained data is used in most of our investigations. It is the bedrock for furthering our investigations and it is critical to our operations.

I conclude on two important statements: ASIO seeks access to retain data or telecommunications data only in connection with the performance of our functions, and reduced access to retained data could significantly degrade

ASIO's investigations into terrorism, espionage and foreign interference. Thank you. I welcome questions from the committee.

CHAIR: Thank you. If I could turn to oversight of ASIO access to telecommunications data, which is paragraphs 29 to 31 in your submission. This committee is well aware of the rigour applied by the inspector-general in her oversight role of the intelligence agencies. Could you reassure the Australian community of the rigour that's applied to ASIO?

Mr Burgess: Absolutely. The Inspector-General of Intelligence and Security is an important part of our oversight. The IGIS, as we refer to her position and her office, has standing powers akin to a royal commission. She has full access to everything we do. We can keep no secrets from her and her staff. Her staff have full access to all of our records. They conduct regular inspection regimes. Yes, as published in the Inspector-General of Intelligence and Security's unclassified report, from time to time they do find issues; that's a matter of public record. We respond to those. Where the IGIS makes recommendations that we need to fix something, we generally, if not always, take that on board and do what she asks us to do. It's a very important part of the oversight of what we do, important in our licence to operate to ensure the public have confidence, that we do act legally and ethically, and if we don't inadvertently that is dealt with swiftly.

CHAIR: I wanted to make that point up-front because in your submission you write that a longer retention period of metadata can greatly assist ASIO's ability to manage the threats of terrorism, espionage and foreign interference. It's important that the Australian public be reassured that it's in the context of very rigorous oversight that you're advocating such a position.

Mr Burgess: Correct.

CHAIR: On that point—and you've given us some helpful case studies in the unclassified supplementary submission—almost two years ago we passed the espionage and foreign interference legislation. Mr Vickery was on the record then in the hearing saying that espionage and foreign interference has been conducted on an unprecedented scale in this country. You said so yourself on Monday during your speech. How important is metadata to prosecuting foreign interference or espionage? Indeed, we're yet to see a prosecution in this country. Can you talk a bit about the importance of metadata?

Mr Burgess: Absolutely. As we've said in our submission, and as I said in my opening statement, access to retained data is absolutely critical in enabling ASIO to identify areas where terrorism, foreign interference or espionage is occurring. In terms of leads generation, it is absolutely critical for us as we go about our work to identify those security threats. It is a significant part of that. Without that, we would be considerably hamstrung.

Of course, it's not the only thing. The important thing to remember here is this is a minimum set of retained data. It is not about the content of communications; it is about the fact that there might be some service being provided, or some communications between devices and therefore people, which leads us to investigate. As we step-up our escalated investigations, where we call on some of our powers and we get to the warrant point of view where, under warrant, we access content, it is critically important for us.

In terms of prosecution, the mere fact of devices communicating may or may not be part of the evidence that is used in any prosecution case but it's absolutely critical in our leads generation. I can assure the committee that the passing of that legislation has had an effect. We've seen tradecraft change. I can assure the committee that we are working hard on a number of cases with the Australian Federal Police. Obviously, prosecution isn't a matter for me as the director-general of security, but we are working very hard on that and it is our intention to move cases through to that.

CHAIR: Thank you. You also mentioned on Monday night a sleeper that ASIO disrupted. With only two years of metadata, we can never really know the extent of the network over however long that sleeper had been operating in Australia, nor indeed the potential damage to our national interest. Is that a fair comment?

Mr Burgess: Absolutely. It's a challenge we face, of course, in the balance between privacy and security. From an ASIO perspective, we've accepted the two-year period. But I would have a strong case for why more than two years, for ASIO at least, would be relevant. I think our case study, the one I spoke about in my opening statement, highlights the fact that that was an activity that went back 10 years. Fortunately, we were able to access some data further than the two-year period. That assisted us, but the legal requirement is that it be retained for two years. That is the obligation on the carriers. We have accepted that, but I guess I could argue for more.

CHAIR: So fleshing out a historical spy network, for example, would be difficult with the current constraints—noting, of course, that they are put in place for a reason.

Mr Burgess: Sure, it would be very difficult. In the case of some of the examples we have given you, the retained data has helped us and been instrumental in the leads generation, which then helps us to unpick what was happening. It's absolutely critical.

Senator FAWCETT: I have a question around the issue of retained data versus data that telcos have traditionally kept—and many still do keep—for seven years or more. In 2015, when this committee was originally considering metadata, there was a concern expressed that, once there was a two-year retention threshold, telcos would start reducing those longer holdings towards that. Have you seen any evidence that telcos, who you traditionally knew would have certain data for up to five or seven years, are now reducing that period? Or, in your experience, are most of those who have kept that data still retaining it for that five or seven years?

Mr Burgess: I will see if my team can give me a bit extra here. From my experience so far, having been in the job for five months—and obviously I had experience with this when I was at Telstra—this legislation has been effective in enabling all the carriers we deal with to retain the minimum set of data. That has been absolutely critical. Yes, there are cases where carriers are making decisions, and had made decisions previously, to retain data and that has been beneficial to us. I'm not aware of any degradation in capability that we had previously. I would suggest that the capability available to us has improved as a result of the legislation.

Senator FAWCETT: I understand that. Where I'm going with the question is that there is an inference in many of the submissions from agencies—a specific one in yours—that extending the period of the retention may be beneficial. What I'm hearing, and in some of the case examples, is that it's almost pot luck at the moment if you have—one of the case examples you give in the unclassified piece is around foreign espionage, or people here in Australia, and it's almost pot luck if somebody happened to have something going back five or seven years where you can track that pattern of life and relationships.

My concern is that if those things are important and we are seeing people reduce their data holdings down to two years then we perhaps need to look at ways to increase the mandatory retention of data, if the serious cases around terrorism and foreign espionage et cetera are the cases where you need that longer data. So if people are still retaining seven years of data it's not so urgent; if they are reducing it then that gives an added impetus to look at how we increase that.

Mr Burgess: Certainly. I might ask Mr Vickery—

Mr Vickery: All I was going to add there was that in our experience the bigger, more traditional providers, if you like, that we've dealt with for many years are the ones that are more likely to keep the data for longer, but in the current environment, with newer providers popping up with less infrastructure—it's probably those providers that keep it for the minimum period, but not for any longer, probably for purely business reasons on their part.

Senator FAWCETT: If we were to increase the period for the mandatory retention of data, bearing in mind there are two discrete sets of data—one set under the TIA, which is mandated, and the broader data that people keep—one of the concerns raised by civil society has been that there needs to be a balancing provision around privacy. The evidence that we have seen from Home Affairs, and also I think from your submission, is that the requests which tend to go beyond 12 months, in terms of the age of data, tend to be for the more serious crimes or incidents. So, if we were to mandate a retention of data beyond two years, would it be a reasonable balance to say that you would need to get a higher level of authorisation, perhaps even a warrant, to access data going back that far, while still keeping up to two years warrant free as it currently is?

Mr Burgess: From ASIO's perspective, the access to retained data is incredibly important in the case study I gave. I appreciate the fact that we don't need a warrant to get subscriber information or the minimum data. I would perhaps disagree with those who think there are privacy breaches in that. The fact that an IP address was given to a customer; that's an IP address. The fact that in the old traditional telephone sense, which still exists today, barely—the fact that someone was calling someone is not giving too much away; it's not access to content. Of course, I recognise there's the IP address assigned versus the URL or the web surfing history. From ASIO's point of view, that's not in play here; that's not retained data. Our policy is that whenever we get access to web surfing history a warrant has to be in place for us to receive that data. In our data and subscriber checks, where carriers give us that data because they believe it is okay, we delete it and report it to the inspector-general. We will only get that when a warrant is in place.

I could argue a strong case for further retained data—but, given the number of requests you see that we're doing for this, if there were warrants in place—because I would deem most of our inquiries, even if they're initial leads, to be serious investigations. But, again, I'll be guided by the committee and the parliament in terms of what requirements you put on us.

Senator FAWCETT: For clarity, my reading of the submission is that having a guaranteed set of data for longer than the two years would assist you in getting early leads in some of the most serious cases that you look at.

Mr Burgess: That's correct, and we have a strong argument for an extension of two years.

Senator KENEALLY: I would like to follow up on that particular point. Home Affairs were here just prior to your evidence. They made clear to us they were not recommending a period of retention beyond two years. I appreciate that the advice you are giving us is that you would welcome a retention period beyond two years in terms of the serious crimes and threats that we face. To follow on from Senator Fawcett's questions: you just spoke about the type of data that's retained, saying it may not reveal a great deal beyond what had previously been revealed—that a phone call took place. However, one of the concerns of this committee relates to the access of data by agencies under the Telecommunications Act, section 280, which goes well beyond what this committee and the parliament were asked to consider when we passed the amendments to the TIA Act requiring the mandatory retention of data. At that time we were told that it was going to be for 20 agencies, such as yours, that investigate these serious crimes and terrorist threats. We've now had evidence in this review that agencies like the RSPCA and the institute of teachers and local governments are accessing metadata under the Telecommunications Act, particularly under the provision to protect public revenue.

So, let's turn our minds to your suggestion that we should extend the data retention. Recognising that the data retained is far greater than simply that a phone call occurred—because the reality is, since state governments gave agencies the ability to access this information of the Telecommunications Act, communications have changed dramatically and metadata reveals a great deal more than just that a phone call occurred—have you thought about how we protect the privacy of individuals in a circumstance where agencies beyond the original 20 that were proposed to us are getting access to this data? In particular, if we're going to extend the data retention period, are there safeguards we could put around it to ensure that it is being used for the most serious crimes and terrorist threats? As Senator Fawcett suggested, is a warrant one possible way to do it? Are there some other limitations? Speaking for myself and noting some of the concerns aired earlier, I think the committee does have concerns about the relatively low-level offences that are being investigated or prosecuted by using the metadata that is now available.

Senator FAWCETT: Could I just clarify that I didn't suggest a warrant as a way of limiting councils and things. That was only for agencies in two years-plus type data.

Senator KENEALLY: My point is that perhaps a warrant would limit councils, if you had a warrant for two years plus. It would curb their ability.

Mr BYRNE: Could I make it starker for you, Director-General: how do you feel about the RSPCA accessing the same information that ASIO does?

Mr Burgess: As a private citizen, I share the committee's concern. As the director-general of security, I actually share your concern. I think all of us who are enabled under this law to get access to retain data should argue why we need it. I can speak for ASIO; I can't speak for the RSPCA. As I said, I remember the conversations at the time. I was working at Telstra at the time, and it's a matter that we raised in terms of: 'This doesn't make sense; there are too many people, on the face of it, that seem to have access to this.' I understand that concern, but I will refrain from further comments in that regard. I believe I have a very strong case for why ASIO needs it. Perhaps everyone else who can legally access it should put their own cases forward so they can be judged by the committee and the parliament.

Senator KENEALLY: But isn't it a question for this committee to consider? If we grant an extension of time because ASIO may have a very good case for it, we also have to consider who else then might have access to a longer and greater store of data and whether or not that's appropriate.

Mr Burgess: I agree with you, Senator. So I can be clear on this: in responding to questions, I can argue, I have not yet asked my minister or the Home Affairs portfolio of the department to press ahead on this. The reason I have is: we have other needs that we're focusing on. At the moment what we have is working for us. Could ASIO use a longer period of the retained data? Yes, we could. I have a strong case, but we have not yet put that forward to government to say that's something I would like my minister and the government to consider.

Mr TIM WILSON: To pick up on that point, briefly, Chair. Director-General, there are principally two concerns: there's obviously the concern around the fact that, say, the RSPCA is accessing people's metadata for a particular purpose, even if it is justified, that hasn't been present. I think the other concern from many of the committee members is that, because they were able to do that, in comparison to the crimes or the investigations

that ASIO is doing itself, it's undermining the—let's use the term—social licence for you to be able to access that information. Do you share that concern?

Mr Burgess: I do share that concern.

Mr BYRNE: Well put, Mr Wilson, if I may say so. Director-General, I noted with a great degree of interest you said that the access to retained data that you wanted to keep the specific dataset and that drew my attention to part 4 of your supplementary submission that you provided to this committee: offshoring of data, which has been another long-held concern of mine. If I may, Director-General, quote from your submission:

Offshoring of data is part of a broader discussion around 'data sovereignty' and comes with a broad set of concerns around commercial, regulatory and security threats to data access, integrity and use.

Then section part 22 says:

In practice, storing data offshore removes Australian data—including sensitive data about Australians—from the full protections afforded by Australian law and Australian Privacy Principles. Even where offshored data is held securely, it is in a foreign jurisdiction and subject to the laws of that jurisdiction. Significant concerns, especially for sensitive information, arise in the contexts of access, privacy and security. The offshoring of data can also prevent the forensic examination of compromises by Australian authorities.

The question I have for you is—and I fully endorse that, I might point out; and you noted further in this submission that there are other countries that are moving to bring data onshore—what's ASIO's understanding of how much data is stored offshore?

Mr Burgess: Thank you for the question. You're right: that is a very important point here and one that was discussed as the legislation was first debated as well. So, it is of real concern for me, for us, for government—the way in which carriage and carriage service providers are managing these risks and protecting the data they hold of their customers for their own business purposes that are relevant to law enforcement and security agencies. There is the telecommunications sector security reform legislation that is actually an effective mechanism by which that engagement between government and the telcos is occurring. On that basis, I'm confident that the right attention is being applied to the way that these companies are retaining the set they're required to under law. It's something we will continue to have under review because we recognise the pressures that businesses have when it comes to their business arrangements and their outsourcing arrangements, and how they maximise value for their shareholders and reduce the costs of running a business. That is incredibly important to us.

The other way of course we look at this is: I'm the Director-General of Security and I'm constantly saying, as is my organisation, that this retained dataset is useful for our investigative purposes, which means it is valuable information, which means it is also valuable to others, such as foreign intelligence services or criminals. They would be able to use it and, whilst if you move data offshore, necessarily the data isn't more secure just because it's on Australian soil; it depends on the measures you put around it. Of course, what you don't have on Australian soil is the protection of Australian law, our privacy principles and everything that goes with that. The data is attractive here, but there are some more protections you can have by knowing where it is, who has access to it, who's protecting it and how well it's protected. When it moves offshore in some supplier or contractor, you've got to keep an eye on that ball and that is an issue that we continue to be concerned about.

Mr BYRNE: Does ASIO know how much data is stored offshore?

Mr Burgess: I don't know. We could take that question on notice.

Mr BYRNE: It's been put to me in a TSSR hearing—let me ask you the question another way: are telecommunications companies compelled by law to advise you about how much data is stored offshore?

Mr Burgess: To my knowledge they're not required to inform ASIO of that. My team might advise me if there's a requirement. I can say, though, that under the telecommunications sector security reform legislation, when they make major changes in how they're implementing telecommunications they have to advise government for security purposes. That's a way in which we can pick up anything that might be problematic from a security point of view, which is the purpose of the legislation.

Mr BYRNE: Without putting words in your mouth, it would be hard for ASIO to determine how much of this data is kept offshore?

Mr Burgess: Well, hard—we would ask the providers we deal with when we're doing the exchange.

Mr BYRNE: Has that been asked for before and not provided?

Mr Burgess: I'm not aware of that. We don't administer telecommunications sector security reform.

Mr BYRNE: To summarise briefly: I'm aware of the fact that there is a lot of data, including metadata, that's stored offshore. Reading your preference, it would be, as a number of other European countries have been doing,

to bring this data that might be offshore back onshore, to maximise its potential to keep it secure and under Australian law.

Mr Burgess: My preference would be for this retained data to be onshore, yes.

Senator KENEALLY: I have another set of questions regarding the internet of things, which your submission also provides some information on. The Department of Home Affairs gave evidence that at this time they are not recommending that the mandatory data retention scheme be expanded to include the internet of things, but they are considering what if any expansion of retained data should occur in the legislation. In your submission you have made some comment as to the usefulness of being able to use data that's either over-the-top data or the machine-to-machine communication. Have you been able to provide any advice through to government? Are you making any specific recommendations for this committee to consider in our review of the TIA Act?

Mr Burgess: We constantly talk about this across the Home Affairs portfolio. I'm not aware of any advice. My position on this would be that the advances in technology—the internet of things is just the reality that the networks are so capable that machine-to-machine communications are going to grow, for a whole range of good, positive reasons. The introduction of 5G will enable machine-to-machine at a scale we've not seen before. Therefore we keep an open mind as to what that means in the reality of things that can allow us to identify espionage. In that context, espionage is not just people. People can be using machines. So at this stage we're not asking for anything in this regard. I think it's too early to say. We flag this and 5G in our submission because it's something we have to keep an eye on. Technology changes all the time. At this point in time we're not asking for additions to retained data. We keep an open mind to that.

Mr DREYFUS: Can you confirm that there's no legal requirement for ASIO to destroy datasets that are no longer in use?

Mr Burgess: That is correct.

Mr DREYFUS: This comes up because the IGIS raised something about this. In ASIO's view, what would constitute an appropriate destruction regime?

Mr Burgess: It's correct that we do not have to destroy. We can keep data for an indefinite period. Obviously that comes out of the nature of our work and the long running activities that we turn our mind to. Noting we're in a public hearing here, obviously we have some espionage investigations that have been running for many decades. On the basis of that, we understand the value of data and its ability to be available to us. Of course, we have an effective relationship with the archives and we work through this, so we do have areas where we have discussed and worked through and removed data that we've identified that we no longer require. But generally our preference is that when someone is subject to an inquiry and those inquiries are ongoing we retain that data for as long as we need. Especially in the case of espionage activity, sometimes those investigation activities go on for a long period of time. It's not because we're incompetent; it's just about how hard it is to unpick a deep penetration in our society, government or private sector.

Mr Vickery: Under the records authority that we have with the National Archives, we keep this particular class of information—in other words material retained from the data retention regime—for a minimum of five years, and at that point we determine whether we still need to keep it. If the determination is that we don't, it's within our gift to destroy or dispose of it.

Mr DREYFUS: That's helpful, too, Mr Vickery. I want to read out to you what the IGIS said when she came to the committee's public hearing on 7 February. This was regarding the 2007 Attorney-General's guidelines that govern ASIO. Ms Stone said:

... we've supported clearer guidance as to ASIO's obligations to destroy data that's not relevant or no longer relevant to security and clearer guidance on how proportionality is to be considered in respect of ASIO's intrusive powers, as well as in granting immunities by ASIO officers.

I want to ask a couple of questions arising from what the IGIS has had to say already to the committee. Firstly, in ASIO's view are its guidelines up to date and appropriate with regard to the data retention regime—noting that the Attorney-General's guidelines predate the data retention regime by some years?

Mr Burgess: On the question of the concurrence of the guidelines, we have been working through and we're close to actually having them updated, because we recognise that it was timely that that happened. That work is well under way and close to completion. Of course that's a management matter for ministers, in that context. In that work we have engaged closely and received plenty of comments, so it's very clear where the IGIS sits on all of this. I cannot but agree that clearer guidance would be useful. When we get to that in those guidelines is still a matter of debate.

Mr DREYFUS: That might be something the committee chooses to comment on. It's good to have the current context. ASIO notes in the submission the usefulness of telecommunications data for assessing security clearance applicants. Are you able to say what role telecommunications data plays in that security clearance process?

Mr Burgess: Mr Vickery might jump in here, but in the broad, obviously if a person is subject to security clearance there is some utility in understanding whether they have links to people of concern or a vested interest to us. That leads to, do we need to explore that? Is that a problem? In some cases it can be innocent. In other cases it can be a concern and will inform our views from a security point of view.

Mr Vickery: I concur with the Director-General there, in the sense that as we start to look at somebody in terms of their suitability for a clearance, it is akin in some ways to the beginning of an investigation. As we pointed out, the sort of information we can collect under the regime is important to an investigation. So as Mr Burgess said, establishing as best we can the contacts and the nature of those contacts through this data is important for us, for that reason.

Mr DREYFUS: I've got a couple of questions about the type of datasets that ASIO requests. When ASIO requests a dataset from a communications provider, what content can such a dataset consist of? What I'm really getting to is, have there been cases where, after requesting a dataset from a telecommunications provider, ASIO has received a broader range of data than originally envisaged?

Mr Burgess: Again, my colleagues might need to give us further information here, but I'm aware of cases where we have been given data we did not ask for. Initially I talked about the web, the URL. Our policy is that we have a warrant for that. We have had at least one case that I am aware of where potentially we were given URLs, and at that point we don't accept that. We purge that from our system. Of course it is electronically given to us. We are very clear that content is, and requires, a warrant. When those mistakes are made we call them out, and the Inspector-General knows about them and we deal with them.

Mr Vickery: Sometimes, for instance, we are simply asking for call charge records for a particular date range. It does happen occasionally that the provider will provide us a bigger date range than we originally asked for. Noting that our investigations are quite targeted, we would have asked for that particular date range for a particular reason, so to get additional information in some respects actually doesn't help us. The other thing to bear in mind is that we are charged for that volume of material, so if we get more than we ask for we have to pay for it. On more than one occasion we will send it back because we don't need it, we didn't ask for it to start with, and it is going to cost us money to keep it.

Mr DREYFUS: Given that ASIO's guidelines stipulate that 'wherever possible the least intrusive techniques of information collection should be used before more intrusive techniques', does ASIO have any internal policies for ensuring that overly broad datasets aren't requested?

Mr Vickery: Yes. There are intelligence procedures manuals around how an investigation is conducted that not only make reference to the guidelines but are part and parcel of an underlying philosophy on how we do our work. So that kind of philosophy is promulgated throughout the organisation. For example, it is something that our new case officers are inculcated with from day one. It is more than just 'the guidelines are over here'. It is a philosophy and a method of operation that permeates the entire way that we do our work.

Mr Burgess: I would add that we are a learning organisation and we do listen to our oversight always. To demonstrate that, recently, as a result of an inquiry the IGIS conducted with ASIO, we have stood up a compliance section. So there is some additional level of assurance that officers are there to ensure that our policies and procedures and the laws are being followed and that when there are issues we learn from them and report them and deal with them quickly.

Mr DREYFUS: For my last matter I'm going to ask you to throw yourself back in time to some extent, Mr Burgess. The Department of Home Affairs, in a very full set of submissions to the committee, spend some time examining what sort of matters were considered by this committee back in 2015, when the data retention regime was first put in place. They helpfully remind us at paragraph 161 of their submission that you bring a depth of experience to this job that is perhaps somewhat unusual, in that in 2015 you appeared before this committee in your then role as chief information security officer of Telstra. Since then, of course, you have been the chief of the Australian Signals Directorate and now the chief of ASIO. The Department of Home Affairs draws attention to a comment that you made to this committee in January 2015. I'll read out their paragraph, because that's probably the best way to get to it. This is the department's view, but they are quoting you as an authority:

The creation of centralised platforms to retain data was foreshadowed by some in industry as a 'honey pot', or target for criminal or other nefarious actors. Major carriers raised concerns that mandatorily retained telecommunications data would

give a hacker 'the pot of gold' to aim for, as opposed to their having to work through their multitude of systems in order to extract the same data.

They are paraphrasing something you said to this committee back in January 2015. Given the experiences that you've had, the roles you've been in, since then, some five years ago, can you offer anything to the committee about that problem and perhaps any assurances about what security regimes are in place, what's happened since 2015—I can think, for example, of the telecommunications sector security reforms—that go to this question or concern that you raised in your then role at Telstra in January 2015?

Mr Burgess: Certainly. I remember it well. In the context of the Home Affairs submission, they are calling that out in an understanding that, yes, we're asking for carriers and carriage service providers to retain this data and we recognise it's valuable and therefore the appropriate security should be upon that data, because actually, whilst it's there to support law enforcement, ASIO and others to get access to that data, it's important that it's protected because, because it's valuable to us, it's equally valuable to criminal gangs or nation-states, the people that we worry about. That's why ASIO will, through government and the telecommunications sector security reform legislation, require those risks to be managed effectively. Obviously I don't work or speak for Telstra now, but back then it was just making the point that Telstra does security well, but you want to make sure everyone does security to the same level, because it's valuable information. As we discussed earlier, I'd be confident that the TSSR is an effective means by which agencies—and ASIO does advise Home Affairs on those matters and we work closely with them, is the way we make sure that is occurring, noting the questions that other committee members have had that will go to allow you to determine whether in fact that is true.

CHAIR: Director-General, if I may, I will summarise the headlines, for me, coming out of this hearing. No. 1 is that the threat environment is increasingly complex, particularly with the advances in technology. ASIO targets are going dark, for example, using end-to-end encryption and other ways to protect their communications. The terrorism threat remains probable, and espionage and foreign interference are being conducted at the highest levels in our history. No. 2 is that the retention of data is critical to ASIO lead generation and also for you to be able to flesh out historical networks and patterns of behaviour. No. 3 is that your access to retained data is rigorously oversighted by the Inspector-General of Intelligence and Security. No. 4 is that longer periods of data retention would assist your work. No. 5—and this is where you may or may not agree—is that use of the regime by local governments, organisations not concerned with terrorism, espionage or foreign interference, potentially undermines public trust in the regime and indeed the social licence you need to do your work.

Mr Burgess: I agree with all of that. I could tweak your last one insofar as, as I said, it's really a matter for those agencies who are seeking the lawful access to justify. But, without that, yes, it would undermine the public trust in why the parliament gives laws like this and why we need them. I totally agree with that point.

CHAIR: There's a reason why you're appearing here alongside other agencies. There are quite a few players out there who won't step in front of us, nor will they make a submission, yet they will still make use of the powers.

Mr Burgess: Sure. On that basis, as I said before, I think those who want to use this power should argue their reasons for using it.

CHAIR: As there are no further questions, we thank you very much, Director-General and Mr Vickery. We appreciate your appearance today. Please get answers to questions on notice to the secretariat by 20 March, and we'll give you a transcript to make any corrections.

Proceedings suspended from 11:38 to 12:47

CARLESS, Mr Maurice, Assistant Commissioner, Intelligence and Covert Services Command, Queensland Police Service

FITZGERALD, Mr Michael, Commander, Forensic Evidence and Technical Services Command, New South Wales Police Force

PHELAN, Mr Michael, Chief Executive Officer, Australian Criminal Intelligence Commission

CHAIR: Welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. Gentlemen, I hand over to you for an opening statement.

Mr Fitzgerald: I'm grateful to the committee for the invitation to the New South Wales Police Force to not only provide a submission but also attend here in person and provide evidence. From the outset, I recognise the important balance to be had between the exercise of authority and the civil rights of citizens. I acknowledge the mandate of the Commonwealth Ombudsman to vigorously review the activities of law enforcement, including access to data by the New South Wales Police Force.

As the New South Wales Police Force submission indicates by way of case studies, the retention of data has proved to be vital in the most serious of cases. The domestic violence murder of a 20-year-old mother in New South Wales and later her two-year-old daughter in South Australia in 2008 provides an inarguable example of the need for long-term data retention. In that case, authorities were fortunate to have access to data that had been kept for seven years. If the offender had used another carrier service, then police would not have been able to link the offender through the metadata to those murders. He would now be in the community, potentially harming more women and children.

What might otherwise be an evidentiary void can be remedied by metadata. We would either not solve or have a much greater difficulty solving complicated murders and long-term missing persons cases without metadata. It is the starting point in the majority of those investigations. In the 2019 calendar year, the New South Wales Police Force made just over 108,000 requests to carriers and providers, which includes 1,476 requests for IP addresses, for all manner of serious crime, including terrorist-related investigations. The overall costs spent by the New South Wales Police Force on metadata exceeded \$2.3 million, which is an indication of the importance and priority placed by the regime on metadata.

The New South Wales Police Force has 477 unsolved homicides on its books. Historical metadata has the potential to provide a missing link once other factors are realised. The remains of victims may be found years after they are murdered. Metadata can be crucial to tracing the movements of suspects at a point in time. As advances are made in DNA and other areas of forensic science, suspects will be identified in many of the cases. Metadata will serve an obvious and invaluable purpose to place those offenders at the scene of the crime. Whilst it is claimed that it is impractical to retain this volume data indefinitely, I respectfully say a data footprint may well make the difference between serious offenders being prosecuted or continuing as a high risk to the community. Even more important in our criminal justice system is that metadata can support the alibies of the innocent and help prevent persons from being wrongly convicted. The prolific use of encrypted programs by criminals to avoid detection means that CCRs, reverse CCRs and cell site information is essential to all major investigations.

The committee will no-doubt understand the delayed reporting in sexual assault cases, especially in cases where children are the victims, which was highlighted in Royal Commission into Institutional Responses to Child Sexual Abuse. The community, rightfully, has placed a spotlight on law enforcement and government to come up with answers on how we can better protect victims of domestic violence. All too often victims of domestic violence are subjected to years of violence before they report their abuse. Police need this metadata as a corroborative tool to prove the stalking and intimidation that these victims unfortunately have to endure.

It is our most vulnerable that are most likely to be best protected by the metadata retention. We need to protect our victims of domestic violence and child abuse, and that is why the New South Wales Police Force are seeking an extension of the two-year metadata retention regime. Our safeguards include the fact that investigating officers cannot access metadata without authorisation from a commissioned police officer. The approving officer must be satisfied that the request is necessary for the enforcement of criminal law or another prescribed purpose.

In 2018-19, the New South Wales Police Force sought 7,474 evidentiary certificates relating to metadata requests from Telstra, Optus and Vodafone. This is an indication of the value of the product from beginning to end. Whilst it is clearly a matter for the committee, my respectful submission is that the current two-year retention

period should be expanded. The New South Wales Police Force join the Queensland Police Service in asking for an increase to seven years. Thank you very much for your audience here today.

CHAIR: Thank you, Commissioner. Commissioner Carless, would you like to make a statement as well?

Mr Carless: Yes. Like my colleague, I also thank the committee for the opportunity to be here today. QPS welcomes the opportunity to appear and answer any questions.

We note the committee's terms of reference has resolved to focus on the continued effectiveness of the scheme whilst also considering shifts in technology since the passage of the bill. I'd like to refer to the QPS submission to the committee and in particular the operational significance that historical and prospective communications data holds across a wide range of preventative, disruptive, investigative and prosecutorial pursuits, targeting a wide range of major and organised criminal activities. These law enforcement activities target drug trafficking, sexual assault, child abuse and related offences, extortion, burglary, robbery, kidnapping, murder, cybercrime, telecommunications offences, serious fraud matters and, of course, counterterrorism. The use of telecommunications data in these investigations is varied and has proven important for promoting community safety. For instance, telecommunications data can help with determining historical relationships between members of criminal syndicates and contact between criminal actors and victims of crime immediately prior to the commission of an offence or information concerning the location of significant patterns of movement of one or more individuals over extended periods of time. As such, telecommunications data assumes a critical role and a complementary role to the overall investigative capability. The changes observed in the use of technology are well documented and undoubtedly known to the committee. Over the past 10 years, the increased prevalence of encryption and encrypted applications has confounded our ability to reliably obtain communications content. Not only has the availability of such applications increased significantly over time, but their accessibility has also increased, in terms of cost and the ease of use. In the absence of communications content and metadata, there's now more than ever a compelling need for law enforcement agencies to have access to an effective telecommunications retention scheme, and I look forward to questions from the committee.

CHAIR: Thank you very much. For the public record, could you state the oversight mechanism that's in place for your respective uses of the metadata regime and how it interacts with the relevant police forces?

Mr Fitzgerald: An investigator or a police officer will make a request. They do that online. They'll put an application in through the iAsk police system. That will go to an inspector of police. As a former commander of the city, and in Kings Cross, where you get a large number of those and you have to be fiscally responsible, I ensure my inspectors review those both from a forensic and an investigative perspective but also from a financial perspective. We ensure that they are not trivial applications. After speaking with those officers, that inspector then approves or doesn't approve those applications. They are then forwarded through to our intelligence area, who then submit that to the carriers. So it's a commissioned police officer of the rank of inspector or above who has to authorise that application.

CHAIR: How many years are you generally in the force before you become an inspector?

Mr Fitzgerald: I was 20 years. It will be between 15 and 20 years.

CHAIR: So it's senior leadership within the police force, whose sole purpose is oversight of these matters.

Mr Fitzgerald: Generally it's duty operations inspectors, who are operational police officers in the field, or it's specialist homicide inspectors or hold-up squad inspectors who understand what warrants an iAsk application for metadata.

Senator FAWCETT: Within that process, as the inspector looks at it, is there also a threshold for the serious nature of the crime? So if somebody didn't stop at a random drug-testing station or something versus a murder suspect or something, is there an element where there's a threshold around the nature of the crime?

Mr Fitzgerald: The criteria relates to the enforcement of criminal law or another prescribed offence. As a commander of previous police stations, you would not be making an application, as you noted, in regard to a traffic matter, even though it's noted in the figures that we've provided that there are traffic related criteria. They all relate to a criminal charge, I've been advised.

Mr LEESER: Could I just understand something about the seniority of the inspector. At a local area command, the inspector is the most senior person at a local area command?

Mr Fitzgerald: A superintendent oversees the inspectors, but they're at the operational arm of that police force. They're the 24/7 response, and they're the most senior officer on deck 24/7.

Mr LEESER: Thank you.

CHAIR: Did you want to add anything, Mr Carless?

Mr Carless: It's a very similar process. It's a commissioned officer or our regional duty officers, which are of senior rank—a similar rank. Effectively the same process applies for the administrative process, and the requirement is that it must meet the threshold of criminal offence before it is actioned. So it's very similar.

CHAIR: Mr Phelan, would you like to make an opening statement?

Mr Phelan: No, Chair. I'm just happy to answer any questions that might be put.

CHAIR: Mr Leeson has a question.

Mr LEESER: I want to ask a question of the state police commissioners. You've posited the idea that we should extend the period for which data should be retained to seven years. Why seven? What's the case for that particular length of time?

Mr Fitzgerald: As I've indicated in the case studies that we've presented to you, without that two-year extension we would not have solved those murders. As I indicated in my presentation, domestic violence, historic sexual assaults and child abuse victims come forward at a later date. We need to support and corroborate their evidence by way of metadata.

Mr LEESER: I don't dispute any of that. I just wanted to know why you've picked seven years in particular.

Mr Fitzgerald: Seven years is what one of the main providers maintains currently, and we believe that is a suitable time. It is not an exorbitant amount of time for those people to retain that—certainly within this cloud environment, certainly with the amount of money that we expend to actually ask for that data to be accessed.

Mr LEESER: Under the present regime, you get access to the two years of data that's retained, but to get further access beyond that you need to go through a warrant process.

Mr Fitzgerald: No, not at this stage. I heard your earlier evidence about a potential solution to obtaining evidence over two years, which we think may well be a valid aspect. At the moment, if they hold the data, which one of the main carriers does, they may provide that to us, but the other two main carriers give you the bare minimum: two years.

Senator FAWCETT: You were here earlier; you heard the arguments around what we're generically calling the 'social licence'—the broader community's acceptance of metadata and, particularly, the retention regime. We raised the concern that this committee, in 2015, in seeking to achieve the balance, wanted to limit the number of agencies who could access the data and make it around law enforcement or ASIO's functions for serious criminal offences. These are the sorts of things you've outlined in your submissions. We believe that the fact that, under section 280 of the Telecommunications Act, through state and territory legislation, other bodies such as the RSPCA or teachers associations can access metadata undermines our ability to justify to the community why you should have that data. One of the things that was suggested was that, if, for example, a teacher's board were concerned about the conduct of a teacher, in terms perhaps of child grooming or some other activity like that, rather than them having access to metadata, if the activity constitutes a criminal offence, they should go to their state law enforcement body—that is, the police force—and basically present that as a case for the police force to access the metadata, if there's a criminal offence attached to it. Under your current laws, processes and thresholds for when you would investigate, would that work? If there were a serious animal cruelty case or a teacher suspected of grooming a child, would that work, in terms of putting in a filter, if you like, of who can access metadata?

Mr Fitzgerald: We'd have significant expectations that the department of education would pass on that information for us to investigate a serious criminal offence of child grooming. Similarly, if an animal is being abused, that constitutes an offence, which we would be satisfied to apply for metadata for, if so required. So, yes, we would be very interested in receiving that information, and we believe we would be the right people to be undertaking those inquiries.

Mr Carless: Equally, we would be concerned if there were such an offence. We would seek to have that information as well and use the investigative techniques that we normally employ. We would prioritise those complaints as we see the community's need and the speed at which the investigation should be undertaken, and I guess the need for whether or not there's any need to actually intrude into someone's privacy to achieve the investigative outcome that we were looking for anyway. So I can't really speak to why they would do it, but certainly, if we got that information, we'd prioritise it and investigate it as we normally would.

CHAIR: Mr Phelan, in what ways has the data retention regime improved the ACIC's ability to investigate transnational serious and organised crime, and could you provide the public with a case study or two of how retained telecommunications data has been used in those investigations?

Mr Phelan: Yes, certainly. Of course, the ACIC is a criminal intelligence agency, so we heavily support the states and territories and Commonwealth law enforcement agencies in relation to serious and organised crime. Over the period of the last five years since the data retention laws have come in, we've made approximately 20,000 requests, which is on par with what the agency did prior to the retention regime coming in. But one thing that is for certain, and certainly in the advice that I've got that I'm willing to put on evidence, is that, so far for all the requests we've made the data has been available, which is important because prior to 2015 it was not. As you're aware, I was intricately involved in giving a lot of evidence before this committee in 2015 and 2014. We've found so far that all the requests that have been made there has been data—whereas before there wasn't—because, as Assistant Commissioner Fitzgerald said, some of the telecommunications companies keep their data for a lot longer for commercial reasons. We found that it was all right dealing with that particular provider, but there were other providers who did not hold the material for commercial reasons for very long. Certainly we've found that all that information has now been available to us.

The vast majority of our requests have been for shorter periods of time—I mean, within, say, three-, four- or five-month periods. When we're investigating the higher echelons of serious and organised crime, particularly around our APOT list, or our the Australian Priority Organisation Targets, which are the highest threat targets to this country as determined by the ACIC in conjunction with our state and territory partners—all the names of groups are put forward there—we've found that we've had to go back a lot further to get data in relation to those individuals, because associations are important, finding out who knows who and who is with who when. And even exculpatory evidence has come forward as well—who wasn't with somebody at a particular point in time—because, particularly, self-sight data is relevant to that purpose. So when mapping serious organised crime, it's the networks that are important. I have seen some commentary, particularly over the last couple of weeks, about that we're able to build a very good picture of individuals and syndicates based on metadata. Well, that's true. That's what it was designed to do—to go and find out information on individuals, groups of individuals, who knows who—so that we could put enough information together to get affidavits to go for the more intrusive law enforcement powers, like telephone intercepts, listening devices et cetera, that require a judicial authority. So, on many occasions we use that metadata, that then helps build the case for us to know how we can target and use those far more intrusive powers when we need to get content. Then, of course, that's the difference between content and metadata.

I could pull out some individual cases but, at the end of the day, it's nearly everything we're working on at the moment, because we're only working on the top echelon of crime at the agency and metadata is extremely important for us. Even when we're doing our money laundering investigations, for example—I'll give a quite generic example—where we may follow cash that's been picked up by launderers, it's nice to know where they've gone afterwards if we pick up which devices they're using et cetera. We don't know who they are. We don't have anywhere near enough information to put before an affidavit to go intrusive, but we can get a picture on where they travelled after picking up cash and who they're potentially meeting off other people who we've got details on. It's about building that mosaic that's extremely important for all law enforcement.

There's been some evidence—you may get around to this. I saw some people saying that perhaps we should go back to reprosecuting the argument of having warrants for all of the data. I publicly said at the Press Club last week that if we went to have warrants for metadata you might as well close us all down. We simply could not do it. Not only that, we would be lucky to get past the thresholds that we would do to get intrusive data. That's why, I suppose, it was brought in for journalists' warrants. We've got to have a lot more information to be able to get information in relation to journalists. If we had to do that for our 20,000 requests—you could imagine that for all the state police and the AFP as well—we'd have to employ a lot more judges as well.

CHAIR: Earlier, the Director-General of ASIO made the case for extending the time that we retain data. His problem set is terrorism and espionage and foreign interference. Does your work at the ACIC cross over into some of those thread groups? I recall last year a Nine story about Crown Casino, for example, where it appeared that there was a fairly strong case to be made for links between foreign interference, money laundering and transnational crime.

Mr Phelan: One of our remits, one of the determinations signed off by the board, is in relation to national security. We have the authority given to us by the board to use our coercive powers, in relation to investigating those types of offences, and we have to have an authorisation for our organisation to investigate stuff in the first place now. We do see a nexus between serious and organised crime and counterterrorism and foreign interference. We haven't had a lot of visibility on foreign interference, and I'm sure the Director-General of Security has a much better view on that.

Certainly in relation to terrorism offences and offences occurring offshore, we've seen those links, particularly through money—the flow of funds backwards and forwards between foreign fighters and their domestic associates here. We do see transactions where money is generated by serious and organised crime, whether it be serious fraud or drug trafficking, transferred back through to known and named terrorist groups. I'd prefer not to name them here. That is a fact. And, of course, there's the crossover between serious and organised crime and domestic terrorism when it comes to weapons supply. Some of the weapons that have been used in terrorism incidents in this country were supplied by organised crime entities and serious criminals in our country.

CHAIR: Given that, would you generally, in principle, agree with the argument for retaining data longer than two years?

Mr Phelan: More than in principle. I would assert that it was a valuable tool back then—when I say 'back then', prior to 2015, for those companies that kept it longer. We were able to use that information and it was valuable. That ranged from lots of years through to nothing, and now, at least, we've got two. But while that information is being kept now—I'm not an IT expert so I don't know the costs of storage for that information—for every year that that information is being kept there is an extra utility for law enforcement and security agencies.

The bottom line for me is it's hard to say, because I don't know what I don't know. We could be investigating serious and organised crime and then I need to go back 25 months to find an important association, because one of our human sources might have said, 'Somebody knows something' such and such a time ago, or it might be 28 months or three years ago. We might have to dig back through our old files and we come across a convergence with another piece of convergence. So we may want to reinvestigate something that we looked at four years ago, to see whether or not there are associations that didn't come up, that we didn't find.

A lot of it is about: we don't know what we don't know. And in terms of intelligence, these are invaluable tools. The longer it goes, the greater utility it has for all of us.

CHAIR: Thank you.

Mr DREYFUS: The first questions I want to ask I'd like you to try to answer separately, but I'll go through it, if I can, and I'm happy to repeat the questions. This relates to the inadvertent provision of web browsing history to agencies. It is something the Commonwealth Ombudsman has drawn to the attention of this committee. We asked the Department of Home Affairs about this this morning—and they put you in it! They said, 'You'll have to ask the agencies.' The context for this is that section 187A(4) of the Telecommunications (Interception and Access) Act says that telecommunications service providers are not required to provide web browsing history. This is quite an important limitation that was put on the data retention scheme when it came in in 2015. I know directly that ASIO and the AFP—and, I imagine, you, too—go and get a warrant, as is required under separate provisions, if you are going to want to look at web browsing history. Assistant Commissioner Fitzgerald, how many times have carriers provided a person's web browsing history to your agency under the scheme? What do the New South Wales police do? Do you delete it? Have you ever used it? What happens?

Mr Fitzgerald: I was fortunate to hear those questions earlier, so I made some inquiries. I have not been informed as commander that we have received any of that information through the data retention regime.

Mr DREYFUS: That's heartening. What would you do if web browsing history was handed over?

Mr Fitzgerald: We would obtain a warrant, and that is what we do.

Mr DREYFUS: What would you do if it came to you inadvertently in the context of an authorisation request?

Mr Fitzgerald: Our policy would be that that would be returned back to the carrier.

Mr DREYFUS: Thank you. What about Queensland Police?

Mr Carless: I too was fortunate to hear the question before, so I made some inquiries. I don't have any information about actual incidents of that occurring. However, I'm told that if that was to occur, if we got information that wasn't authorised, it is quarantined away from investigators and self-reported to the Ombudsman. That has happened on a number of occasions, but I don't know the details of those.

Mr DREYFUS: Again, that's heartening. Thanks very much. Mr Phelan?

Mr Phelan: I didn't have the advantage of hearing that evidence, but the advice I had before coming in is that the vast majority of the checks we have done have been for subscriber checks and CCR data, which wouldn't include that material. It's my understanding that we haven't got web browsing history, but I'm happy to take the notice.

Mr DREYFUS: Could you spell out the acronym 'CCR' for those listening.

Mr Phelan: It is 'call charge record'—and the other is just subscriber data. If that web browser information did come to us inadvertently via a carrier, it would be quarantined in our system. We do have processes for when that happens. For a listening device product or a telephone intercept, for example, where there could be professional legal privilege, it is hived off and put in a separate component; and if it was inadvertently provided to us it would go back to the carrier as well.

Mr DREYFUS: Thanks very much, Mr Phelan. Assistant Commissioner Fitzgerald and Assistant Commissioner Carless have got the drop on you for this question. This relates to something I asked the Department of Home Affairs about this as well. It is about what these numbers represent. Queensland Police, in 2018-19, made 24,000 requests or authorisations for telecommunications data. New South Wales made about 106,000 requests. That's from the report on the Telecommunications (Interception and Access) Act tables. Assistant Commissioner Fitzgerald, have you got some notion of how many individuals those 106,000 authorisations might relate to?

Mr Fitzgerald: Once again, when I heard that question earlier, I sought some advice. That will be provided to the committee in due time. It is accessible and it is something we can achieve, but the data search at the moment hasn't come through.

Mr DREYFUS: That's fine. I'm really indebted to you. It goes to establishing the scope of this scheme. It's one thing to learn, as the reporting tells us, how many authorisations—and it is really helpful that we do know the scale of that—but what we are trying to get to is the number of individual Australians concerned. It is almost certainly—and you can probably confirm this—going to be a smaller number than 106,000.

Mr Fitzgerald: Indeed. I have read the previous transcripts that you had in 2015. It is well documented that drug suppliers use multiple phones. They drop phones very, very frequently. They would not all be individuals, but we will be able to provide that to you in a very short period of time.

Mr DREYFUS: Thank you very much. Assistant Commissioner Carless?

Mr Carless: It's less clear for us. We did hear that as well, and I made some inquiries. We are not certain that we can get the actual numbers, but we do believe that the number of applications or authorisations is very close to the number of individuals. But I can't be certain on the exact amounts. Whilst it is true that much of the work is around drugs and the criminal syndicates often have multiple phones, it is less clear how many phones they may have had for an individual and how we have recorded that in our QPRIME system. It would be close, but I can't give you an exact figure.

Mr DREYFUS: Thanks very much if you could take that on notice. Mr Phelan, your number for 2018-19 was 6536 authorisations. You weren't here before, so you're not really at all on notice about this question. Anecdotally, can you suggest how many individuals or what ratio we could apply to that number?

Mr Phelan: It would be an absolute guess on my part. It is obviously less—

Mr DREYFUS: Perhaps you could just take it on notice.

Mr Phelan: I will take that on notice. My knowledge of our systems says we should be able to extract that—but please can I not make a promise about that?

Mr DREYFUS: Fine.

Mr Phelan: I'll get as much as I can.

Mr DREYFUS: Thank you. This is directed at trying to get as good a picture as we possibly can of what's represented by the absolute numbers that are reported on. You've heard the questions that I put to the Department of Home Affairs about actual offence provisions that authorisations relate to. The reason for the question is that some of the categories are very, very broad; others are quite precise and you can see the offences. Is it a possibility that you can quickly access this on notice and come back to us with some information about what offence provisions under your criminal legislation these authorisations relate to in both cases?

Mr Fitzgerald: We can advise you on the offences in the document we provided the committee, but I've just been advised that we probably don't have the ability to interrogate the data about specific offences. Our Professional Standards Command uses 'miscellaneous offences' for neglect of duty offences and other things that don't have criteria. In regard to section 179s, in regard to the non-criminal sanction, our licensing enforcement area uses them in particular for firearms related offences that don't carry a period of penal servitude.

Mr DREYFUS: Even that's helpful. Could I ask you to take it on notice.

Mr Fitzgerald: We will.

Mr DREYFUS: I'm not looking for you to do a vast amount of work, but it would be good if you could give the committee any greater clarity or particularity as to the offences. Even what you have told us now about what 'miscellaneous' represents for you is quite helpful. It gives us a better picture—that you use it for internal investigations.

Mr Fitzgerald: That's right.

Mr Carless: For Queensland, I'd have to get some advice on it. I am advised that, depending on the level of authorisation, that may be particularised in there. The forms do have some specificity in them, but I'd have to get some more advice on exactly what they do.

Mr DREYFUS: Thank you. We've got some time left for this inquiry, so we'd appreciate it if you could do that. This is a question that was also slightly handpassed to you by Home Affairs. I'm not critical of them for that, because, overwhelmingly, the vast bulk of authorisations don't come from Home Affairs themselves. They're very much the supervising agency here and are responsible for the legislation. The department wrote this in their supplementary submission:

... the regime already contains a number of rigorous conditions that must be satisfied before these agencies can seek access to telecommunications data for their investigations and operations. When these thresholds are applied in succession, it ensures that agencies exercise their power to access telecommunications data appropriately, and only when necessary.

Assistant Commissioner Fitzgerald, do you agree with that comment?

Mr Fitzgerald: I believe we do act appropriately in regard to this scheme and this regime.

Mr DREYFUS: I'll come to you in a minute, Assistant Commissioner Carless. How resource-intensive is the process of working through these thresholds? I suppose what I'm getting to is: can you give us a picture of how much time an officer would spend looking at a request? Again, I appreciate it's hard to generalise and they'll all be different, but can you give us some picture of that?

Mr Fitzgerald: I can only talk about the previous commands that I have been in charge of. You have a finite amount of money that you can actually spend and that you're budgeted for, so you generally have to work with that. A cell dump can cost between \$15,000 and \$20,000, which will blow your budget pretty extensively, so you have to ensure that your requests are legitimate. They are interrogated, and the inspectors do speak to those officers to ensure that there is not another means of inquiry to do. But, as I indicated in my submission, it is generally, for your serious investigations, your first line of inquiry to ascertain who that person has been speaking with. Then, for a missing person who has been located, where a homicide is suspected, you want to know who was in that area at the time when that person was last sighted.

Mr DREYFUS: How much knowledge would the authorising officer have—that is, the officer who's going to authorise the release—about a particular investigation? What does it look like when the investigating officer goes to the authorising officer? Just speak to your own experience.

Mr Fitzgerald: For a criminal investigation, if your detectives are requesting it, they need to go through your crime manager, who's an experienced criminal investigator with 15, 20 or 30 years of experience. So they will know whether they're asking for information frivolously or not, and they'll also know that we have a fiscal responsibility to ensure that we're not making these requests without merit. The other five duty officers who work in a PAC, a police area command, will all be operational police officers. If it's a general-duties officer making a request for a DV matter, they will know what to advise that person. They may eventually expand the request and say, 'You probably need more,' and that's what I would advocate, because this is a great tool.

Mr DREYFUS: How much time would the authorising officer take in looking at a request?

Mr Fitzgerald: I would like to think—and this is not a good answer for you—as much as it takes. It could be 15 or 20 minutes of briefing, going through the investigation to the crime manager. It could be extended. As I say, the person signing this has to sign off certain criteria that they have reasonable cause to believe this is relevant and required. So they have to sign off on it. That commissioned officer has to sign off that this is a function that is required.

Mr DREYFUS: Can you put a number on how many authorised officers there are in New South Wales?

Mr Fitzgerald: We have 818 commissioned officers in the New South Wales police. Not all of those work in operational commands where they would be applying it, but I would like to say that between 400 and 500 inspectors across the state, who are working 24/7, would be those authorised officers, because these requests come in night and day, as you can imagine. Some are exigent and some are not.

Mr DREYFUS: So around 400 to 500 out of the 24,000?

Mr Fitzgerald: Twenty-four? I'll go with that number.

Mr DREYFUS: Is that about right?

Mr Fitzgerald: I thought it was 20,000, but 24,000 sounds better.

Mr DREYFUS: I don't know how many there are in Queensland. This is the last thing: are the decision-making criteria and the idea that it's only when reasonable and necessary consistently applied, as far as you know, across the New South Wales police?

Mr Fitzgerald: Yes. In my opinion, it is a very good regime. It is a good checking mechanism. It ensures that there is enough probity around it, that they are not done without good means.

Mr DREYFUS: Have you got internal guidelines in the New South Wales police about the authorisation process?

Mr Fitzgerald: Yes, and they can be provided.

Mr DREYFUS: That would be helpful. Thank you. Coming to the Queensland assistant commissioner, perhaps I can shorthand this by asking: is there anything strikingly different in Queensland from the process that Assistant Commissioner Fitzgibbon described?

Mr Carless: No, we have a similar authorisation process. It's generally for an investigative matter. A detective or a senior investigator will make the application through their chain of command—to a detective inspector generally, although all commissioned officers are authorised. They don't generally do them because they're not familiar with them. In the day-to-day routine it's generally the investigative units that do this. That then goes to the relevant area, which actions it. They double-check the forms and make sure all the criteria are met and the significant issues that must be met are all ticked off. Again, it's checked when it comes back to make sure it's exactly what we've requested. Obviously then you have the ombudsman and other internal checking systems that apply in terms of compliance as you would with any normal use of power in a police service.

Mr DREYFUS: How many officers in the Queensland police are authorised officers?

Mr Carless: It's every commissioned officer. I'm not sure how many commissioned officers we have exactly. It's all commissioned officers and regional duty officers. Our force is 15,000, roughly. I would have to get the exact number for you.

Mr DREYFUS: Could you do that, please.

Mr Carless: Yes.

Mr DREYFUS: The last point for you, Assistant Commissioner Carless, is about the processes. What steps or arrangements have Queensland police got to ensure consistency of decision-making in relation to authorisations?

Mr Carless: We have our policies and we have detailed instructions on how to go about the actual applications, authorisations and so forth. There have been a number of training programs, and the ombudsman reports back to us. The advice that they give us we roll out as we see fit to try to improve the operation and also the compliance across the organisation. So it's a continual process.

Mr DREYFUS: Finally, Mr Phelan, can you say or can you take on notice how many officers within ACIC are able to take authorise?

Mr Phelan: I'll take that on notice. I understand they are getting someone to find out for me right now, so I should be able to get that for you.

Mr DREYFUS: Thanks very much. I would assume that ACIC also has guidelines and processes to make sure there's consistency of decision-making?

Mr Phelan: Yes, very similar to our Commonwealth partners such as the AFP and others. Exactly like the Assistant Commissioner Fitzgerald put on record, cost is also a factor for us. It costs a lot of money to get CCRs and so on, so we're very prudent in what we ask for.

Mr DREYFUS: It's something to observe, isn't it, that there is a check in itself placed on the use of these powers by certainly all three of your agencies through that cost that makes you think twice before going to seek what could cost potentially tens of thousands of dollars?

Mr Phelan: Absolutely.

Mr Fitzgerald: We'd be very happy for that cost to be removed and for the committee to put in other checking mechanisms, if it wishes.

Mr DREYFUS: It may not be up to us. But we're interested in knowing that cost has, self-evidently, that effect. This is a question directed at the two of you from the state police forces. I was struck by the disparity in the use of these powers between the New South Wales police and the Queensland police. New South Wales police

used these powers more than four times as often in 2018-19 than the Queensland police. New South Wales is not four times larger than Queensland, nor does it have four times as many people. The ratio, I think, is about five million in Queensland to eight million in New South Wales. And the crime rate, I'm happy to say, in New South Wales is not four times higher than in Queensland. How would either of you account for the discrepancy? We're running a national scheme here. I'm interested as to why one police force in Australia is using this Commonwealth set up scheme a bit more than four times as often as the other.

Mr Fitzgerald: As per my earlier evidence, I genuinely believe that our use of metadata is appropriate.

Mr DREYFUS: No, I'm not criticising. Do not take this in the least as an implied criticism. I'm trying to find out why you might think this has occurred.

Mr Fitzgerald: It is certainly the investigative tool that our investigators use as a No. 1 inquiry, certainly in protracted and difficult investigations. I can't answer why ours are four times more, but it's certainly a practice that we support and advocate as a good way forward to start your investigation.

Mr DREYFUS: Do you have a thought about this, Assistant Commissioner Carless?

Mr Carless: I don't know—that's the short answer—but I could speculate that potentially we have a lot of remote communities where there would be only a single tower. The known locations of people is not as necessary as critical as in a city or urban area, but again it would be speculation. I've done no analysis on that.

Mr DREYFUS: I accept the point about remote communities. It wouldn't necessarily be true though for the regional towns up and down the coast. They would have a number of towers.

Mr Carless: Yes, although we do have a lot of very small towns in Western Queensland, in the cape communities, on islands and so forth—

Mr DREYFUS: Which might even have satellites rather than towers.

Mr Carless: Possibly, and that may contribute to a different approach to investigative techniques.

Mr DREYFUS: I'll go back to you, Mr Fitzgerald. New South Wales made over one-third of the total number of authorisations in 2018-19—105,000 out of 291,000. Looked at another way: New South Wales Police made over 70 per cent of the total number of authorisations of all the agencies for the release of telecommunications data in the enforcement of laws imposing a pecuniary penalty. Can you offer a thought as to why New South Wales is using these powers it seems in all categories and generally overall more than other states?

Mr Fitzgerald: Because we genuinely and truly believe that is the appropriate method to go forward in our investigations.

Mr DREYFUS: The discrepancy to me raises some question about whether these federal powers, which don't require any independent authorisation by any third party, are being used consistently across Australia. Self-evidently they're not, because just by the numbers they're being used more in New South Wales than Queensland. There are differences between other states, but the striking one is between your two police forces. Do you think it would be the case that there's a consistency of approach across Australia?

Mr Fitzgerald: Those figures that you produced would indicate not. I can only speak on behalf of New South Wales. We do believe that metadata opens up pictures and opens up avenues of inquiry that we normally would not achieve through traditional means of investigation.

Mr DREYFUS: I ask you to take that on notice. It might be that there isn't a simple explanation; it might be a complicated one that we can't all think of.

Mr Fitzgerald: We'll take that on notice.

Mr DREYFUS: If you can contemplate what might be a reason. I go to you, Mr Phelan, on the same point. From a national point of view or the national overview that you have, can you suggest why there are these differences between the states in all categories?

Mr Phelan: I actually don't have an opinion on that.

Mr DREYFUS: That's alright.

Mr Phelan: I can only talk about our own—and that would be like comparing apples with oranges—unless I actually worked against the serious and organised crime component of New South Wales Police or Queensland Police.

Mr DREYFUS: I want to go to another discrepancy that's a lot more specific. Queensland Police made over 4,000 prospective telecommunications data authorisations in 2018-19 and New South Wales made only 1,062, so it's a reversal in terms of this type—prospective data authorisation. I also add that prospective data authorisations used by the Queensland Police seem to have been on average in force for twice as long. So not only were there

four times as many but they were twice as long as well. Assistant Commissioner Carless, can you perhaps explain why that might be so—why there's this greater emphasis in Queensland on the use of these prospective telecommunications data authorisations?

Mr Carless: No, I can't explain why it's higher than New South Wales, but I do recognise that there's an additional authorisation threshold for those. There is additional oversight for the prospective data, and, to meet that, the officers, investigators or whomever would have to satisfy a higher threshold. Therefore it may be that—

Mr DREYFUS: What do you use them for?

Mr Carless: There's understanding the drug networks where the threats are immediate or within the next months or month or so ahead; when there's a community safety issue, where we need to know the location of particular individuals; if there are, for example, allegations of abduction of children and we need to identify immediately where they are and who they're with; and so it goes on. There's a broad range of offending that might come into a prospective data application.

Mr DREYFUS: Going to a much smaller matter, this relates to authorisations for what are described as 'public order offences', in terms of historic telecommunications data. In the last reported year, New South Wales made 76 authorisations; Queensland Police made 28; and the AFP made 14. Can you elaborate on what those public order offences would have been?

Mr Carless: From a Queensland perspective, I don't have the details on those applications.

Mr DREYFUS: It's a very small number; you may not. That's fine.

Mr Carless: No, I don't have the details on what those public order offences would have been.

Mr DREYFUS: I'm trying to track this through from the data rather than the very useful, but rather more anecdotal, examples that have been given.

Mr Fitzgerald: If I may, Senator—

Mr DREYFUS: Are you able to cast any light on this one?

Mr Fitzgerald: Generally there's a criminal offence—an affray. Having worked in environments where there are large brawls in the city and King's Cross, it's an offence where we're not actually 100 per cent sure what actually occurred in regard to that brawl. Someone has been seriously hurt and a number of people were involved in that melee. That's where I know some of my investigators have used that criteria: for affrays. I can't explain why it could be used in any other way, but I'll take it on notice again and get back to you. I know for a fact that affrays are used for that type of criteria.

Mr DREYFUS: The last statistically related question is also New South Wales. According to the annual report by Home Affairs on the use of these powers, New South Wales Police used the power under section 179 to access data for the enforcement of a law imposing a pecuniary penalty for the protection of the public revenue on 1,220 occasions. The report also suggested that 14 of those authorisations related to terrorism offences, 24 related to homicide, 33 related to abduction and 268 related to organised offences, which presumably means organised crime related. I don't know of any terrorism offence that has a civil penalty provision. Those are crimes.

Mr Fitzgerald: When I was reading this during the week, I asked for that updated information. Figures that have been produced are incorrect. I can state on the record, in regard—

Mr DREYFUS: I didn't mean to discover that; I'm sorry to hear it. But I'm more getting at the reason—

Mr Fitzgerald: I'm not saying that we don't have that amount of section 179s, but certainly there is no homicide related non-criminal offence that we would investigate, so they are incorrect.

Mr DREYFUS: I was going to say: why would you use the power under section 179, rather than the one under 178?

Mr Fitzgerald: They are incorrectly recorded, and the author of this report, sadly, is on long-term sick leave, so I can't ask that officer. But you have my word that a new table will be produced in the coming weeks and be put before this committee.

Mr DREYFUS: That's very helpful. That was a relatively small one. There's a final question about warrants. We've got numerous submissions that have come to this committee calling for warrants to be applied across the whole of the scheme. There are a number of rebuttals that have occurred to us and a number of rebuttals have been put forward by Home Affairs. I want to go to one of them. One of them is that agencies use historic telecommunications data to rule out innocent parties from suspicion without having to resort to more privacy intrusion and costly investigative measures. Would you agree with that?

Mr Fitzgerald: I would. Yes.

Mr DREYFUS: Assistant Commissioner?

Mr Carless: Yes, I would.

Mr DREYFUS: Mr Phelan?

Mr Phelan: Yes.

Mr DREYFUS: Are you able to say even approximately how many of the tens of thousands of authorisations—that both police forces have used and that the 6,000 or so that ACIC use—related to innocent parties were ultimately ruled out from suspicion?

Mr Fitzgerald: I can give you a story from my investigative career.

Mr DREYFUS: That would be helpful.

Mr Fitzgerald: We had a murder inquiry in a tavern in Chinatown. It was obviously an inside job. We had 10 people who had access or knowledge of where the licensee put the money. We did subscriber checks on those 10 employees. Nine of them came up squeaky clean; one of them didn't. Fortunately for us, we identified he was engaging with a known criminal. That led to the arrest of that offender. So those nine other persons weren't subjected to the same intensive physical and electronic surveillance that the other manager of that hotel was subjected to. So that will be across every investigation that we've undertaken; we exculpate people on a daily basis. From a cell site dump they were obviously not at that location at the time of the offence. I could speak for quite a bit on a number of different cases. But that is as good an example that I can say. We exculpate people every day.

Mr DREYFUS: And we would all want that to occur and we all readily understand the use that is being made there. I'm just trying to see whether there's any quantification that can be put on that. I'll ask the related question: is it possible to say, in respect of the authorisations that related to ruling out innocent parties, how many of those authorisations were in fact followed by the use of more privacy intrusive and costly investigative measures being deployed?

Mr Fitzgerald: I could help you with prospective data: 20 per cent of our prospective data lead to a telephone interception. That is the only figure I can give you today. If you want other figures in relation to other sections of the metadata, we could take that on notice. But, in the majority of our matters, most of those requests for data don't lead to any more intrusive supervision.

Mr DREYFUS: Do you have a comment there, Mr Carless?

Mr Carless: Yes. I endorse those comments as well. But the other side of it is confirming a victim's version of events or dismissing the victim's version of events. Equally, as we've mentioned, when there are large numbers of people that may have been in an area where a serious offence has occurred, it will rule out large numbers of people but identify and hone in on the particular individuals of interest. Equally, we've had a number of cases where people are ruled out through the use of the metadata and you won't then see them in court, naturally enough. In terms of them leading to more intrusive telecommunications interception, that may not be the only intrusive surveillance we employ and it would be impossible to determine in history how many of those went into physical surveillance or other sorts of surveillance or DNA or something like that which perhaps we might otherwise use in terms of determining who committed what and when.

Mr DREYFUS: I'll take you to be saying is that, while we can all understand the link that is being proposed here by Home Affairs, it is not really possible to put numbers around it?

Mr Carless: No.

Mr Fitzgerald: No.

Mr DREYFUS: Do you have anything to comment on that, Mr Phelan, since you're here?

Mr Phelan: I couldn't put a number on it, Mr Dreyfus. Certainly just from a number of operational scenarios that we do quite often, particularly around corroboration of human source information and human intelligence—and it would be no surprise to this committee that we don't take what's said by human sources as gospel. It needs to be verified and corroborated. Certainly, at times there will be a number of cases where the information hasn't been corroborated—as a matter of fact, it will be to the negative—by the use of metadata. An example would be saying someone was there when they clearly weren't, or at least their phone wasn't.

Mr DREYFUS: Thanks very much.

CHAIR: Thank you, Mr Dreyfus. As there are no further questions from the committee, I thank you, gentlemen, for your time today. You will get a transcript of your evidence to make corrections. If there are any questions on notice, please get your answers to the secretariat by 20 March. Thank you.

Proceedings suspended from 13:50 to 14:03

KENT, Mr Karl, Deputy Commissioner, Specialist and Support Operations, Australian Federal Police

KERSHAW, Mr Reece, Commissioner, Australian Federal Police

CHAIR: Good afternoon, and welcome. Although the committee does not require you to give evidence under oath, I advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I invite you, Commissioner, to make an opening statement.

Mr Kershaw: Good afternoon, Chair and committee members. Thank you for the opportunity to make a brief opening statement. This afternoon marks my first appearance before this committee as AFP commissioner. As such, I would like to acknowledge the important role of this committee as constituted under sections 28 and 29 of the Intelligence Services Act 2001. I note the important role played by this committee during the 44th Parliament, which saw the data retention bill passed into legislation in 2015.

I acknowledge mandatory data retention supports law enforcement investigations. I can also say that access to telecommunications data has proven to be and continues to be a very valuable tool for law enforcement. It assists us to uphold the law and it keeps our community safe. Since 2015 it has ensured the maintenance of our longstanding investigative capabilities in the face of rapid technological change.

The mandatory data retention laws standardised the practices of traditional communication providers in relation to the retention and protection of telecommunications data. Importantly the laws did not provide agencies with any new powers. Instead the obligations in the laws have improved agencies' ability to access, on a fee-for-service basis, critical evidence and intelligence when required and lawfully permitted to do so. The laws also introduced new recordkeeping accountabilities oversights by the Commonwealth Ombudsman, which we welcomed. Where we uncover noncompliance, we are swift to self-report to the Commonwealth Ombudsman and execute changes in response to their recommendations. We also make sure to record lessons learnt to ensure continuous improvement.

Compared, though, with lawful interception or surveillance, the use of metadata for the purposes of criminal investigations is a non-invasive means of progressing inquiries. While the majority of authorisations relate to data less than two years old, some of our most complex and serious investigations necessitate authorisations being made closer to two years after the fact. In the 2018-19 financial year the AFP received data in response to 760 requests for information older than two years and received data in response to 175 requests for information between 21 and 24 months old. While this sits against the data we received in response to almost 12,500 requests for information aged less than three months, quantity cannot be confused with quality in these investigations.

To tell you the story behind the statistics, I would like to discuss two case studies that demonstrate why telecommunications data is of enduring value. In 2018 the AFP commenced a counterterrorism investigation relating to offences committed in 2016. Again, this time frame indicates the complexity of our investigations. The focus of this matter was a group suspected of being involved in a plan to travel to Syria to engage in hostile activity. Their travel did not eventuate due to members of the community becoming aware of their plans. Historical call charge records—CCR—data from 2016, just under two years old, was used to identify the frequency of contact between persons of interest as well as businesses they called while making preparations for travel. Obtaining the historical CCR data provided evidence of contact between the primary person of interest and chemical companies, as well as calls to the Australian Passport Office. Witness statements revealed the POI was calling chemical companies to acquire materials for use in creating and testing explosive devices. They were calling the Australian Passport Office to acquire a passport to facilitate travel to the conflict zone. Both these records were used in the brief of evidence for this matter. Putting forward this information in the brief has been key in substantiating the elements of the charges and ensuring that the POI faces justice.

As I recently highlighted in my address to the National Press Club, the AFP is increasingly involved in multijurisdictional investigations regarding the production and distribution of access to online child sexual abuse materials. These investigations are often protracted for many reasons, including the involvement of international agencies, the global nature of the crime and the complex nature of the criminal network being investigated through the use of anonymity and technologies.

The AFP receives voluminous referrals both from foreign law enforcement partners and international nongovernment organisations. In August 2019 Australian police received a referral relating to a suspect in Australia using Tor, the onion router, the dark web, to access child exploitation material. The suspect was linked to an email address with an internet protocol allocated to an Australian internet service provider. In the investigation of this case, police sought access to telecommunications data from April 2017. Unfortunately, this

was outside the two-year retention period by a matter of months, and while some companies may have retained the data for slightly longer, in this case it was unavailable. It meant that our investigation was unable to proceed due to the inability to access telecommunications older than the two-year mandatory retention period.

With regard to journalist information warrants, of which eight have been issued to the AFP since 2015—two in 2017-18 and six in 2018-19—these warrants are obtained in limited circumstances to identify a source where there is criminality involved, which is likely to involve the unauthorised disclosure of classified and sensitive information. I acknowledge that the parliament viewed access to telecommunications data for these investigations as being a sensitive matter. This is why, when the AFP applies for a warrant of this type, it requires both the involvement of a public interest advocate to ensure balance is applied and for the issuing authority to impose any condition they see fit.

Along with these legislative safeguards and a commitment to improve oversight of sensitive investigations, the AFP is currently implementing the independent review of the AFP's response to and management of sensitive investigations, conducted by Mr John Lawler AM APM. I have provided the committee with a copy of Mr Lawler's report in the context of a separate inquiry. Investigations into criminality, whether politically sensitive or focused on community safety or child protection, are complex and access to information is crucial. I support the two-year limit for retention set by parliament, and the maintenance of the current retention period is strongly supported by the AFP. I want to take this opportunity to also thank the providers that store data longer than the mandatory retention period. I am seriously concerned, though, that reducing the two-year period could increase the risk of harm to our communities, including the safety of children, because of a loss of ability to access such crucial data. Chair, I now welcome any questions you may have.

CHAIR: Thank you very much, Commissioner. If I may, I will start with some questions which I put to the director-general of security earlier on in the day. The data retention regime is essential to your work in the AFP—is that right?

Mr Kershaw: Absolutely critical.

CHAIR: For lead generation and for development of criminal networks, historical patterns and all the rest of it?

Mr Kershaw: It is one of our most valuable tools.

CHAIR: For the public record, could you restate the oversight arrangements in place for the AFP?

Mr Kershaw: We have the Ombudsman as an oversight. We also have ACLEI. In the act there is the inspector-general, intelligence services, various committees, the minister—the list probably goes on. I can continue on.

CHAIR: So it's a pretty rigorous oversight ecosystem that looks closely at what you do in this space.

Mr Kershaw: Yes. As I said, we are committed to making sure we self-report and fix any errors. We're committed to having processes that abide by the law.

CHAIR: Excellent. We also talked about 280 and section 313 of the act and how that's, in a way, provided something of a gateway for state and local organisations to access metadata. Do you share any concerns about that?

Mr Kershaw: Yes. If it's alright, I might hand over to my colleague, who is our subject matter expert in this area.

CHAIR: Sure.

Mr Kent: In supporting the states and territories to garner access to this regime, the state and territory police agencies are bigger users of the regime than the AFP, so it's critical that access is enabled.

CHAIR: Sure, but they're law enforcement. We're talking about the local governments, RSPCA, any other examples—

Mr BYRNE: We're not exactly sure.

CHAIR: We're not exactly sure is the point.

Mr BYRNE: Just to back up the chair here, Mike Phelan was here before and involved in the construction of the architecture. The point that I made to you two gentlemen separately is that there was an understanding, when we were compelling the companies to keep this specified data set for a two-year period, that there would only be a set number of agencies that would be able to access that subset of data. What was also missed as part of that was that that gateway that had been used by others, which were not essential organisations in our view, was going to be closed. You couldn't get local councils accessing, at whim, metadata or telecommunications data. One of the

reasons I was a bit annoyed earlier today was that that gateway has not been closed. I think the point that the chair is making to you is that the public then has a perception that the RSPCA and the local counsellor that was sacked recently can access that data that you can access if you're chasing someone who now could be involved in foreign espionage or who wants to wander around Federation Square and kill a lot of people. The question is just in terms of proportionality. Do you think that they should be getting the same information that you're getting without having to go through the due diligence processes that you do?

Mr Kent: No, absolutely not. We wouldn't support that at all.

Mr Kershaw: We would be, and are, concerned about that, given the fact the RSPCA have no remit for countering terrorism. In broad terms, it needs to be used by the authorised organisations that are protecting Australians and upholding the law in various ways, whether you're a security intelligence agency or not. That's what we support.

Mr BYRNE: I want to come back onto that point and then we can talk about offshore data as well. Right from the outset of this creation of the scheme there was compelling evidence provided by Michael Phelan when he was in the AFP and ASIO as to why they needed to ask the telecommunications companies to hold it. We agreed upon a two-year period because you were going dark and we had to stop that. It's the absurdity of the very serious work that you do in keeping us safe. We've seen some horrific evidence, in terms of child sex predators, with the sorts of people we want to put away. We want to give you the powers that are being used by a council and being used by the RSPCA we're just not quite sure. My concern is that weakens public support for the work you're doing, and that, to me, is completely unacceptable. All of us on this committee support the work that you're doing. When you need legislation or you need something to be able to discharge your duties, our committee has got a great track record of being able to give you the powers, within reason, that you need, with appropriate safeguards. Those organisations are not subjected to the safeguards that you are, and yet they can access the same data. This is what is vexing the committee so strongly at this point in time.

Mr Kershaw: We would support the committee's view.

CHAIR: We don't want unaccountable organisations feeding like piranhas off Australians' data.

Mr BYRNE: The data that you need to keep the country safe.

CHAIR: Correct. That's great. The Director-General also made the case for extending the amount of data that's held or retained. Do you have a view on that?

Mr Kershaw: As in for the mandatory data time?

CHAIR: Yes. It's two years now, but it would help ASIO's operations significantly if they could reach back, particularly when you're uncovering spy networks, for example. I know the AFP now has a job ahead of it prosecuting spies and those conducting foreign interference on our shores.

Mr Kershaw: We would and that's why I said we've got over 760 that are beyond that period. Luckily, the telcos and others have held that material for us. Given the complexity and the rapidly changing environment, we would definitely welcome it to go longer than two years.

Mr BYRNE: Could I jump in with a bit of history, because some of the people and witnesses before seem to have forgotten the history—and by the way I'm not talking about any of our agencies, who I strongly support. The fact is that what was occurring around 2012, and when this proposition was first put in 2013, was that you would have a company that would keep the data for 30 days and you would lose it. The whole thing was to compel the companies to keep it for two years, so that gave you a framework, because otherwise you'd lose it all, other than one major service carriage provider that I know you guys worked with, and we did, and do, too.

I think that's the framework that is lost: that we created a scheme to ensure that we had a foundation, which was a two-year foundation, that the data that was required to be kept—and, by the way, the carriage service providers were provided with compensation in the order of something like \$120 million or \$130 million, which I will touch on a bit later—you're having to pay substantial amounts of money, as we're hearing. That is something that we can explore another time, particularly given that they were given a lot of money to create the capacity to create these specified data subsets that could be accessed appropriately and readily.

The point here is that the committee basically created that through extensive consultation. We basically want to continue to reiterate those points, just for history's sake. Sometimes people are having a debate and because they have seen other organisations accessing it, they're not aware of where the data is being kept at the present time. When the committee first looked at it, they will think that it wasn't very concerned about where you're putting this. It was almost like a world first. The UK couldn't get it up and the United States was going through the NSA and some of the difficulties. People forget that we were one of the first jurisdictions that put in a scheme of this

type, and we did it on a bipartisan basis. Any threat to that worries me a lot. That was just to provide a history that can help inform the rest of this debate.

Mr Kershaw: Thank you very much for that.

CHAIR: Commissioner, whilst we're on the topic of foreign interference and espionage, we heard Mr Vickery in 2018, when the laws were passed, tell us in a hearing just like this that espionage and foreign interference is being conducted at unprecedented levels. The Director-General of Security said the same thing on Monday. Last year the government announced a task force to go after these people. How are we going? Are we closing? We're yet to see a prosecution?

Mr Kershaw: We're on a good trajectory. I'm confident that we will have a prosecution. It is just a matter of time. It's not if, it's when. We have restructured ourselves to look at those tactical teams and how we work with ASIO in particular. As you know, we have a long history with ASIO, a very successful history in protecting Australia and Australians in the counter-terrorism area. Recently we had an international partner come out and do some training with our officers. We're going to build that capability very quickly, and we are, and we've already actioned some of the information that has been supplied to us.

Mr BYRNE: On that note, were they there to assist? I know exactly who it was and when it was and where it was. Obviously not for the public record here, but is that then assisting you in terms of your move towards proceeding to prosecution?

Mr Kershaw: Yes, it is similar to us with counter-terrorism, as in the doctrine; then what's required as far as the brief of evidence goes and to ensure that—it's a very complex area. There are ripple effects across the globe. For us, it's that we go in with our eyes open and we have our intelligence arm that are upskilled. We have learnt from our partner agencies. Some, as you know, are very skilled in this area. I personally spoke to their director, who was able to say 'We're here to help as well.' You can learn from them. We're going to be pretty aggressive in our approach. That's my style anyway. I still enjoy locking up crims, even though I'm not on the tools. That's our mandate and we'll stick to that.

Mr BYRNE: Excellent. To round out this line of questioning: the metadata regime is a critical pillar in that overall effort to identify and then prosecute spies and those interfering in our system.

Mr Kershaw: It is. If anything, I would say that you would end up with greater criminality and greater harm to our community, not just here in Australia but overseas, because as you know everything is connected now. It's a global criminal environment. It's an invaluable tool for us.

Senator FAWCETT: Commissioner, welcome. Can I take you to table 5 in your submission, which looks at authorisations granted under sections 178, 178A and 179. It usefully splits into different time brackets. The data between financial years 2016-17 and 2017-18 is somewhat variable. In the 24-months-plus category there is a very clear trend of increasing authorisations. Can you talk to the committee about the importance of data that's available beyond 24 months? In the light of very clear requests by both New South Wales and Queensland police for an extension of the mandated data retention, would you support those calls? Are there investigations where you have been frustrated by the fact that some telcos don't hold data beyond that mandated period?

Mr Kershaw: Yes. The example that I gave, without me being emotive, was tragic in the sense that that probably would have led us to either an individual or a group of individuals who were exploiting children. My argument would be that that's just one case. We had many, and that's why I'm also very grateful to those carriers and so on that do keep that data longer than two years. Our officers will still request, because they often just hope that that data is there, but for us to substantiate—in that particular case, it was identifying the actual offender. We already had the evidence pretty much in from the other agency, the referrals that come in to say we've got this IP address et cetera. It would probably mean that criminals are getting away with it and probably continually offending in Australia and beyond. We would encourage that change and we'd welcome that. It's a serious thing. Historical matters are always going to come up, especially when we take down some of these servers and other things. Not just child protection but drug trafficking now is all done on the dark web. A lot of it is anyway, as far as international goes. It goes back a long way now. We're facing encryption and other techniques that criminal networks and criminals are using to avoid law enforcement detection. So this is a primary tool for us.

Mr LEESER: Can I interrupt Senator Fawcett on this point? How many years would you want the extension to go to and why?

Mr Kershaw: We'd probably have to talk to our Home Affairs portfolio. That would be a matter for us to discuss at a portfolio level. And we would have to talk to our partner agencies as well.

Mr LEESER: The state police suggested seven years.

Mr Kershaw: That is a decent figure, given the fact it relates to the telephone interception act, as far as seriousness of the offending goes. That is something that we'd want to talk with our Home Affairs portfolio agencies about.

Senator FAWCETT: Table 4 in your submission is a very helpful breakdown of the range of offences. I note that the peaks of inquiry deal with things like illicit drugs and terrorism and the sort of offences where we give our full support to the AFP to have access to the data. But I am somewhat surprised to see, compared to the 1,764 terrorism authorisations that were requested, 16 traffic and vehicle regulatory offences. You've heard the concern of the committee about some other agencies at a state level accessing metadata for things that are not what we would call serious crime. As we look at that, and we look at 31 requests for property damage and environment pollution, I'm interested to get your perspective on why they are there and what the impact on you and like bodies in state jurisdictions would be if we sought to limit this to purely the majority of your table, which is serious and violent crime?

Mr Kershaw: To get the detail of those particular 16, that was in 2015-16. Could I take that on notice? I myself would be interested in having a look at what those particular matters entailed. Would that assist?

Senator FAWCETT: It would help if you could take that on notice. As well, there's 'miscellaneous offences'. I would be interested to know what's included in that. There's also 'offences relating to the enforcement of law imposing a pecuniary penalty'. I would be interested to know about that.

Mr Kershaw: I could take all them on notice.

Senator FAWCETT: And 'property damage and environment pollution'. That would be just good to know. They seem at odds with the rest of your table, which is large and extensive and deals with all the issues that we consider that you need to have the access for.

Mr Kershaw: I am only speculating, but I would suspect it has to do with ACT policing and our other functions, even with some of our establishments and other operations. But I'll come back to you.

Senator FAWCETT: That is unique, in that you have that dual role with these federal tasks as well as essentially the equivalent of a state or territory police force.

Mr Kershaw: Yes.

Mr DREYFUS: Thank you for coming to your first appearance, Commissioner Kershaw. You mentioned in your introduction the simultaneous inquiry that this committee is conducting about press freedom, where we got a joint submission from you and Home Affairs yesterday. I want to take the opportunity of you being here to ask a couple of follow-up questions. The first is: is it still possible that the ABC journalists Sam Clarke and Dan Oakes could be charged in relation to the Afghan files matter?

Mr Kershaw: I have to be extremely cautious here as it's an ongoing matter. I'm aware now that that matter has been finalised as far as the court process goes in relation to that warrant.

Mr DREYFUS: The challenge to the warrant in the Federal Court?

Mr Kershaw: That is right. That would be a matter for our investigators. They would have to expeditiously—which they are—go through that material now. Then they would either submit a brief or not to the DPP, or progress the investigation further.

Mr DREYFUS: Is it still possible that Annika Smethurst could be charged in relation to the ASD matter?

Mr Kershaw: That matter is before the High Court. Again, that is something that it wouldn't be appropriate for me to speculate on.

Mr DREYFUS: The other matter I want to raise with you really arises from the fact that this committee recently completed a review of a proposal for a national facial recognition system. We're told that the government is going to introduce legislation again on that subject in this current session of parliament, so it will come back. There are media reports today that agencies across Australia are using the facial recognition technology of a company called Clearview AI. Does the AFP use this technology?

Mr Kershaw: I have asked that question today myself, off the back of media reporting. To give you a fulsome answer, I'd like to take that on notice until I've clarified the information.

Mr DREYFUS: The media report says the AFP has rejected several freedom of information requests in relation to Clearview AI. Do you know why those requests have been rejected?

Mr Kershaw: I have had advice from my legal team, who have advised me that they need to do some further digging, given the media reporting and the matters raised in those articles.

Mr DREYFUS: You will appreciate the concern in in this committee that, in the absence of existing legal framework in Australia, the thought that such facial recognition technology was being used by the Australian Federal Police would be a concern. We would like you to take that on notice.

Mr Kershaw: I'd like to take that on notice.

Mr BYRNE: This is not a criticism, but to add to that, we're also advised that that particular service has been hacked. When we've been looking at the biofacial data regime, one of the key points of concern is that it's almost like a fingerprint. If someone can steal your fingerprint, the ramifications of that are gravely concerning. So I am gently flagging our concerns. If this is something that's being used by law enforcement and it has been hacked, then you have a system that is potentially vulnerable. We're keen to understand where it's at.

Mr Kershaw: I'll come back to you.

Mr DREYFUS: To come to the data retention that's before us, the first question is one that I asked the other agencies that have come here today. It goes to the question of getting web browsing history by inadvertent disclosure. For the purpose of the question we'll assume it's inadvertent. The ombudsman alerted us to this happening, but not necessarily in respect of the AFP. Has the AFP been provided with web browsing history in response to an authorisation?

Mr Kershaw: Yes—I might get the deputy commissioner to give you an example, one that is probably a good example, of where that occurred.

Mr DREYFUS: Our particular focus is on what happens when that occurs.

Mr Kent: In terms of the AFP, we acknowledge that URLs do occupy an interesting grey space between data and content, as they reveal content that a person may have searched for. For example, if we had <https://www.qantas.com/frequentflyer.html>, then that is information that a person may have accessed particular information relating to the frequent flyer program. The data retention amendments intentionally took a very cautious approach and the TIA Act did not mandate for the retention of URLs by carriers, in terms of this regime. There are internet service providers that retain the information for their own business purposes and/or it may be difficult for them to separate the URL data from the other metadata prescribed under the act. So, the ombudsman, as I understand it, suggested to this committee that it should consider whether to amend the TIA Act to include a definition of the term or to strengthen the definition of the term 'content' or 'substance of a communication or document' and certainly the AFP would welcome the opportunity to assist the committee down that path.

At this stage I can say that we have no information that we've been provided with URL data. However, data that comes from carriers to us comes in many different formats and our systems are not automated to detect a URL—that the response from a particular carrier contained particular URL information. Therefore, it then would come back to the officer concerned to detect that and make a declaration that it was outside the scope of a mandatory regime.

Mr DREYFUS: Do you have processes for what is to occur if there is inadvertent disclosure of URLs or web browsing histories?

Mr Kent: We have processes that very clearly articulate under the regime what are actually the datasets that are to be included. So, it would come back to individual officers to be able to detect that when the data was provided, or indeed our central area. What I'm saying is that there is no system that is filtering for that information. Therefore, it is possible that URL information has been provided and we haven't detected it. I would love to tell you that the system is fully automated in detection of that information—it isn't.

Mr DREYFUS: What suggestion could the AFP make to, as far as possible, maintain the distinction that's there in the law and which the law seeks to presently protect?

Mr Kent: I think clarifying even more strongly the nature of what is content verses metadata, in relation to this particular issue around URLs. It would be helpful. Then, that would be a process for us to update our guidelines and procedures to ensure that, where this data was detected, either by a central area or by individual officers receiving the information, they dealt with that information appropriately and in accordance with the act.

Mr DREYFUS: The reason I'm pressing it is that the law is already quite explicit. It says that this information is not to be provided. Can I take it that you're suggesting that it's not explicit enough or that it should be made more explicit?

Mr Kent: It might be necessary for us to reinforce the difference between a URL being provided, as being content—to strengthen that definition as it applies under the act would be helpful.

Mr DREYFUS: I will take you to be saying that you're not aware of any web browsing data having come to the AFP. If it did, you are relying on individual officers understanding that they're not to use it.

Mr Kent: Correct.

Mr DREYFUS: Just a small thing on the stats—thanks very much for the breakdown you've provided in your submission—it only goes up to the 2017-18 year. We've got, in the Home Affairs annual report of the last year, your high level stats for 2018-19. I wonder if I could ask you to extend the table that you've already provided to encompass the 2018-19 figures but broken down in the way that you have in the table?

Mr Kershaw: Yes, we can do that.

Mr DREYFUS: Thanks very much. On the question of individuals, which I've asked the other agencies about, in 2018-19 the AFP made about 17,000 authorisations for historic telecommunications data under sections 178 and 179. I'm sure you haven't got it to hand, but are you able to estimate or tell us something about how many individuals that is likely to relate to?

Mr Kent: Our current systems don't actually capture the number of people that that would relate to. Attribution then back to persons would be quite challenging for us to obtain, so the short answer is I don't believe we could do that quickly or easily using our current systems. They simply don't carry that attribution. I think it goes to the efficiency of the system. Unlike other aspects of the act, we're not required to record efficiency as it pertains to this particular provision.

Mr DREYFUS: Can you offer an anecdotal view of this, Deputy Commissioner? I'm assuming that the 17,000 authorisations definitely didn't relate to 17,000 individuals.

Mr Kent: Without doubt there would be multiple devices for individuals. It would be more than likely that the number of individuals impacted would be much lower.

Mr DREYFUS: I appreciate you not keeping this stat. I invite you to take on notice that question of giving the committee some idea of what number of individuals this might relate to, even if it's a range, or even if it's just to state formally to us, 'It's less than the last year. It's less than 17,000 individual people.'

Mr Kent: Yes, certainly, we can take that on notice.

Mr DREYFUS: See how you go. I asked the other agencies who were here earlier about the department's proposition that the regime already contains a number of rigorous conditions that must be satisfied before agencies seek access to telecommunications data for investigations and operations. When these thresholds are applied in succession it ensures that agencies exercise their power to access telecommunications data appropriately and only when necessary. It's paragraph at 94 of the department's submission. How many officers in the AFP have got power to make these authorisations?

Mr Kershaw: We did hear that question. To give you the exact number I will have to come back to you, but it's commissioned officers, which we're estimating around 250 in the AFP.

Mr DREYFUS: Out of?

Mr Kershaw: Out of 6,000.

Mr DREYFUS: Are there processes or guidelines within the AFP that are directed at ensuring consistency of approach among those 250 officers?

Mr Kershaw: Yes.

Mr DREYFUS: They're written guidelines?

Mr Kershaw: Yes. I have in front of me the standard forms and it shows you the whole trail from the beginning to the end and who's authorised what. I will give you an example. This one here is authorisation to Optus regarding IMEI. It states, 'The AFP is an enforcement agency within the definition of enforcement agencies,' so it's reminding our officers of that by virtue of the subsections. Then it has the superintendent's name as an authorised officer of the AFP within the definition of an authorisation officer. So we comply with that. Is the personal authorising not necessarily the applicant?

Then it is quite detailed on what that officer is authorising. For example this one reads: 'I authorise the disclosure of the following specified information or documents, being information or documents that came into existence before the time the person from whom the disclosure is sought, being Optus, receives notification of the authorisation. I am satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law'—and it goes on. It's quite detailed. There is also: 'I'm satisfied that any interference with the privacy of any person or persons that may result from the disclosure or use of the information or document specified above is justifiable and proportionate, having regard to the matter.' That officer has to basically go through all of that and be satisfied based on the application, so it's quite rigorous. Then it shows the history of the said note, when we sent it off to the carrier and what the request is and the response. So it's all open and transparent.

Mr DREYFUS: So all authorised officers use this same form and that, in a sense, dictates a standardisation?

Mr Kershaw: Yes.

Mr Kent: And a process that is to be followed which includes the form going to our online training and investigator toolkit, so our investigators can access at any time information relating to, 'How do I do this?' It's available to them, as well as face-to-face courses that are run for our authorised officers. We have a handbook for authorised officers and also our annual training program that they must complete online to maintain their authorisation.

Mr DREYFUS: I've got a couple more questions. One is in relation to the specific category of authorising historic telecommunications data to enforce what are described as public order offences. This, again, is out of the annual report. For the AFP, it's a very small number. There are 14 authorisations, but it still struck me as a somewhat unusual category for the AFP. Can you say what those offences would have been?

Mr Kershaw: It's highly likely it's limited to perhaps our ACT policing, but also it could be our establishments that we protect as well, including Parliament House, for example, but we will take that on notice and come back to you.

Mr DREYFUS: When you do that, could you perhaps also elaborate on how many of those authorisations resulted in arrests, how many resulted in charges and how many resulted in prosecutions? It's only a small number.

Mr Kershaw: Yes.

Mr DREYFUS: The final matter relates to warrants. A number of submissions that we've received suggest that there should be a warrant regime introduced across this entire scheme. One of the rebuttals put forward by Home Affairs relates to their proposition that agencies use historic telecommunications data to rule out innocent parties from being under suspicion, without having to resort to more privacy-intrusive investigative methods. Is that the experience of the AFP?

Mr Kershaw: My colleague might add something or say something slightly different, but my view is that it's often about speed, as well, with these matters. If we don't move quickly—for example, if you have a siege or an incident and you need to get up quickly on the comms, we don't want to be walking around trying to get an on-call judge or someone or a magistrate, then have the affidavit, where we can move much faster in this area. I would say there are probably public safety issues here as well and, obviously, the community harm aspect. We need to be able to move very quickly and, as you would be aware, sometimes going before a judge or going through that process is far slower than the current, and we're able to show that we've met the threshold of the law and that we have a process that we can disclose and that can be audited and so on. So I'd question: what would be the benefit of going—if anything, it could be a hindrance and a concern or a risk to public safety, if that caused us to have to slow down the process in some of these matters.

Mr DREYFUS: Thanks very much, Commissioner.

CHAIR: Any further questions from the committee? Commissioner and deputy commissioner, thank you very much for your attendance today. I appreciate your being as forthright as you can, particularly with ongoing operations. It's a nice shift. We will send you a copy of the transcript so you can make corrections, and, if answers to questions on notice could be sent by 20 March to the secretariat, it would be appreciated. Thank you.

Mr Kershaw: Thank you.

Committee adjourned at 14:50