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, 7 February 2020

Members in attendance: Senators Fawcett and Mr Byrne, Mr Hastie.

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

BLIGHT, Mr Jake, Deputy Inspector-General,
Office of the Inspector-General of Intelligence and Security ................................................................. 1

BUTLER, Mr Shane, Director Electronic Collection, Law Enforcement Conduct Commission ............ 25

COTTERILL, Ms Emma, Senior Assistant Ombudsman, Assurance, Commonwealth Ombudsman .... 7

DRAYTON, Ms Melanie, Assistant Commissioner, Regulation and Strategy,
Office of the Australian Information Commissioner ............................................................... 17

FALK, Ms Angelene, Australian Information Commissioner and Privacy Commissioner .............. 17

GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section,
Law Council of Australia .................................................................................................................. 31

HINCHCLIFFE, Ms Jaala, Deputy Ombudsman, Commonwealth Ombudsman .................................. 7

KFIR, Dr Isaac, Private capacity ........................................................................................................ 22

LEONARD, Professor Peter, Member, Media and Communications Committee,
Business Law Section, Law Council of Australia ........................................................................... 31

MANTHORPE, Mr Michael, Commonwealth Ombudsman ................................................................. 7

MARRSHALL, Ms Sarah, Executive Director Operations,
Australian Commission for Law Enforcement Integrity ................................................................. 25

MOLT, Dr Natasha, Director of Policy, Policy Division, Law Council of Australia ......................... 31

NEAL, Dr David, SC, Co-Chair, National Criminal Law Committee, Law Council of Australia ...... 31

RENTON, Ms Lara, Senior Lawyer, Australian Human Rights Commission ................................. 12

SANTOW, Mr Edward, Human Rights Commissioner, Australian Human Rights Commission ...... 12

STONE, the Hon. Margaret, AO FAAL, Inspector-General of Intelligence and Security,
Office of the Inspector-General of Intelligence and Security ....................................................... 1

WATSON, Mr Brett, Director, Regulation and Strategy,
Office of the Australian Information Commissioner ........................................................................ 17

WEST, Ms Bethany, Director, National Assurance and Audit, Commonwealth Ombudsman .......... 7
BLIGHT, Mr Jake, Deputy Inspector-General, Office of the Inspector-General of Intelligence and Security
STONE, the Hon. Margaret, AO FAAL, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security

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 by the Senate 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 of the Inspector-General of Intelligence and Security 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. I also ask that you are mindful of the written advice provided by the secretariat regarding current legal proceedings. Inspector-General, over to you for an opening statement.

Ms Stone: Thank you for inviting us to appear today. Given that this is a public hearing, I will make a brief opening statement.

The role of my office is to ensure that each intelligence agency within our jurisdiction acts legally, with propriety, due consideration for human rights and compliance with ministerial guidelines and directives. To that end, we carry out regular inspections of agency activities. We investigate complaints and conduct in-depth inquiries as appropriate. As explained in our submission, my staff review telecommunications data authorisations issued by ASIO as part of our periodic inspections of ASIO's investigative cases. In these inspections, we generally find a high level of compliance with the legislative requirements. While not wishing to detract from ASIO's diligence, we note that this is not surprising given the low threshold for issuing such authorisations.

We also inspect ASIO's information systems to ensure the data that has been erroneously provided to ASIO is removed from its systems. Our office does not have a policy position on matters concerning the mandatory data retention regime or access to telecommunications data by intelligence agencies. However, our submission highlights a number of areas for possible enhancements to the existing regime aimed at strengthening oversight, enhancing transparency and promoting accountability. I would be happy to answer any questions the committee may have.

CHAIR: Thank you, Inspector-General. Just before we proceed any further, I would like to correct something. In my formal opening statement I mentioned legal proceedings, there are no legal proceedings that you need to be mindful of, just to be sure.

Mr Byrne: One of the concerns I've had for some period of time is the length of time that ASIO will keep the metadata that it has accessed or called for. Are you able to share with the committee your understanding of how long you think they are keeping this metadata and when it's being destroyed? That's something I read in your submission that you referred to as well.

Ms Stone: Retention of data is a matter of concern to us. In relation to the data collected under chapter 4, there is no obligation to destroy it. That's correct, isn't it?

Mr Blight: Yes.

Ms Stone: But we have not had any complaints about the retention of data. It's something we do look at, but at the moment I don't have specific instances in mind. We have reported, in our annual report, about the destruction of data that has been incorrectly collected—for instance, generally due to a typographical error where data has been collected from a system that the authorisation did not extend to or was not the proper target. I think we've found that ASIO, once it becomes aware of this, is quite diligent in deleting the data. One of the problems, and I think it was mentioned in our last annual report, is that it may take some time for them to realise that this data was incorrectly obtained. When I say they're quite diligent, it doesn't mean there are not any mistakes. Sometimes, for instance when it's been decided—and this is an example from our annual report; do you have the page number,
Mr Blight?—they omit to delete the data for some time. It does appear in our annual report on page 32. That was an error in collecting information not relevant to ASIO's functions. In one instance they deleted it within 48 hours. I think in a previous case there was a longer period.

Mr BYRNE: What would your understanding be of, say, for example, how long on average? Do you have a sense of when the data is collected? It's not clear in my head whether or not it's kept for perpetuity, and we don't know whether or not it's being destroyed. In a sense, when the metadata is collected for investigative purposes, from that point on, we don't know how long it's kept for and we don't really know if it's actually been destroyed.

Ms Stone: It is kept indefinitely.

Mr Blight: There's no obligation for ASIO to destroy data—leaving aside data that's been erroneously collected. For data that is lawfully collected there's nothing in the act, the guidelines or the archives rules which requires destruction. So there's no noncompliance if it's kept indefinitely. What there is in the ASIO guidelines is a general statement saying that ASIO may keep a large reference dataset. In the, I think, 2015 committee hearings around this, we raised the issue—and I believe the ASIO submission brought up the archives rules. They have some internal guidance that says: data will be destroyed when required by the archives guidelines. The archives guidelines mandate retention of certain data and permit destruction but never require destruction. The archives guidelines are around protecting Commonwealth records for a different purpose.

Mr BYRNE: That's what I thought. When we first looked at this scheme in 2012-13 that was one of the contentious issues: how long would you keep the data for; would you destroy it?

Mr Blight: I believe the committee made recommendations—

Mr BYRNE: They did.

Mr Blight: In 2014 or 2015, around that issue.

Mr BYRNE: Is there any view that IGIS would then have with respect to that? Because it seems to be unclear. From my perspective it looks to be a bit of a challenge that you've then got—whilst not impacting on the agency's need and desire to access this information for lawful purposes, which I'm not implying they don't—a dataset that could be kept for perpetuity. You have a dataset that you don't know whether it's going to be destroyed or not destroyed. That to me is fairly ambiguous.

Ms Stone: It's a matter of policy, of course, as to whether the data should be destroyed. Where there is no obligation to delete or destroy the data, then there's no legality breach and, without a consideration of the value of keeping it, it would be difficult for us to say that there's an impropriety breach.

Mr BYRNE: Sorry, I don't for a moment impugn, if I've created that impression, the agencies in terms of what they're doing; it's more that it is a policy decision. They'll keep the data as long as they possibly can because it suits their purposes. Then again that's generally our decision, and we've looked at this from 2012 onwards. But does the Office of IGIS have a particular view about whether or not that's a satisfactory state of affairs? Again, I want to emphasise: this is not a criticism of the agencies; this is a policy question for us.

Ms Stone: Our general principle is that we don't express opinions of policy. I think we can say we understand what's behind that question of policy, but it's not really a matter for my office.

Mr BYRNE: Sure.

CHAIR: Noting that you don't express an opinion on policy but if we were to manage the issue with an amendment of some sort, do you have a view as to how we could best implement a framework?

Ms Stone: In general principle?

CHAIR: Yes.

Ms Stone: Any obligation like that imposed on ASIO would need to be overseen by us, and that oversight is greatly enhanced if the terms on which it's to be destroyed are very clear. With generalities, for instance, under the ASIO Act, there is a provision relating to warranted interception, I think, that relates to destruction, where the director-general is satisfied that the material is no longer relevant to issues of security. It may well be that in the Attorney-General's guidelines more specificity can be given than that. But it's very difficult for us to take issue with the director-general's view of satisfaction and, moreover, if the director-general isn't mandated to address that issue then it's very difficult for effective oversight. So our concerns would be not with the policy but with the wording of the provision, to make sure it allows for sensible and efficient oversight.

CHAIR: Thank you. Just to touch upon something that the deputy chair discussed earlier and cleared up, we're not implying the agencies are acting improperly.

Mr BYRNE: No.
CHAIR: I just want to follow up on what you wrote in the annual report. The IGIS's annual report noted: IGIS staff identified a small number of instances in which ASIO retained metadata, or telecommunications interception data that was not relevant to security.
And—
… ASIO intercepted a telecommunications service for two months before realising that the service was not used by ASIO’s investigative target.

Generally speaking, you're satisfied that ASIO is acting appropriately under the current regime?

Ms Stone: The answer is yes, but it needs to be qualified given the fact of our resources and the extent of this activity. It's very difficult for us to do other than targeting, as best we can, a look at a very small number.

Mr BYRNE: Are you aware of any instances where content was accessed, not just erroneous, but information—our committee looked at this, and I was chair in 2011 and 2012. The agencies have come to this committee and said, 'We want these powers for this particular reason and we'll make sure there are appropriate safeguards.' Having been to the gestation of this, where we've mandated data retention into law, one of the things was, in fact, how long they would keep the metadata sets before they destroyed them.

The other key issue that kept coming up was the straying of a dataset and information could be then provided that wasn't meant to be in that dataset, which is always about substance, about content. You've mentioned that, and a number of other submitters have mentioned that, that the changed datasets being kept and the information being kept is broadening. What is the risk, when the agencies are going to the telecommunications companies to get that dataset, that content is being provided? Are you aware of any instances where content has been provided where it shouldn't have been?

Ms Stone: I need to take that on notice. I think the answer is no. But I need to make one further observation—that is, because the nature of telecommunications has changed so much in recent years, there is this assumption that you get more from content than metadata. But when you look at the range of metadata and what it tells you, there's an argument that could be made that it is just as intrusive or almost as intrusive as content. You can tell a lot about what a person's doing from that. It's not for my office to express a view on whether that's desirable or not, but I think there is a trap to go straight to content and ignore the range of information one can get from metadata.

Mr BYRNE: You're talking about location et cetera, so you can profile from—clearly, the committee's understanding is that you get a pretty good overview about where the person is, what the person's doing, who the person speaks to et cetera when you look at those—

Ms Stone: The number of calls that are made to a particular person.

Mr BYRNE: Yes. And that is one of the issues that this committee has grappled with right from the inception of this. And looking at the US example as well, which is how close would it go to actually needing a warrant? It is not necessarily a view that this committee shares but it is something that's worth continuing to explore. Just to flesh out what you've said a little bit, are you saying that the intrusive nature of the powers that are being exercised by the agencies—which the agencies made a compelling case that they need I might point out—are almost as intrusive as seeking content?

Ms Stone: I don't know that I'm equipped to say they're almost as intrusive. To make that comparison is hard, because we know what you get from metadata and by hypothesis we hope we don't know what you get from content. It is hard to make that comparison. I note for instance that the Home Affairs submission refers to these provisions in chapter four as being one of the least intrusive means. I think that one could adopt a different view from that, because they can be very intrusive—not in the sense of what they tell ASIO and not in the sense of the person being aware. But certainly they are less intrusive than, say, an overt search of your house. In terms of what metadata tells you they tell you a lot about a person. I think, personally, that would qualify that comment by Home Affairs. Much of this could possibly find some more detail in a revision of the Attorney-General's guidelines for ASIO. We've been saying for many years now that those guidelines need revising. There has been movement, to be fair, in the last year, but particularly towards the end of last year and the beginning of this, where we are being consulted on revisions to the guidelines. They're well out of date as their present guidelines.

Mr BYRNE: Is there anything that you wanted to elaborate further with respect to the guidelines, because you mentioned frequently in the submission that you've made that it's out of date. Is there anything that you wanted to say that would further elaborate on that particular point?

Ms Stone: It is in our submission. Over some years now, in consultations and previous public submissions, 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. The issues I’ve already mentioned about relative intrusiveness of access to telecommunications data, as opposed to other collection techniques—the present guidelines were issued in 2007, so guidance in relation to new powers introduced since then would be very helpful.

**Mr Byrne:** In a sense there isn’t anything with respect to the new powers that provides a guideline that is sort of like a benchmark that says how you should be acting around those new powers that are granted?

**Ms Stone:** I’m sorry I didn’t catch what you said.

**Mr Byrne:** You said the ASIO guidelines 2007 haven’t been updated, so are you saying that with some of the new intrusive powers that we’ve granted the agencies the guidelines wouldn’t even cover that?

**Ms Stone:** Other than at a level of generality that might not give as much guidance as you might would hope. For instance, special intelligence operations, the use of force against persons, they’re the sorts of things that would be assisted by being specifically addressed in the guidelines.

**Mr Byrne:** ASIO has given how important they are. That’s concerning. Is it your understanding that that was contemplated in the Richardson review in terms of the ASIO guidelines? I know that that was looking at legislation but were you aware of whether or not the Richardson review looked at—

**Ms Stone:** I confess, I haven’t read all five volumes yet. I’m ploughing my way through.

**Mr Byrne:** We haven’t read anything. We’re still trying to work out when the government is going to release an unclassified version of it. But it is certainly something that I’m most interested in. I believe that Mr Richardson has done a great job, from what I hear, but it would be nice for us to get a clearer idea too, particularly if the issue that you’re raising has been contemplated within that review.

**Ms Stone:** Given this is a public hearing I would prefer just to rely on our own views.

**Mr Byrne:** Agreed.

**Mr Blight:** Yes, the guidelines do have that general high-level guidance, saying that the ‘least intrusive techniques should be used’ and they should be proportional, and that general guidance would apply. I guess our submissions have suggested that high-level guidance, while important, doesn’t really provide the granular guidelines and guidance that would aid the agency and aid our oversight. There are also more contemporary examples. Our British equivalents, for example, have issued much more detailed guidelines to their agencies, which provide a public record of the minister’s expectations around how powers will be exercised.

**Senator Fawcett:** Ms Stone, thank you for your submission. Paragraph 5.1 is about the threshold for authorisation. You talk about the fact that there is a great increase in both the volume and content of data that is held by telecommunications providers, and you then go on to raise, eventually, a question around privacy. It seems to me—I’m just seeking clarification here—that the main concern is that, with more data and a bigger range of data, if a request is made and the provider gives a dataset which is larger than the minimum dataset which was originally envisaged, that could constitute an unreasonable intrusion on somebody’s privacy. Is that your concern?

**Ms Stone:** Let me make it clear. The question of whether a particular statutory provision provides for reasonable or unreasonable intrusion is a matter of policy, and not for us. What we look at, given the mandate that is given to ASIO, is whether that mandate has been discharged with propriety; and whether the mandate given has been discharged with propriety is the context in which we would look at whether the action of ASIO is reasonable or unreasonable.

**Senator Fawcett:** I guess what I’m trying to get to here is what outcome would address your concern, because you differentiate between an enforcement agency and ASIO, and the additional requirements enforcement agencies have for the kind of information they want. But I can also infer what I believe to be the reality—that the providers retain the dataset they wish to retain for their own purposes, as well as the obligations they have under law, but the real concern is the data in excess of the minimum dataset. I’m just wondering if part of the solution perhaps is to say that the existing threshold for authorisation should continue if it’s just the minimum dataset that is provided, but if agencies wish to ask for an expanded dataset that may be available—and perhaps in current practice is provided because it is easier for the provider to do that—they need a different threshold for authorisation. Would that kind of nuanced approach address your concerns?

**Ms Stone:** It’s difficult to see where the policy part ends and where the oversight begins.

**Senator Fawcett:** If you tell us what you need for oversight, we can adjust the policy to make it fit!

**Ms Stone:** We’ll leave the policies to you. I think that one thing needs to be clear, going back to the ASIO guidelines. As Mr Blight said, the guidelines possibly could apply to some of the changes that have been made since 2007. But where they apply at such a high level of generality, it is very difficult for the agency both to know
exactly what is required of it and for us then to oversee compliance. So our concern always on a statutory or legislative requirement, in the statute itself or in guidelines, is always whether it is sufficiently specific, as the House, for instance. Privacy is to be weighed against the value of the information that is sought in terms of security—how that should be weighed up. It is difficult to express that in guidelines that will apply. But for that to be addressed as specifically as possible would be of great assistance not only to us in oversight but, I think, also to ASIO in making its decisions. I'm not sure whether that addresses what you were trying to get at.

Senator FAWCETT: That's fine. I'm interested to understand, in your oversight role, what frequency of occurrence you have seen, in your judgement, of ASIO acquiring and perhaps using information that is unreasonably intrusive. For example, you talked about destruction and then in the detail of your submission outlined that, as you made very clear in your oral presentation, ASIO are actually very diligent at destruction of stuff and that there are very few occurrences where it has not been destroyed in a reasonable time frame. On this privacy side, can you give us a similar indication? Are you concerned that this is a widespread occurrence or have you only seen a couple of instances where you think perhaps they have too much information of a private nature, or is this just a general, in-principle concern that you have?

Mr Blight: To clarify the earlier evidence: where data has been collected in error—for example, a typographical error leads to the wrong selector being sent to the carrier—that data is deleted promptly by ASIO, in our experience, with a few exceptions. That data is dealt with diligently and is promptly deleted. Data that is lawfully obtained—the correct selector—is not deleted. That's retained, there's no requirement on ASIO to destroy that data and there are no specific limits on disclosure of that data. I want to be clear that the comments around diligence in destruction are referring to diligence in destruction of data that has been obtained in error—often the carrier's error and occasionally ASIO's error. The percentage of errors is very low. We can't disclose the number publicly—ASIO considers that classified—but the number of errors identified is a very small percentage of the overall volume of data requests. I wanted to clarify that that comment about data destruction was only about the erroneous data.

In terms of proportionality and the threshold, the threshold is, as you would know, very low that the request is made in connection with the performance of any of the organisation's functions. The number of requests that don't meet that threshold—I don't think we've found any. It is such a low threshold that it would be rogue action that wouldn't meet that threshold, and that's just not an issue. So, if your question is around how often they do not reach the current threshold, it would be an exceptionally low frequency.

Senator FAWCETT: I accept the fact it's a low threshold. The implication, as I read it—and tell me if I'm wrong—is that you are concerned that the quantity and content of the data above the minimum data set may constitute an unreasonable intrusion into people's privacy. Have you seen examples where you've thought, 'That was unreasonable,' or is this just an in-principle concern you have?

Mr Blight: I think there are two issues there. One is that ASIO, when they make the request, won't necessarily know what the data carrier has. They don't necessarily know what that carrier will return. They might know what a particular carrier's general practice is, and it may not always be possible for the carrier to separate their data into the minimum and other. It's probably a question better directed to the carrier and to ASIO as to how they actually store that, because there are commercial imperatives—they want to store it as efficiently as possible. So ASIO may not always know what they're going to get back. When there is no obligation to destroy or even to analyse what they get back, we would say that they're not in breach of any obligation, because there is none. We are checking whether ASIO stays within the rules that are set for it. Where those rules allow freedom for ASIO to operate and they're operating within those rules, that's not something we flag as noncompliance. What we flag as a general issue that the committee may like to consider is whether that threshold remains appropriate in today's technological environment.

Ms Stone: Could I just clarify one point: I'm not sure, but Senator Fawcett's reference to my comment about ASIO's diligence in my opening statement was related to a high level of compliance with the legislative requirements for authorisation by ASIO. I said that there was a high level of compliance and that it wasn't surprising because of the low threshold for issuing such authorisations. It wasn't a reference to deletion.

CHAIR: Notwithstanding ASIO's diligence with compliance, it sounds like there is scope for review of the framework and potentially creating a better oversight mechanism.

Ms Stone: Yes.

Mr BYRNE: I have an observation, which is: when we first looked at this and we spoke to the telecommunications companies, all of them basically said that the major ones could keep metadata in a subset. As I understand it, through the architecture of the scheme that was implemented by the government, they were
supposed to be able to create a specific subset that could then be accessed by the agencies. To hear your testimony that the agencies are not sure what they're getting, I'm going to have to explore that with them and with others, because that's not the way the scheme was designed. It was supposedly designed—and I was given numerous assurances by telecommunications companies; I think the person sitting over from the secretariat would remember this as well—in that they were supposed to keep subsets. The danger was and the concern was that they would keep these subsets or have access to a capacity or a program to access the subsets, as required by the agencies. I think the federal government actually gave these telecommunications companies a substantial amount of money to ensure that that has actually happened. So, if that's not happening, that's of grave concern to me.

Mr Blight: Could I just clarify, because I don't want my comment taken out of context: we have no oversight of the carriers, so I have no visibility of their systems and no knowledge about how they manage that. Just for the record: that's not what I was saying. What I was trying to convey was that ASIO makes a request and then, if the carrier were to provide more than the minimum, ASIO wouldn't necessarily know that that was what was coming, nor would it be unlawful. As long as it's not content, there's no prohibition on the carrier giving back more than the minimum. I don't know the architecture of—

Mr Byrne: No, but I've been involved in the architecture of it, and even the fact that you don't have clarity, as the oversight body, person or organisation, is of concern to me. Sorry, it's not a criticism of you or the agencies. The fact is that—when we've asked the public—we need to build confidence. We've given the agencies very intrusive powers—the powers are intrusive. There were numerous discussions about this capability being granted lawfully to the agencies and parameters being set in terms of what data could be accessed. I was involved very early on and directly with the telecommunications companies, at some of the companies' locations, actually, and they said they'd be storing the data and/or creating programs. I'm just flagging with you that that is of concern to me because there should never be more than what has been requested. There was, we were informed, very, very specific information that would be required by the agencies or law enforcement agencies, and the companies would have requisite programs to ensure that there wasn't any additional information or data that was provided. So if there's something that is breaking down, that has changed since we've given the okay lawfully for that to occur, that's something that concerns me as someone who was involved in giving the agencies the lawful power to create this data subset.

Ms Stone: Can I just seek clarification here: I'm not sure whether your concern is arising from Mr Blight's comment that the agencies don't know what they're getting led you to think that they might be getting content as well as metadata. Is that the concern?

Mr Byrne: I think my conclusion, based on what I've heard from Mr Blight, is that the agencies are not sure what they're getting. The agencies have got an almost mandated series of requirements or information they can require from the telecommunications companies, so they should never not be sure about what they're getting I guess is the question.

Mr Blight: I just don't want my comment to be taken out of context. What I meant was if the carrier were to give them more, ASIO wouldn't necessarily know that in advance. I'm confident that ASIO understands what the carriers, the big carriers particularly, would retain and understands what would normally be returned. Because it is not a specific area of focus of investigation for us, I don't want to cause alarm where there might not be and I would suggest this is a question best directed to the carriers and to ASIO.

Mr Byrne: As someone that was intimately involved in the construction of this to create the appropriate safeguards, you can imagine I have some form of justification in listening to a comment you've said like that—this is not a criticism of you—and then to go, 'Hang on, that doesn't add up with what I've been told.' Again, I am not criticising you or the office and I am not criticising the agencies. We are undertaking a review of this mandatory data retention regime—whether or not it works, whether or not it can be improved—so any information, as legislators, that we can have is useful to us. So it's nothing more than that.

Chair: Do you have any closing statement, Inspector-General?

Mr Blight: It is always a pleasure.

Chair: We'll get you the transcript of your evidence and you'll be able to make any corrections. If you have any additional information, if you could get it to the secretariat by 5:00 pm on Wednesday 19 February, that would be great. We'll suspend for five minutes.
COTTERILL, Ms Emma, Senior Assistant Ombudsman, Assurance, Commonwealth Ombudsman
HINCHCLIFFE, Ms Jaala, Deputy Ombudsman, Commonwealth Ombudsman
MANTHORPE, Mr Michael, Commonwealth Ombudsman
WEST, Ms Bethany, Director, National Assurance and Audit, Commonwealth Ombudsman

CHAIR: 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. Mr Manthorpe, do you have an opening statement?

Mr Manthorpe: Yes, a short one. First of all, we welcome the opportunity to appear before the committee today as part of its review of the mandatory data retention regime. We canvassed a number of issues relevant to that regime at a private briefing with the committee on 12 September last year, and we've also made a public submission to the review, which you will have. So I won't, therefore, restate the various issues we have identified in any detail now. However, the overarching point we would want to make is that we think independent oversight of how the mandatory data retention regime works is incredibly important, just as it is with respect to other schemes that permit covert and intrusive actions by law enforcement and intelligence agencies. Our focus, in contrast to that of the IGIS—who you have just heard from—is in the law enforcement realm, as distinct from the intelligence realm. We oversee 20 law enforcement agencies in this area and produce annual reports on their compliance with the law. You have seen our 2016-17 report and our 2017-18 annual report. Our report on inspections conducted during 2018-19 is currently in preparation.

Overall we perceive that the agencies we oversee take their compliance obligations seriously, but that doesn't mean that we don't see issues of concern through our oversight activities. Errors and omissions that fail the legislative requirements do occur, and these matter, going as they do to the privacy and liberty of citizens and the validity of legal proceedings upon which covert activities might rely. Sometimes a seemingly simple error, like failing to keep delegations to issue authorisations up to date, can tarnish the validity of a significant number of investigations or call into question the material collected. So, in addition to our inspection and reporting activity we also work hard with the agencies themselves to encourage good practice and we track improvement or lack of it over time.

Finally, although, like IGIS, we're not a policy agency, we do sometimes see through our oversight activities areas of the architecture where we think the regime could be improved, and that is the focus of our submission, and I have with me my deputy and colleagues who are involved in this work day-to-day and are all very happy to take your questions.

CHAIR: Thank you, and thank you for the very fulsome submission. I'd like to discuss with you the verbally issued authorisations and the lack of a framework for agencies to operate in. Could you just tell us, for the public's view, particularly, how a verbal authorisation takes place, the circumstances under which it takes place and why this needs a framework?

Mr Manthorpe: Certainly. Basically we have observed that in some instances law enforcement agencies, particularly I think where they are operating in a spirit of urgency—there is some real or present matter that they need to investigate and they see the need to access telecommunications data to help them investigate that urgently—issue an internal authorisation based on verbal advice. At an operational level, I can understand why that might occur, but it isn't catered for in the legislation. We think that is a gap in the legislation. There is a policy question as to whether or not that should be permitted to occur, and if it is permitted to occur then it should be clarified in the legislation. Sometimes agencies, if they issue a verbal authorisation, subsequently commit to writing the considerations that they had regard to, consistent with the law, in issuing the authorisation. So, they sort of get to it after the event. But we think that area needs to be clarified so that there is a sound framework within which verbal authorisations, if they are to be permitted, occur.

CHAIR: What percentage of authorisations would be verbal versus deliberate and written?

Mr Manthorpe: I would imagine that it's quite low, but my colleagues might have a bit more of a feel for that.

Ms Hinchcliffe: It's a very small number that we see. I don't have a percentage with me. I'm happy to do some work on that if you would like, but it is a very small number that we see.
CHAIR: So, currently the process would be a late-night phone call, pen and paper, date and time group, signed by someone of authority and off we go, and then formally recorded in days subsequent. Is that sort of how it takes place now?

Mr Manthorpe: Yes. There is one other comment I would make. We will have a look at our data to see whether we can discern a percentage, but we see noncompliance in a small minority of cases generally, and this is one area of potential noncompliance. So, I do want to emphasise that there is a big volume of authorisations, and as far as we can ascertain most of them are authorised appropriately.

Ms Hinchcliffe: And if I could just add one more thing that I just thought of, in terms of our data, it's useful to remember that we sample the authorisations that we look at. The number of authorisations are such that when you go and do an inspection you can't look at every single one, so we have a sampling process to determine which ones we look at. Of course, any data that we give you goes to a subset, which is the subset that we have inspected.

CHAIR: Thank you. Could you talk about your concerns regarding ambiguity around the definition of 'content' and whether or not agencies should have access to that when disclosed by a carrier under an authorisation?

Mr Manthorpe: Yes. Essentially the piece of ambiguity we have observed through our inspections is that sometimes the metadata, in the way it's captured—particularly URL data and sometimes IP addresses, but particularly URL data—does, in its granularity, start to communicate something about the content of what is being looked at. That is essentially the point we're making.

CHAIR: So you get the URL and you get the full www.—whatever it is—.com, which can indicate what they're looking at.

Mr Manthorpe: That's right, exactly, and it can be quite long or it can be quite short. In some cases the descriptor is long enough that we start to say to ourselves, 'That's almost communicating content, even though it's captured in the URL.'

CHAIR: And then—we are getting too technical—multiple clicks on a thread would generate more and more content?

Mr Manthorpe: That's right, yes, exactly. We're simply highlighting that, when the scheme was commenced, the concept of metadata was probably thought to be quite a clean and delineable thing, but we know that there is a greyness on the edges here that we thought we should call out.

CHAIR: Sometimes there's information on the envelope, so to speak, to use the analogy from a couple of years ago.

Mr Manthorpe: That's a good analogy.

Senator FAWCETT: You expressed some concern in your submission about premature deletion of data. It's interesting. We just had the IGIS come in and talk about concerns about retention of data. Could you talk to us about your concerns and any examples of that?

Mr Manthorpe: I was interested in hearing the IGIS's evidence on that, and I can understand where they're coming from as well. It's two sides of the same coin. There needs to be an appropriate framework to determine what data is accessed and that it's appropriately authorised and then how long it is retained and for what purposes and then what the regime is for its deletion. In some of the other regimes where we have an oversight role, this has been made more clear. There is greater clarity around the requirements.

Mr BYRNE: What other regimes?

Mr Manthorpe: Surveillance devices is one.

Ms Hinchcliffe: The surveillance devices regime and even the telecommunication intercepts regime.

Mr BYRNE: I just wanted to clarify that, because I think it is something that the committee is obviously going to have to look at. It's just good to have a comparison. That's why I asked. Apologies.

Mr Manthorpe: That's all right. First of all, we think clarity is key. The point we were getting at, in contrast to but not in contradiction of the IGIS's point, is that, if an authorisation is given and data is accessed and we come along six months later and do an inspection—bearing in mind that we do our inspections retrospectively, essentially so that we don't disturb or prejudice ongoing investigations—if the data has already been destroyed, then we can't make an assessment about whether or not the data that was accessed and used in some way was in accordance with the authorisation. The authorisations are kept, as I understand it—

CHAIR: That is what I was about to ask.
Mr Manthorpe: So the authorisation is kept, but the resultant data is not, and so the point is: we can't therefore provide you or the public with assurance about the full picture.

Senator FAWCETT: In a perfect world, with unlimited resources, you'd check every case and you could tick a box and say, 'We've completed our review, and you can therefore delete the data.' Given that you only sample, there is obviously a percentage, however large, of cases where you will never physically—or digitally, whichever way you do it—sight the data and so be able to sign off on that. The tax office says, 'Keep your receipts for seven years,' sort of thing. Do you have an idea of the kind of time frame where you would want them to retain that there so, if you wanted to audit, you could? Otherwise they could write a thing and say, 'When we've finished our case'—and it might be two months—'bang, it all goes.' And you come in three months later and do your audit and there is no data.

Mr Manthorpe: Absolutely. It's a good question. The way I would start to think about answering that question would be to say: during 2018-19, we conduct inspections at all 20 agencies over the course of the year 2018-19, and we are looking at records that were accessed in 2017-18. So that would be the time frame, and, even if we don't access a record, in five years time we're not going to be looking at 2017-18 again, if that makes sense. We come to the financial year after the data was accessed, so that provides a time boundary that a framework could be built around.

Senator FAWCETT: So, in broad terms, to try to balance out IGIS's concerns, and yours, if guidelines were issued that you should keep data for at least this long, but not longer than this, after the case is closed, would that be the kind of framework that you would be comfortable with?

Mr Manthorpe: Yes, that's right—or simply by reference to the year in which the Ombudsman visited or something of that ilk. We think it's important that the data is available for inspection when we come to do our inspection, basically. But, yes, something in that realm sounds workable to me.

Senator FAWCETT: Thanks, Chair. That was my main concern.

CHAIR: In the absence of the metadata, if it has been destroyed by the agencies or the law enforcement agencies, does the verbal authorisation give you enough of a sense of what it might have been, for the purposes of your inspection?

Ms Cotterill: What the data that was returned looked like?

CHAIR: Yes.

Ms Cotterill: Unfortunately not. We would have a similar issue, I suppose, to that which IGIS has put before you, in that agencies will know what they have requested but don't always know what will be returned. So there certainly are instances where we do see data returned outside the parameters of the request. So we can't assume that, because the request was clear, the data returned was—

CHAIR: And then, because it can be deleted or destroyed, you, as the Ombudsman, will never know, which makes—

Mr Manthorpe: Which leaves a gap.

CHAIR: That's correct.

Mr Manthorpe: We would be able to satisfy ourselves of some of the things that we inspect for—for example, whether the relevant considerations were ticked off before the authorisation was given. Things of that ilk would be apparent to us. But it's whether the data that was accessed met the terms of the authorisation; that would be the thing we wouldn't know.

Mr Byrne: In your estimation, what percentage of the data that you sample has been destroyed?

Ms West: It is fairly low. The reason that is put forward sometimes by agencies could just be 'an administrative error' or that the usefulness was not there. But it's fairly low. We don't have statistics on that, but if it were of interest to the committee we could have a look at our data.

Mr Byrne: If that is possible, only because we're looking at quality assurance here. I'm concerned that we have a situation where, when we're reviewing this, our review is going to be impeded because there are difficulties, in terms of your benchmarking. If you don't have a dataset then you can't benchmark how that matches against the verbal or written authorisation. So it's a bit concerning. And there's this ambiguity now about how long data is kept for or not kept for, destroyed or not destroyed. It's looming through your evidence and the evidence of IGIS as a fairly substantial problem.

Mr Manthorpe: Yes. What we would say is that the potential solution to the problem is clarity. There needs to be clarity about how long things are kept—how long they may be kept if they are of ongoing use; if they're to
be destroyed; in what circumstances they are to be destroyed; how that is authorised; all that sort of thing—in such a way as to permit oversight activity to occur.

Mr BYRNE: Yes. That's something for us to look at. This is part of the mandated review. Do you get a sense of how often data above what the agency has been requesting has been provided to the enforcement agencies?

Mr Manthorpe: Again, there is evidence about that in our two most recent annual reports. We do report on that specific matter. The numbers aren't high, so I don't want to overstate that.

Mr BYRNE: They may not be high in proportion to the actual number of requests.

Mr Manthorpe: Correct.

Mr BYRNE: But they might be high if anyone was looking at them as just a figure separately because, as you know, the requests in terms of the enforcement agencies across the board are very substantial.

Mr Manthorpe: Yes.

Mr BYRNE: So, even though it might be a low proportion, we could be talking about a lot of instances. That's where I'd be trying to get some clarity in our review.

Mr Manthorpe: Sure. Ms Hinchcliffe has found the pages on this in our most recent report, and I will ask her to reflect on that.

Ms Hinchcliffe: In our annual report for the period 2017-18 we spend a few pages talking about this particular issue, where telecommunications data is provided outside the parameters of the authority. I'd be happy to send a copy of those pages to the committee if that would be useful for you.

Mr BYRNE: Sure.

Ms Hinchcliffe: In that part of the report we talk about there being four distinct categories that we see in our inspections. We see variations or admissions to names for searches conducted on the Integrated Public Number Database. So that's No. 1. We see telecommunications data outside of the authorised period; we see telecommunications data received after revocation took effect; and we see receipt of telecommunications data that was not specified in the authority.

Within our report we talk about the number of instances that we've seen during our inspections for that year. For example, in relation to differences, variations or admissions of names on the IPND we saw 13 instances of that in our inspections in 2017-18. We saw 45 instances of telecommunications data provided to agencies outside of the authorised period, we saw 41 instances of telecommunications data received after a revocation took effect and we saw 13 instances of telecommunications data that was obtained that was not specified on the authority.

Mr BYRNE: Thank you very much for those figures. They are actually very useful. Are you aware of whether or not in those instances the data was destroyed by the agencies in question?

Ms Hinchcliffe: Our normal practice would be to advise agencies that they should quarantine that material and then go through a process of destruction. But we would need to go back and have a look. I'll take that on notice.

Mr BYRNE: I know you have limited resources. You said the 'sampling'. If might be better getting a private figure on that but, if you are doing a sort of triage-style sampling, what proportion would you be looking at in terms of the overall authorisations?

Mr Manthorpe: I think we'd want to take that on notice.

Mr BYRNE: Yes, if you could, please. Again, sorry to put you through this but it is quite important because you are our key oversight mechanism, particularly with the law enforcement agencies.

Mr Manthorpe: No; we fully understand that. I think I'd just prefer to take it on notice—partly because I don't have it in front of me but also for the very reason you are implying.

Mr BYRNE: Absolutely. The evidence thus far has been very useful in terms of some expectations that I have had that are clearly not sort of occurring. So it's very useful.

Mr Manthorpe: Actually, there is one other thing I might just mention about the point that Ms Hinchcliffe was just working through. We have oversight of the law enforcement agencies and the Office of the Australian Information Commissioner has a role with respect to the telcos. I noticed in her submission—and I think she may be appearing before you later today—she refers to the desirability of the different oversight agencies being able to talk to each other effectively and exchange information. We agree with her that there is a bit of a gap there. If we see something that the telcos have provided to the law enforcement agencies that is over and above what the law enforcement agencies were asking for or were authorised to get, we would like to be able to have a good discussion with the Information Commissioner about that so there is appropriate oversight of all the different
elements of this. That may be something she raises later in the day, but I thought we would mention it since we were talking about that sort of space.

Mr BYRNE: So at present you can't do that?

Mr Manthorpe: The confidentiality provisions in the law are such that there are very strong limitations on what we can do with the data that we receive.

CHAIR: Mr Manthorpe, could you talk us through section 180H? You mention in your submission that it unintentionally limits the application of the requirements for journalist information warrants. Could you take us through the current limitations of this section, and how you might improve it?

Mr Manthorpe: Yes. The information that I think we're raising with respect to journalist information warrants also came up in the media freedoms inquiry last year.

CHAIR: Mr Manthorpe, could you talk us through section 180H? You mention in your submission that it unintentionally limits the application of the requirements for journalist information warrants. Could you take us through the current limitations of this section, and how you might improve it?

Mr Manthorpe: Indeed. The point we were making was that, as the provisions are currently framed—and you might recall that we took a particular interest in this, off the back of the journalist information warrant breach which was self-identified by the AFP a couple of years ago. We went in and had a look at what had happened for that to have gone wrong, and that's all on the public record. But a particular issue we identified in that context was an ambiguity, or what we think is a gap, where, on the one hand, it is very clear that if an agency wants to access a journalist's information, and the target is the journalist, they have to get a journalist information warrant. But what's not so clear is that if an agency has a sense of who the source might be, they can get an internal authorisation to access the potential source's data and, in so doing, identify those phone numbers and so forth that the potential source was communicating with, and it may turn out that one of those is the journalist. And so there is a way in which the journalist's source is identified but without accessing a journalist information warrant. We're simply raising that as an issue for consideration, as to whether or not it is consistent with what was intended in the scheme.

CHAIR: Just to be very clear: the journalist information wouldn't be accessed, just the source's information, but, by proxy, information about the journalist and their contacts would be uncovered. Is that right?

Mr Manthorpe: That's right.

CHAIR: And the question is: are we happy with that arrangement as it stands?

Mr Manthorpe: That's right. So the parliament has passed laws to try to put a higher threshold over what law enforcement agencies can do, in the context of them trying to identify journalist sources. And what we're pointing out is that there is a means by which, arguably, that is weakened—or, arguably, a gap.

CHAIR: I'll move to the retention period. Is there anything that you wanted to say on the public record with respect to that? It's two years, clearly. I'm just having a look at the data that you've provided—80 per cent of the requested data was zero to three months old, and less than seven per cent was over a year old. This is something that we as a committee looked at. That means that, basically, 93 per cent of the data that's being requested is requested within 12 months—according to the information that you've provided—and seven per cent, then, is within that second year.

Senator FAWCETT: That is of that subset that's been audited.

CHAIR: Of that subset, yes. Do you have any reflections on that that you would want to share with the committee?

Mr Manthorpe: If you're talking here about the period that the telcos have to retain the data for, I don't think we'd have a sort of policy view on it. I can imagine the law enforcement agencies or intelligence agencies might argue that although the numbers that they want that are older may be small, the imperative sometimes to access that data is great. I would leave to them to make that case. We don't look behind the merits of the data access. I think those are really the only observations I'd want to make. I don't really think we have a strong view on the point.

Mr BYRNE: You reflect on that in your submission. I might leave that point there, Chair.

CHAIR: There being nothing further, thank you very much, Mr Manthorpe, and your team.

Mr BYRNE: And thank you for the submission as well, which is very detailed.

CHAIR: Yes. We will get a transcript to you for correction, and, if there's anything further, if you could get that to the secretariat by 5 pm on 19 February that would be great. Thank you.

Proceedings suspended from 09:45 to 10:01

RENTON, Ms Lara, Senior Lawyer, Australian Human Rights Commission
SANTOW, Mr Edward, Human Rights Commissioner, Australian Human Rights Commission

CHAIR: I now welcome representatives of the Australian Human Rights Commission 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. I now invite you to make an opening statement.

Mr Santow: Thank you, Chair, and thank you for inviting the commission to give evidence. The stated aim of Australia’s mandatory data retention regime is to address serious criminal offences and to protect national security. It's clearly legitimate for the Australian government to pursue those aims. However, the government has acknowledged that the data retention regime does restrict human rights, especially privacy and freedom of expression. The commission considers that impact is disproportionate, more than is necessary to achieve the legislation's legitimate aims. I will briefly elaborate on some of our concerns.

Firstly, the revised explanatory memorandum said that this legislation was necessary to combat:

… serious criminal offences (including murder, sexual assault, kidnapping, drug trafficking, money laundering and fraud) …

However, the law in fact permits access to personal data for a much broader range of purposes, such as enforcing a law imposing a fine or to protect public revenue. In practice, personal data has been accessed by law enforcement in situations where there is no serious offence alleged. For example, almost 15 per cent of authorisations have been for apparently minor offences, such as public order and traffic offences.

A law such as this one inevitably restricts people's human rights. This can only occur if there is a strong justification. For example, in the Digital Rights Ireland case, the European Court of Justice said that accessing an individual's personal information could be justified only if the crime being investigated were sufficiently serious to warrant the limitation on the individual's privacy. So the commission proposes that this law be amended to bring it into line with its stated purpose of national security and combating defined, objectively serious crimes.

The second concern is that under the act service providers must keep relevant data for two years. While some retention of personal information is permissible under international human rights law, there are real limits to how long a country can lawfully retain such data—even for law enforcement purposes. Australia cannot hold on to personal information just in case it might be useful at a hypothetical later date. For example, the Court of Justice has assessed the impact of similar regimes in Europe on privacy and freedom of expression, and it found that retaining personal data for six months to two years was disproportionate to the aim of fighting serious crime. In any event, the operation of this law suggests that there may be no compelling need to retain this information for two years. The operation of the legislation since its inception suggests that over 80 per cent of requested data was only zero to three months old and less than seven per cent was more than a year old.

Thirdly, our submission draws attention to some problematic ambiguities in this legislation. For example, the act provides that only metadata should be stored and that this does not include the contents or substance of a person's communications. However—and I note others such as the Ombudsman and the Law Council have made a similar observation—the terms 'contents' and 'substance' are not defined in the act. There is a serious risk that providers who are worried about falling foul of the law will retain more personal data than is necessary to combat serious crime. The commission has recommended at least a non-exhaustive definition of those terms—'content' and 'substance'—because it would help clarify the obligations of providers to retain metadata, it would reduce the risk of unintended restrictions on people's privacy and other rights, and, indeed, it would keep the legislation more close to its stated aims. We're happy to answer questions.

CHAIR: Thank you, Mr Santow. From the top, are you in favour of repealing the regime?

Mr Santow: What we've recommended is some amendments to the regime. We haven't specifically recommended an entire repeal.

CHAIR: Okay. The AHRC submitted two years ago that two years was too long a period to retain data. What's the ideal retention period, in your view?

Mr Santow: We haven't made a proposal along those lines. We feel we have some insight, but we're not purporting to have the full insight. What we're saying is that, clearly, under international law—looking at similar international law obligations or very, very similar international law obligations that apply in Australia—a period of six months to two years, undifferentiated by reference to the relevant crime, is too long. So, clearly, what we currently have is too long. It would have to be a period under six months. But we wouldn't want to state a very
arbitrary figure when law enforcement agencies and the Department of Home Affairs and others might have a very specific view. But that gives some range.

Senator FAWCETT: Mr Santow, you mentioned before and in your submission you talk about the fact that some of the data is being obtained for quite minor things like traffic offences. Clearly you think it should be retained for more serious crimes. When it comes to the period of retention, whilst there may only be seven per cent that are more than a year, do you have any evidence about how many of those were serious crimes? Clearly, if even two or three per cent of those are online exploitation of children or organised crime or terrorism offences, that's exactly why the data is there. But, if we don't retain it, when we need it to pursue those serious crimes, it wouldn't be available. Do you have any comment on how we balance the serious crime in that seven per cent, because that's the purpose of the regime—to enable us to catch those serious offenders?

Mr Santow: The data that we refer to has come from the Department of Home Affairs. We don't have any insight into differentiating the data that is held for longer than a year. What we would say is that law enforcement agencies have a range of tools at their disposal, as well they should, in order to investigate very serious crimes. There could be orders sought to preserve certain information from being destroyed by the telecommunications provider if the law enforcement agencies are concerned when investigating very serious crime that they would otherwise lose some potential evidence before it can be properly considered in the usual way, if that makes sense. I guess what we're saying is that this seems like a very blunt instrument in order to combat very serious crime. There would be more targeted ways of combating more serious crime than simply having a blanket retention period of two years.

Senator FAWCETT: Sure. The point, I guess, is that if the data is not there then even to retain warrants and higher levels of authorisation, you can't access it if it's gone after six months. When we were initially bringing forward the legislation around data retention, one of the things that was highlighted to us was that there are cases which only come to light courtesy of partner agencies overseas et cetera, who will highlight that something has occurred, which will then trigger an investigation, which may well be after that six-month period. So my question is: how do we balance your concerns about having two years of data? And rather than saying to the telcos, 'You only have to hold it for six months', is an alternate path to say: if agencies want to access data that is more than, say, 12 months old then they have to justify it. So you're limiting the access but not getting rid of the data that you may well need for that seven per cent, which could be serious crimes.

Mr Santow: I think your proposal, your mooted amendment, there would go some way to addressing that concern. But the fundamental point we are making is that law enforcement agencies have a range of tools and we would think that they are sufficient in combatting serious crime. In a sense, if your concern is that the information might leak away before it can be used then why limit it to two years at all? It could be two years and one day when the relevant law enforcement agency becomes aware of it. The whole point about international human rights law is that there has to be a balance struck and that balance acknowledges two things: first, that there is a real impact on individuals' privacy, including, and perhaps especially, individuals who are never accused of any serious crime, and that can only be justified by reference to the serious crimes that are being investigated or combatted; but secondly, that then also imposes some burden on our law enforcement agencies to be really diligent and creative and so on to make sure that they are able to investigate crimes as quickly as possible. And what we're saying is that the balance with a retention period of two years is not right.

Senator FAWCETT: Sure. But surely people's rights are only infringed if the data is accessed because otherwise we would have similar concerns about social media providers, for example, who hold far more intrusive and personal data than telcos do for much longer periods. It's not accessed by the government; therefore, people don't have a concern. So if the telcos hold data that's not accessed by the government—hence my comment about warrants for longer periods et cetera—then surely their rights, their privacy is not being infringed upon just by the fact that a commercial entity is holding that data?

Mr Santow: I understand the point. It's a bit like: if a tree falls in the forest and no-one hears it, has the tree really fallen? I think the OVIC has, in its submission, gone into depth on that issue. There are genuine risks in simply retaining information. Two really critical ones are: first, it presents what OVIC referred to as a honey pot argument raised during the original inquiry. Do you have any evidence or examples of such data breaches occurring, because I've not heard or seen of any?
Mr Santow: That's not something that is raised with us because we're not the agency responsible for data breaches, so that might be a question better put to the OAIC, which is responsible for those issues. All I can do is direct your attention to OVIC's more recent submission, which does set out the sorts of situations that they are concerned about. From memory, what they are drawing attention to is that very significant data breaches have happened in the holding of information by government agencies and by commercial or non-government agencies—in this case, telco service providers. This has actually happened; it is not just a purely hypothetical risk. But the precise details are probably best put to those bodies.

CHAIR: I have a question in regard to the definition of the terms 'contents' and 'substance' as it applies to sections 172 and 187A(4)(a). Noting the challenges of defining those two terms, do you propose any words that we might consider in constructing a definition or at least if it is redrafted?

Mr Santow: Yes. What we have said at part 4.1 of our submission is that there may be a way of defining it non-exhaustively. I think the Attorney-General's Department's position previously was that if you provide an exhaustive definition it doesn't provide any flexibility. At the moment, you have too much flexibility. So there is a middle way. I don't think we have specifically set out any particular words. On the whole, as we are not a technical agency, we are better placed in responding to the proposals of others. Again, that is an expression of our own humility. I am to consider that further in due course. If we do have something to add, we can perhaps follow that up in writing.

Mr Byrne: Your recommendation 4 relates to external oversight. This is a discussion we have had for a long period of time—which is the issue of warrants. I am mindful of the fact that there are people who will be listening to and watching your testimony but won't be reading your submission. I think it's important to have a discussion on the public record about what your organisation feels about warrants. If you could flesh that out a bit, that would be great.

Mr Santow: Under the legislation, access to metadata does not require a warrant but access to the content of data does require a warrant. What I think has become really clear over the last few years—and this has been set out by authoritative courts and other bodies—is that international law provides that accessing metadata can lead to breaches of human rights, especially the right to privacy. The UN Human Rights Committee, which is the authoritative body that interprets the International Covenant on Civil and Political Rights—which, of course, applies here in Australia—has made that point loud and clear.

I would make another observation as well. The current practice is simply to provide verbal authorisations. But there is no legal framework that sits around that. That's a point that I think is elaborated by the Commonwealth Ombudsman in its submission. What we are saying is that there should be oversight, through a warrant system, for accessing metadata. We don't see that that would unreasonably inhibit—if at all—law enforcement agencies from carrying out their work. If the concern is that having to apply for a warrant might lead an individual who might be the subject of an investigation to try and destroy the information—I don't know how they would be able to do that, because the metadata isn't held by the individual; it's held by the telco. And so we would see that a warrant scheme would provide that additional protection for unintended or other breaches of privacy that are not justifiable, but it wouldn't provide an unreasonable burden on the law enforcement agencies in just fulfilling their basic functions.

Mr Byrne: How would you see that? The committee's explored this, as you'd probably appreciate. What is put back to us from the agencies is that the volume of requests is such that it would be an onerous burden on them to apply for a warrant. What's your response to that? I think you've canvassed it a little bit but just—

Mr Santow: Look, I think it would, first, help to focus the mind of the agency that is seeking the data, if they have that additional—and it's a fairly modest hurdle to overcome to work out whether they genuinely need the information or whether it's just something that is so readily accessible that they may as well have it whether they truly need it or not. Secondly, I think what we've seen over the last 20 or so years is that governments have become more and more efficient in the way in which they create a framework for seeking and granting warrants. While some time ago that may have been a very onerous process, I think now the balance has been struck much better in the way in which warrants can be sought and granted. So we don't see that that would be a disproportionate burden on the agencies.

Mr Byrne: Thank you. Are you aware of any other comparable jurisdictions that do have the requirement that warrants be issued to access metadata?

Ms Renton: We haven't looked at it specifically, but I do know that in the Home Affairs submission they've set out a comparative analysis internationally, which is quite helpful, and a number of the countries listed there need some kind of independent authorisation method.
Mr Byrne: So, as a consequence of that, you'd like our committee to look at—and this is your recommendation—as part of our review, the issue of warrants and whether or not it's possible to build that in as a confidence-building measure and a quality assurance measure.

Mr Santow: That's correct. We also acknowledge that there are broadly speaking two categories: a separate category that applies to journalists—and there's already a warrant regime—

Mr Byrne: Yes, there's already the journalist information warrant.

Mr Santow: And we would endorse the views of some other stakeholders to this inquiry that that process itself can be further improved.

Mr Byrne: I was just going to say: if you were prioritising each of your recommendations, is the warrant the key one?

Mr Santow: It's like choosing between your children.

Mr Byrne: No, it's not really. I didn't mean it that way because you say in your submission if you can't get four, you can go two and three. It's more along the lines of—not seeking to draw that but looking at this from your agency's perspective and in a world where you could get what you wanted—what would be the thing that you would say was your key priority there? So I'm not trying to tease you out to say, 'We'll trade this off;' it really is a genuine question.

Mr Santow: I am a little reluctant to respond to that question because I think the legislation needs to be considered holistically and the benefit of looking at legislation in a review like this—and I think it was very good that this statutory review was built into the legislation so you can look at it by reference, not just hypotheticals but the actual operation of the legislation. Our view is that all of the recommendations are necessary and important.

Mr Byrne: The reason why I ask you that is that I've been involved in this since the inception almost of the scheme. Its precursor, the international security legislation, was tabled in 2013. It was a very specific subset, and I think the thing that's emerging in evidence this morning from you and other bodies that have appeared before us is the unintended consequence—the consequence that the information that's being collected goes way outside of the subset of information that we were looking at. What the chair has helpfully drawn to my attention is that you deal with international bodies. I guess the question is: how do you think people internationally regard our data retention regime? I would be interested to hear from you. Of course I get that perspective directly from enforcement and from agencies from around the world—they tell me what they think—but I don't necessarily get that from organisations like yours and comparable organisations from overseas.

Mr Santow: I'll make a couple of observations, and then my colleague may want to add to this. First, I would again draw your attention to the Department of Home Affairs' submission, which very usefully provides an appendix that sets out comparable regimes around the world.

Mr Byrne: Sorry, but I'll just to cut across you there. Thank you for drawing my attention to that, but this is more me asking you, as an independent agency. I mean, Home Affairs is Home Affairs, and that's all good. They come at this with a very different perspective, I suspect, than what you do.

Mr Santow: Yes, they do, but the only point I'm making there is that it shows that we are something of an outlier in that this is a much more permissive regime and is going to inevitably lead to more limitations on people's human rights like—

Mr Byrne: And that's what I'm trying to tease out. You're saying this right at the end. It would be good to get from your organisation a frank assessment of how you see this scheme and how it's viewed from overseas that helps us, in terms of the committee, to inform our views?

Mr Santow: I'm just struggling to find the relevant part in our submission where we refer to this, but the United Nations Human Rights Committee has made observations about Australia's data retention regime, from memory. I'll correct the record if I'm wrong about that.

Mr Byrne: Sure.

Mr Santow: It has expressed concern about the extent to which our legislation impinges on privacy and related rights. And so I guess what we would say then, applying the two observations that I've made—that we're something of an outlier compared to other jurisdictions, and that authoritative bodies that look at this legislation have made statements that, essentially, some of these core provisions go further in limiting privacy and other rights than is necessary to achieve legitimate objectives—that we need to do better. We can do better and we need to do better in making this legislation very targeted at combating serious crimes only and advancing national security, and bringing that within that scope.

Mr Byrne: You used the term 'permissiveness'. Can you elaborate on that?
Mr Santow: By 'permissive' I mean it is permissive in allowing personal information to be retained and then accessed beyond what is strictly necessary to combat serious crime and protect national security.

Mr Byrne: There was one more thing that I wanted to touch on—it was drawn to my attention—about the number of people. When this scheme was first created, there were a very limited number of organisations that should have been permitted to access something. Previously, we had organisations like the RSPCA, local government et cetera that could access this. When I looked at this I thought if there was going to be a legal framework, then organisations like that should not have that capacity. In keeping with what you've said, they should be very serious organisations that are looking at very serious offences. There are some reports of a particular provision, I think it's in one of the telecommunications interceptions acts or another act, being used that gives other organisations the capacity to bypass that and to access the metadata. I have a view that I'll share with you after, but I'd be keen to get your view and the view of your organisation with respect to that.

Mr Santow: Quite simply, we think it needs to be as targeted as possible, and one way of doing that is to be really, really clear on which agencies truly need this information. I think there's evidence that has already been put before the committee that a fisheries agency, a local government agency, has been able to take advantage of this scheme. It's hard to see how those bodies would need this information in order to fight serious crime.

Mr Byrne: I just wanted to add, I guess by way of commentary, that I share your concerns. It's my understanding, and this committee's understanding, that when this scheme was crafted, knowing the intrusive nature of these powers, the committee felt, and people felt, that it should be limited. I would say, on the public record, that I'm deeply disturbed by the number of organisations that, through some dint of legislation, can access that. I'll certainly be doing everything within my power to ensure that gateway is closed. Thank you for your view with respect to that.

Chair: Thank you, Mr Santow and Ms Renton, for appearing today. We'll get a transcript to you so that you can make corrections, and if there's anything further you would like to add, it would be great if you could get it to the secretariat by 19 February.

Proceedings suspended from 10:30 to 10:44
DRAYTON, Ms Melanie, Assistant Commissioner, Regulation and Strategy, Office of the Australian Information Commissioner

FALK, Ms Angelene, Australian Information Commissioner and Privacy Commissioner

WATSON, Mr Brett, Director, Regulation and Strategy, Office of the Australian Information Commissioner

CHAIR: I welcome representatives of the Office of the Australian Information Commissioner 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 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 now hand over to you for an opening statement.

Ms Falk: Thank you, Chair; if I may take five minutes to make an opening statement this morning. Thank you for this opportunity to appear before the committee for this very important review of the data retention regime. The Office of the Australian Information Commissioner promotes and upholds both privacy and information access rights. Under the Privacy Act, I have two functions that are of relevance to this committee. Perhaps unlike the IGIS, I do have a statutory function to monitor proposed enactments and also proposals from government that impact privacy and to seek to ensure that any adverse impacts are minimised. In this opening statement I'd like to set out my role in the data retention regime from my regulatory perspective and then turn to the matters raised in my submission.

My regulatory role pertains to the data regime. In particular, retained data is deemed to be personal information, and service providers, such as the telecommunications providers, are required to comply with the Privacy Act in relation to that retained telecommunications data. This enlivens my regulatory powers—for example, to receive complaints; to investigate; to conduct audits, known as 'assessments' under the Privacy Act; and also to educate and monitor service providers' handling of retained data. Entities are also required to notify my office of any eligible data breach that may occur in relation to retained data. In addition, under the Telecommunications Act my office can monitor and inspect telecommunications service providers' compliance with record-keeping obligations when disclosing telecommunications data to agencies. My office has taken a proactive regulatory approach to monitoring the data retention regime since 2015. We've provided guidance and carried out inspections and assessments of telecommunications providers. Our inspections and assessments of large telecommunications providers have identified both good implementation of obligations and areas where improvement is required. In those cases, recommendations are made and have been accepted by the regulated entities. My office will continue to carry out inspections and assessments in order to assess and address any privacy risks in the system.

Returning to the matters raised in my submission for the committee's consideration, the review of the retained data regime presents an opportunity to consider the operation of the scheme and also to take stock to ensure that the appropriate privacy safeguards are in place for the next decade. Privacy is not an absolute right, but it's well established that laws which intrude upon privacy should be necessary and proportionate to achieving what is a legitimate public policy goal. Some of the privacy issues raised by the Office of the Australian Information Commissioner back in 2015 were addressed in the enacted legislation. However, other key recommendations that sought to establish privacy safeguards to better ensure the proportionality of the regime were not adopted or fully adopted. For example, we recommended that access to retained data be limited to where it is reasonably necessary to prevent or detect a serious offence and to safeguard national security. Our submission to this committee on this occasion reiterates previous recommendations and makes further recommendations designed to address the proportionality of the regime and further mitigate the impact on privacy for the committee's consideration.

In summary, we ask that the committee consider the following. The first is reducing the potential for personal information to be collected outside of what is intended or reasonably necessary under the regime. This goes to the issue that has previously been raised around defining what's out of the regime through the meaning of content and substance of communications. Other submissions to the committee have noted that advances in technology in the time since the commencement of the regime have resulted in the generation of new types of telecommunications data, the status of which may present some uncertainty for the purposes of the regime.

The second proposed consideration is to consider reducing the retention period, noting—from the Department of Home Affairs annual reports—that a high proportion of telecommunications data accessed by law enforcement is less than 12 months old, with the majority of data accessed being less than three months old. To complement that, there is the proposal to introduce an express obligation to destroy or de-identify communications data after a
defined period, noting that the impact of any data breach can increase with the commensurate increase in the volume of data that is retained.

There are three other matters that we ask the committee to consider. The first is that measures to ensure that access to retained data is appropriately limited to agencies operating under the telecommunications interception and access regime and who are subject to those important privacy safeguards set out in the legislation, and that any increases to the agencies who are lawfully able to access that data be set out in the legislation by way of legislative amendment. I also ask that the committee consider limiting the purposes for accessing historical retained data to where it is reasonably necessary for investigation of serious offences and safeguarding national security, more closely aligning with the test for accessing prospective telecommunications retained data.

Finally, consider introducing a warrant system. The introduction of a warrants based system for access is one that was traversed at some length in 2015, and elicits views from law enforcement agencies and the community, as well as those concerned about privacy. My role is to bring to the committee's attention the safeguards that I consider would provide the strongest privacy safeguards, and I appreciate the committee then needs to balance that with other evidence that is provided.

Warrants would provide one of the strongest forms of privacy protection through the exercise of real-time independent oversight over the operations of the regime, noting the operational impact for law enforcement. An analysis of telecommunications data can paint a detailed picture of an individual's location, movements, habits, relationships and preferences, with accuracy and detail that increases in line with the nature and volume of the data is available. As technology in predictive analytic capabilities continue to evolve, the insights that can be derived from telecommunications data will increase in detail and accuracy. While the current legislation reflects a distinction based on the collection and use of telecommunications data thought to be less privacy intrusive than real-time interception, I would ask the committee to consider in this review whether that distinction remains operable and how that might change over the next decade.

There have also been international developments that have been brought to the committee's attention which have emphasised the role of prospective independent oversight and also the utility in limiting the purposes for accessing retained data as important mechanisms for striking the proportionality in the regime. With this in mind, I do recommend that the committee consider limiting the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to investigate serious offences or safeguard national security, and to consider, within the context of all of the evidence, whether a warrant system should be introduced. In the absence of a warrant scheme, I suggest that the importance of the other measures I've outlined commensurately increase. Thank you. That concludes my opening remarks.

CHAIR: Thank you very much, Ms Falk, for the orderly evidence and for being comprehensive and getting to the point. We do appreciate that. In your view, what would be the appropriate period for data to be retained that would best balance the need of agencies and the rights of Australian citizens?

Ms Falk: It's a very important question. It's a complex question. Without wishing to sidestep the answer in any way, I acknowledge that the committee will need to hear evidence from the law enforcement agencies and to assess their perspective. What I'm looking at is what's on the public record from the Department of Home Affairs, which indicates the majority of accesses are under 12 months with, I think, only two per cent being outside that time frame.

So it does bring to question the proportionality of the regime. I appreciate that there may be very meritorious matters that lie outside that 12 months. The question is: where does the parliament draw the line to ensure the limits on a system which is an indiscriminate collection and retention of millions of Australians' personal information who are not under suspicion? So it's with that context that I think the committee is well placed to look at the issue of how long the data should be retained.

I'd also draw the committee's attention, as other submitters have, to international developments and the fact that whilst Australia always needs to make up its own mind, in terms of what fits its domestic context, we operate in a global environment with global data flows from the perspective of law enforcement agencies but also from my perspective as a regulator regulating personal information that knows no borders. From that perspective, I do have regard to international developments and note that we are more of an outlier, in terms of the length of time that data's retained.

CHAIR: You recommend that we amend the TIA Act to put upon carriage service providers an express obligation to destroy or de-identify metadata after a set period. Are there any risks associated with such an amendment?
Ms Falk: I think it would need to be carefully considered. I've heard evidence of the Commonwealth Ombudsman this morning raising some issues, I think, around also needing to ensure that records are kept and can be inspected and the appropriate oversight can occur. But with that in mind, the nub of the issue that I'm asking the committee to look at is whether it would enhance privacy protections to have a clearly defined time for deletion of data.

In my mind, in 2015, when the two-year retention rule was implemented, I had anticipated that at the end of that two years the data would be deleted. What we're finding, from our assessments that we've conducted, is that there might be the data deleted in one part but kept in other parts of telecommunications entities for other purposes, like corporations law and so on. I think these matters need to be looked at and some certainty around a cut-off date would, again, assist in addressing the proportionality issues in the regime.

CHAIR: My colleagues will have more questions for you, but the flavour of your submission is that the act needs tightening up, the regime needs tightening up, and I don't hear anyone yet calling for significant overhaul but more accountability, more proportionality and more obligations on those who have access to the data. Is that a fair summation of—

Ms Falk: Yes, it is. I think that we've now had an opportunity not only to have the practical experience of how the regime is operating but also the experience of comparable regimes internationally, and there are some opportunities for tightening up. There are a couple of technical matters, if I may raise it at this instance, that I also think would help with the oversight regime.

CHAIR: Yes.

Ms Falk: One is in terms of the cooperation and collaboration with other regulators. I have some inhibitions because, under section 29 of the Australian Information Commissioner Act, I'm prevented from sharing information in most circumstances. That doesn't mean that we're not relating closely with the Commonwealth Ombudsman on tactics and methodology, programs and so on, but I think it would also be helpful to be able to share findings more fully.

The second—and this is something that we've been considering more recently and is a matter that's been raised by the committee this morning—is that I do think there is potentially a gap in oversight of the disclosure under the Telecommunications Act. Currently, my oversight is to look at the records that are kept by telecommunications companies of the disclosures they've made to law enforcement agencies. They need to keep certain information—the name, the date, the provision under which it was authorised—but they're not required to particularise the kind of information that has been disclosed pursuant to the provision in the Telecommunications (Interception and Access) Act. I think that requirement might provide some additional accountability and it would be something, then, that my office could inspect.

Senator FAWCETT: Could I just follow up on that last point. Concerns were raised by IGIS and others that, whilst an agency may request a dataset in accordance with the legislation, what is provided to them may actually go outside of that and they would not be aware there's additional information. What you're saying is that the telcos are under no obligation to report to you what they have actually provided, so you have no visibility of the fact that they're, in some cases, apparently providing more than the agency is legally allowed to ask for?

Ms Falk: Yes, that's correct. The inspections that we undertake look at the datasets that I've outlined. They don't go into that degree of particularity. The assessments that we've undertaken have looked at disclosures that are made to law enforcement agencies from the perspective of the security arrangements in place and the processes, but we've not had the opportunity to look in that degree of particularity, absent a power that I've suggested.

Senator FAWCETT: Your submission and your oral evidence talked about limiting access to the metadata to serious crimes. What's your definition? How would you see that the regime should define serious crime?

Ms Falk: The regime currently does set out, in the legislation, reference to serious crime in relation to access for prospective information or documents, under section 180. There are some definitions set out there around serious offences or imprisonment for at least three years. I'm suggesting that that's a useful model to replicate for not only prospective retained data but access to historical retained data.

Senator FAWCETT: So you're happy with the current definition; you'd just like it expanded?

Ms Falk: There are no issues that have come to our attention in relation to the current definition.

Senator FAWCETT: Can I just go to the issue of warrants. There's an implied acceptance that, if the serious nature of a crime met the standard from the independent body to grant a warrant, the retention and then access to data would be an appropriate balance of privacy versus national interest. I think I'm correct in saying that.
Ms Falk: Yes. It provides the independent prospective oversight to authorise the access, and we see that that's a stronger safeguard than the current very thorough work that's done by the Ombudsman's office but, nonetheless, after the event.

Senator FAWCETT: Sure. Where I'm going with this is that you, like several others, have said that you think two years is too long for data to be held and that, to balance privacy, it should be limited in time. You, and others, have also acknowledged that small percentage—depending on which metric you use, it's seven or two per cent—may well have quite valid serious criminal actions that are being pursued. If we cut it off at, say, six months and so you don't have to retain data, then, potentially, serious crimes can't be effectively prosecuted. Rather than deleting the data or not requiring it to be held, if there was a requirement for data that was older than a certain threshold to require a warrant, would that be an appropriate balance of still limiting the access to older data but at least it would be there for those instances where the authorities wanted to pursue a serious crime?

Ms Falk: If I go back to my statutory function in terms of advising parliament around litigating privacy risks, a warrant regime that applied holistically would be the stronger safeguard. I appreciate the committee will hear evidence of necessity from law enforcement agencies, and it will be a matter for the committee to weigh up those issues that are put before you. What you are raising, I think, is a methodology for seeking, perhaps, a compromise position which allows access to the data through additional safeguards whilst at the same time allowing the data to be retained. It's that kind of balance that does speak to issues of proportionality and necessity. I note that it wouldn't be as strong as what we're seeing internationally, but it would be a further safeguard than what is currently in place now. Of course, on that basis, it would be a privacy enhancement to the current regime.

Mr BYRNE: I have some questions about telecommunications companies with respect to the datasets that they actually have. Have you or your officers actually physically seen the datasets that are handed over to the agencies?

Ms Falk: No, we have not. We've not seen the actual disclosures. We've seen the documents that are required to be kept under section 306 of the Telecommunications Act, which are the matters that I've outlined around time, date and provision that's been authorised.

Mr BYRNE: As part of quality assurance, do you think that that's something that, with appropriate precautions, you should be able to see?

Ms Falk: I do think that it would enhance the oversight. I think there'd be a couple of things that would assist in enabling that more readily. One is to include within the provision of the Telecommunications Act section 306 subsection (5) a list of the kinds of information that are permitted to be disclosed under the TIA Act. That would then enable me and my office to look at what has been provided. In terms of looking at the actual documents themselves that have been provided, I would likely need some enhancements to my enforcement regime and the ability to compulsorily acquire information in the context of an assessment, which I don't currently have.

Mr BYRNE: Is that something that you would like to have?

Ms Falk: It is something that I would like to have. The government's announced a review of the Privacy Act, and they're the kinds of matters that I'll be putting forward.

Mr BYRNE: With respect to the datasets, do you know where they're stored?

Ms Falk: In relation to the storage—

Mr BYRNE: By the telecommunications companies.

Ms Falk: Our inspections have visited storage centres in Australia.

Mr BYRNE: Do you know how much of the data that's kept by telecommunications companies is kept offshore?

Ms Falk: I have information current at the time that assessments have been conducted, where my staff visited data centres within Australia. I think the question of any current practice, as of today's date, would be best put to telecommunications providers.

Mr BYRNE: But are you aware of it?

Ms Falk: I'm not aware, no.

Mr BYRNE: You're not? They obfuscate about providing that information. When we first envisaged this scheme there was an impression given to committee members at the time that the data would be kept onshore. I can flag with you that it is of some concern to me that data is being kept offshore and we are not being given figures by the telecommunications companies as to what percentage of that information is kept offshore. That
does bother me. Perhaps that's your concern, as well, particularly given the security of that information that's being held by the companies. Have you raised that, incidentally, with the telecommunications companies?

Ms Falk: Under the Privacy Act, Australian privacy principle 11 requires the telecommunications providers to take reasonable steps to secure the data and protect it from unauthorised access, loss and disclosure. And so what we're looking for is to ensure that the controls that we would expect—the access controls, the physical security and the governance—meet that 'reasonable steps' test. The location of the data is one aspect that any provider will need to consider in their risk assessment. They need to ensure that they have the reasonable steps in place. So that's the perspective that we take in looking at it. The location of the data in and of itself is not the issue; it's the security parameters around it.

I think at the heart of what you're raising are issues of data localisation. As we're aware, there isn't a data localisation provision in the law. I'm not submitting that there should be. I note that in the My Health records provisions there is a requirement to store that data onshore. So these are all, I think, valid lines of inquiry with the telecommunications providers for the committee.

Mr Byrne: So, just to be clear for my own purposes, the telecommunications companies don't provide information to you that indicates whether or not this data is located onshore or offshore?

Ms Falk: I didn't have information that suggests that it's located anywhere other than Australia at the time when we conducted the assessments last year.

Mr Byrne: Would you like to have the power to determine whether or not this information is kept onshore or offshore?

Ms Falk: Again, it's a line of inquiry that could be open to me in looking at whether reasonable steps are in place to secure information.

Mr Byrne: The only reason I say that—and, again, it's not trying to lead you down a pathway—is that, particularly given I've had fairly long involvement with this, one of the undertakings that was provided to the committee was that it would be kept onshore. And, all of a sudden, that's not happened. One of the things that was also put to us was that, in the past, the data would be specifically kept or could be kept in a subset of the information that the telecommunications companies would hold. For them to do that, though—and I will be exploring this with the telecommunications companies, should they deem to see it fit to appear before this committee—they were seeking government financial assistance. I've got some evidence, along with the evidence that you've provided today, that leads me to think that that's not happening. That's of concern to me as well. I certainly will be exploring that, because it's not in keeping with what we were told when the scheme was originally envisaged. So I'm pretty concerned about that, particularly the arguments in terms of offshoring and the information that's been provided to us in terms of the amount of data that is being kept offshore, regardless of the commercial things. I know you can't say anything about that, but I'm just sharing my concerns with you given what we were told would occur when the scheme was originally legislated. It appears that that is not occurring. To me, that has privacy implications and security implications as well. I'm aware of the fact that some of those concerns are shared by the agencies themselves that are seeking to access that information. Thank you. You've been very helpful.

Ms Falk: I appreciate the matters that you've raised. Just to make my evidence clear, I don't have information that suggests it is being held offshore, but I appreciate the matters you're raising.

Mr Byrne: I'm not seeking to put those words into your mouth, but it is disturbing that I am even aware of information that's being kept offshore and the fact that that hasn't been provided as a matter of courtesy, almost, as to the integrity plank of our scheme that is your organisation bothers me a lot.

Ms Falk: It is correct that there would be no positive obligation on the telecommunications companies to so advise.

Mr Byrne: No, I understand completely.

Chair: Thank you very much for your evidence today. If there is anything further you'd like to add, could you get it to the secretariat by 19 February. You'll also get a transcript of your evidence so you can make corrections. Thank you.

Mr Byrne: Thank you for your evidence. It was fantastic.

Ms Falk: Thank you.
KFIR, Dr Isaac, Private capacity

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 the 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.

Dr Kfir, I hand over to you for an opening statement.

Dr Kfir: Good morning. I would like to begin by thanking the Parliamentary Joint Committee on Intelligence and Security, the chair, the committee secretary and the staff for enabling me to appear for you. I make this submission in a private capacity. I want to emphasise that I will only speak to the value of metadata retention as it pertains to counterterrorism. I acknowledge the exceptional hard work undertaken by our security services, the federal and state police and the many other public officials and community activists who work tirelessly to keep us all safe from those that wish to do us harm.

In my submission of July 2019 I raised three main points as to why I believe the measure is not effective as a counterterrorism tool. The measure is disproportionate when it comes to counterterrorism; I'll touch on that in the Q&A and in the submission. Such measures help fuel conspiracy theories and support extremist narratives as to the need to undermine the current political system we have. There is an assumption by many within that world that the government already surveils them and, therefore, that they need to find different ways to challenge the system.

On the questions of efficacy and proportionality, I argue that those committed to using violent extremism use a plethora of platforms and develop and maintain their own systems in order to promote their agenda; therefore, the collection of metadata cannot address those. If we are to tackle online violent extremism content and propaganda, we must appreciate that this space is multifaceted. It is also clear that violent extremists are migrating from mainstream platforms either because they're being pushed out due to measures taken by the mainstream social and tech companies or because they believe they are being tracked already.

Violent extremists adapt regularly; therefore, we need to adapt our systems. They also adopt new encryption methodologies. They develop their own software and hardware, including the use of VPNs and end-to-end encryption applications and the use of platforms and tools where there is no regulatory supervisory regime; for example, they use a lot of Russian-made systems. If we are to look to at right-wing violent extremists and the emergence of what has been described as the alt-tech space, there is no publicly available evidence that metadata can breach or help identify the extent of this phenomena because the community is so disaggregated and because it operates on the margins of society.

The final point I will make is that one academic study pointed out that approximately 60 per cent of people were aware of potential terror attacks but only 10 per cent of people came forward and informed security services. The academic study seems to suggest it's because of a distrust in the political system and in the authorities. There is a suggestion that what often happens is that individuals use this claim of surveillance as a way to claim that the government and the security services can't be trusted. I thank the committee and will take your questions.

CHAIR: Thank you Dr Kfir. From the top, are you for repeal of the metadata regime?

Dr Kfir: That's a challenging question. As I said, I can only speak on the counterterrorism aspect. As a counterterrorism measure, I will say it is not effective. I understand that both Vicpol and the other police services have made their submissions and have presented evidence as to why metadata retention is effective. As law enforcement, it might be; as counterterrorism, it is ineffective and, therefore, I would suggest it needs to be revisited.

CHAIR: Are you coming at it from a de-radicalisation perspective rather than a law-enforcement perspective?

Dr Kfir: Yes, very much so.

CHAIR: So, it's not whether it's effective or it is, in an operational sense—I'm just trying to make sure we understand you. Are you saying the metadata regime is operationally ineffective for law enforcement or ineffective for the purposes of de-radicalisation because it fuels, as you say, a conspiracy narrative?

Dr Kfir: Both, I would say. It certainly fuels the assumption that the government is always listening; therefore individuals are migrating to other platforms and therefore it is ineffective in that capacity. So they are not using your traditional methods, like WhatsApp—they'll create their own version. The data that will be collected will be collected from WhatsApp; we are not collecting, as far as I am aware, from TomTom, Telegram or other platforms. They are also establishing their own systems that metadata retention will not be able to collect. So,
there's that aspect. They are already migrating from what the purposes of the measure were. In counterterrorism
prevention, metadata retention might be useful after a terror attack, that's certainly the case, but in terms of
predicting, there is no—at least to my knowledge—publicly available information to show that the retention of
metadata helps foil a terrorist attack.

**CHAIR:** So what sort of amendments would you suggest to the TIA?

**Dr Kfir:** I would simply say that to try to promote it as a counterterrorism tool doesn't work. As a law
enforcement mechanism it does, and I would let the professionals speak to that. But as a counterterrorism expert, I
would simply say there is no evidence to suggest that it works.

**CHAIR:** If I could just tease this out a little bit—if we get inside the head of a garden-variety terrorist who
wants to do Australians harm, whether or not the government's interested in their data doesn't necessarily change
their fundamental assumptions about the world, their cause or, indeed, deter them from doing harm to fellow
Australians. So I just want to get to the core of your argument because I'm not quite following how their
conspiracies or otherwise negate the effectiveness of the metadata regime.

**Dr Kfir:** My argument is simple: as a counterterrorism tool it doesn't work, and therefore we should use the
money for other purposes, whether it is deradicalisation, prevention and other systems. I would suggest to you
that because we are collecting all of that data as a counterterrorism tool we are simply wasting valuable resources
that could be allocated to do other things. As law enforcement, it might be effective to prevent organised crime,
another mechanism, which is, I believe, what New South Wales and Vicpol have made, but as a counterterrorism
tool to try to identify a potential threat, there is no publicly-available evidence to support such a claim.

**CHAIR:** So infiltrating terror groups through human sources—

**Dr Kfir:** That would be a much better source.

**CHAIR:** physical surveillance, other technical means—you're not averse to those sorts of approaches?

**Dr Kfir:** No, a hundred per cent. I think human intelligence, penetration using warrants and working closely
with our partners is absolutely crucial if we are to effectively counter the terrorist threat. But, in terms of just
collecting metadata for counterterrorism, there is no evidence that it works.

**Senator FAWCETT:** My interpretation of your evidence is that there may well be a rationale for spending
the money for law enforcement around organised crime, child exploitation and other things.

**Dr Kfir:** Yes.

**Senator FAWCETT:** So we've already committed the money, but your argument is, 'Don't justify that
commitment of money on the basis of counterterrorism', in which case that's a different argument to amending or
repealing the regime. It just says, 'Don't justify it on the basis of counterterrorism, because there's no evidence.'
Would that be an accurate summation of what you're saying?

**Dr Kfir:** Yes.

**Mr BYRNE:** I think the evidence is fairly comprehensive. Because it is a public hearing, I wanted you to
articulate what platforms you think, say, young people in Melbourne or Sydney who might be radicalised are
using when communicating with each other. I note and read for the public record that you're the head of the
counterterrorism policy centre at ASPI, so you obviously bring a lot of expertise to this discussion.

**Dr Kfir:** I was.

**Mr BYRNE:** You were formally—my apologies. But I think it's important, if anyone is listening to this, to get
an understanding that you are very well-versed in this area.

**Dr Kfir:** They would use TamTam. They would use a variety of DWeb facilities. They would use even the
dark web. They would form their own little niche communication systems. They've moved away from the
mainstream platforms for which the measure was designed in 2015. That's the thing. I'm here simply to make an
efficacy argument. Our resources are limited at best. They are stretched. Again, we haven't even touched upon the
whole issue of languages. As far as I'm aware, we're primarily collecting and assessing data in English. We're not
talking about other languages, which need to be assessed. All of those mechanisms need to be re-evaluated. This
type of legislation might be effective for law enforcement, but as a counterterrorism tool, as far as I'm aware,
there is no publicly available evidence to suggest that it works.

**Mr BYRNE:** There are some statistics that you use in your submission. One of the striking aspects that you
referred to was that you felt—and I don't have the exact figures where you were talking about a certain percentage
of people who might come forth from within a community to volunteer information. Are you saying, of more
recent times, that that's become less as a consequence of people's lack of faith in government and institutions? I
think it's not often enough reported in the mainstream media about how much support we do get from—if we're talking about Islamic extremism, if we want to use that terminology—the Muslim community here in this country. What you've said concerns me a little bit, which is that there's probably less of that, in your experience, given that you're an expert in this area.

**Dr Kfir:** I would suggest to you yes. Three days ago, the Norwegian security services issued a report explaining how they've worked to identify potential terror plots. They looked at 96 cases, and the data seems to suggest a decline in the willingness of individuals to actually report cases. What the data seems to suggest is that about 60 per cent seemed to know that something was afoot but didn't come forward. Only 10 per cent of those 60 per cent actually came forward. Now, again, there are a variety of issues, one of which seems to be a decline in the political system in democracies. There was a study that was issued last week from the University of Cambridge's centre on democracy talking as well about a decline in trust in democratic institutions. I do think we need to be mindful that ethnic minority communities are very concerned about how the data is collected, why it is collected and the ramifications that will come with such collections.

**Mr BYRNE:** That is a good point. Do you think that there was enough discussion with the affected communities when this mandatory data retention regime was implemented? Do you think that there was enough consultation?

**Dr Kfir:** I'm not sure about that as I wasn't privy to those conversations.

**Mr BYRNE:** But you clearly have expertise in this area. You have contact with the communities. To some extent I would ask you then what was the perception of the communities that you deal with and study when the mandatory data regime was implemented?

**Dr Kfir:** The only knowledge that I have is primarily anecdotal, and I would be cautious to expand on it. It is definitely something that might be worthwhile examining in much more depth.

**Mr BYRNE:** One of the key aspects of your evidence was that you were saying that the implementation of this—and we do hear this from some communities. I have some affected communities in my constituency. There was a terrorist event at the Endeavour Hills Police Station and then there was the foiled Anzac Day plot, so I have fairly direct experience in working with the communities there—who, for the record, have been tremendously cooperative. In my experience, they've provided a lot of information to the security services to support them in minimising harm. To some extent, it's useful to get some guidance from you. It's likely that this committee will recommend—without pre-empting it—that the regime be retained. It might be in a quite modified form. With that, and given that we're facing some of the constraints that you faced, what would you suggest to this committee—and this can be part of the committee's recommendations—to further explain and to make people within those affected communities feel less targeted? If we keep this regime, and knowing what you've just said, I'd ask you to advise us on how we would advise or request the agencies to communicate the regime's true purpose and make people feel more comfortable with this regime rather than seeing it as a direct attack on the communities in question.

**Dr Kfir:** Again, I think regular community engagement works. In my experience, Australia is actually one of the leading countries when it comes to good PVE and CVE operations. I often note the successful campaign by the Victorian government of 'Victorian and proud'. I think that element of social integration and the image behind that campaign was certainly positive and helped reinforce the value that we are all Australian. I do think we need regular engagement. I would suggest that over the last couple of years the level of engagement with communities has maybe not being of prime interest, so I would encourage all policymakers at all levels to go back and reach out to communities on that. I would note the excellent work that somebody like Nick Kaldas, the former deputy commissioner of the New South Wales police, did very effectively with communities in New South Wales. I do think we need people like Nick and others to reach out to those communities and emphasise to them that we are all Australians. If you like, take 'Victorian and proud' and make it 'Australian and proud'. I think that would be of enormous value.

**CHAIR:** Thank you very much for your evidence, Dr Kfir. We'll get a copy of the transcript for you. If there's anything further you'd like to add after our discussion, please do so by 19 February.

**Proceedings suspended from 11:43 to 13:13**
BUTLER, Mr Shane, Director Electronic Collection, Law Enforcement Conduct Commission

M ARSHALL, Ms Sarah, Executive Director Operations, Australian Commission for Law Enforcement Integrity

CH AIR: I now welcome representatives from the Australian Commission for Law Enforcement Integrity and the Law Enforcement Conduct Commission to give evidence. Although the committee does not require you to give evidence under oath, I should advise you 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 contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make an opening statement.

Ms Marshall: Thank you for the opportunity to appear before you today. The Australian Commission for Law Enforcement Integrity’s function is to support the integrity commissioner to detect, investigate, prosecute and prevent corrupt conduct in designated Commonwealth law enforcement agencies. ACLEI’s purpose is to make it more difficult for corruption to occur and for it to remain undetected. In accordance with the Law Enforcement Integrity Commissioner Act 2006, the integrity commissioner must give priority to serious and systemic corruption. ACLEI’s investigations have shown that Commonwealth law enforcement officials are at risk of criminal infiltration and corrupt compromise by organised crime groups and those other entities with interests inimical to Australia’s.

ACLEI is unique among those enforcement agencies that are able to access telecommunications data under the Telecommunications (Interception and Access) Act. Firstly, ACLEI has jurisdiction over Commonwealth law enforcement agencies, which themselves have significant powers and access to sensitive information. And we have oversight of agencies including, but not limited to, those agencies which have the power to access telecommunications data.

Secondly, ACLEI faces operational challenges which are peculiar to many of the investigations that it conducts. One significant challenge is that, with very few exceptions, the targets that ACLEI investigates possess knowledge and understanding of law enforcement capabilities, strategies and practices. The law enforcement officials that we investigate are skilled at countering our investigative techniques to avoid scrutiny. This brings a level of complexity to ACLEI’s investigations which is rarely experienced by other Commonwealth government agencies. In order to achieve its legislative mandate, ACLEI requires every possible lawful investigative capability at its disposal. For this reason, in 2006 the parliament equipped the integrity commissioner with a number of coercive powers, for example, the power to compel people to attend hearings, and the ability to issue notices to compel the production of information. ACLEI is also equipped with traditional policing tools and covert information-gathering powers.

While ACLEI's investigations have certainly benefited from the judicious application of coercive and other information-gathering powers, no amount of power to require production of information is of use if the information is not there. The nature of corruption is that it almost always occurs in secret, meaning that it is rarely uncovered immediately—often only coming to light months or even years after the event. The overwhelming majority of ACLEI's investigative work stems from the discovery of indicators of historical conduct. There is often a considerable period between the time corruption begins or occurs, its evolution, its discovery and then, eventually, it being reported. This means that ACLEI's investigations usually only commence a long time after corrupt events have occurred and that a significant proportion of ACLEI's investigative activity is focused on conduct which occurred in the past, sometimes many years previously. There is a view that the retention period for telecommunications metadata should be reduced from the present mandatory two-year retention period to a period of six months or even less. If this were to become a reality, ACLEI's work would be even more difficult than it already is.

I would like to thank you again for the opportunity to appear today. The committee has ACLEI's submission and I would be happy to answer any questions that you may have.

CH AIR: Mr Butler, are you going to make a statement as well?

Mr Butler: Thank you, yes. The Law Enforcement Conduct Commission is an independent body, exercising royal commission powers to investigate, detect and expose misconduct and maladministration within the New South Wales Police Force and the New South Wales Crime Commission. It is a declared agency under the Telecommunications (Interception and Access) Act. We are able to apply for and execute telecommunications interception warrants and, for the purpose of the committee's review, we are also a criminal law enforcement agency able to access telecommunications data.
The general view of the LECC is that the regime has worked quite well since its inception. It allows us to access telecommunications data lawfully but also provides rigorous oversight and requires us to have robust systems in place so that the lawful access of data is ensured. The investigative value of telecommunications data is very high. Whilst we conduct investigations of misconduct of police, we also conduct many criminal investigations, and it's where we conduct investigations into criminal activity by police that we would use access telecommunications data. And I'd like to assure the committee that it is quite targeted. In the last financial year we authorised 459 requests, and of that a substantial proportion—276—was specifically just to find out a name associated with a telecommunications service. For prospective data, to give you a feel, at the moment we are collecting data on six telecommunications services, and it all relates to criminal activity by police officers. So, we believe it's worthwhile.

The systems and procedures that the LECC has implemented include a dedicated system for our analysts and investigators to request telecommunications data access. We require them to go through yearly training to enable them to request data, and within that we require them to turn their mind to the interference with privacy. We also require them to acknowledge that it does or does not relate to a journalist, and we have not sought data for journalists to date. After that, authorised officers must consider the test under 180F of the act. So, we have a double consideration by both the requesting officer and the authorised officer.

We would like to say that the role of the Commonwealth Ombudsman provides, in our belief, a rigorous oversight regime. Our experience is that the Ombudsmen would send four inspectors. We give them full access to our systems. And because we access a comparatively small number of requests, they go through every request, and they will review every request and every authorisation from our agency.

We'd also like the committee to consider that, as Ms Marshall pointed out, the particular crime type around corruption relates to a pattern of behaviour that occurs over a number of years and is often not detected immediately. We find in our statistics that certainly more than half of our requests, where the data is dated—there is a lot of undated data, but where the data is dated—is more than six months old, and around 20 per cent from last year was over two years old. In fact, we've requested data four, five or six years of age. So, those operations would be compromised if we didn't have access to those data.

We'd also like the committee to consider that under section 68 of the TIA Act we are able to disclose lawfully intercepted information, which we regard as much more intrusive, to police for the purpose of disciplinary proceedings or for the police commissioner to consider the suitability of a police officer. We can also, under that same section, disclose lawfully intercepted information to police or other agencies for their criminal investigations. With the data retention regime we are unable to disclose telecommunications data to police except for criminal investigations. We would like the committee to consider provisions similar to that of section 68 to be included under section 182 where we may provide information to police at the end of one of our investigations so that they may consider non-criminal issues but issues around the suitability of police officers. This may relate to associations, for example, with known criminals and issues like that, where they have obligations to declare but haven't done so. Finally, I'd like to thank the committee for inviting us to help assist in your inquiry.

CHAIR: Thank you very much. This question is for both of you. Are you quite happy with the minimum period of two years for retaining data for operational purposes?

Mr Butler: From our perspective, we do access data further back than two years, and some of that data recently has been in support of direct evidence towards fraud and other criminal conduct by police officers. We understand that you must balance the community's views, so we do support the two-year retention period, but we are currently able to request and receive data beyond that two years, and we do. We do rely on that for some of our investigations. The last financial year was around 20 per cent of that dated data. The year before it was closer to 30 per cent.

CHAIR: So if we treat the two years as a maximum, it could potentially compromise your investigation of—indeed, not just yours but our law enforcement agencies' ability to investigate legacy cases, missing children—

Mr Butler: Definitely.

CHAIR: You name any list of potential offences.

Mr Butler: Yes. I have a policing background. I think the crime type of corruption tends to rely on more historic data compared to many other crime types. But certainly in a general law enforcement community there would be many other crimes that do date back beyond two years, where data would be a fundamental tool, if available.

CHAIR: And if not? It might potentially be the only lead we might be able to get, for example, on a cold case?
Mr Butler: There certainly would be occasions. I wouldn't want to comment on police activity, but I'm certainly aware of cases in the media where corroboration of certain evidence, certain phone calls made historically, would be vital to either corroborate or exonerate people. So yes, it definitely makes sense that it would be beneficial beyond two years. Certainly for our agency it would be.

Ms Marshall: By way of example, ACLEI has a current operation, which I won't go into too much detail about, whereby we were notified of a corruption issue in the first quarter of 2018. The information had come to light in late 2017. It concerned the possible corrupt conduct of a law enforcement agency back in 2015-16. In order to properly investigate the corruption issue, metadata dating back to 2015 was required. While some telecommunication providers happened to retain that data and we were able to get it, others didn't. That did have an impact on the investigation.

Senator FAWCETT: Can I confirm from your graph at paragraph 50 that last year over 45 per cent of your authorisations were for data in excess of two years?

Ms Marshall: That's correct.

Senator FAWCETT: I think that is a very appropriate scope for ongoing investigations.

CHAIR: I know you're dealing with corruption, but I'm thinking more broadly. In these sorts of public discussions we tend to take a focus on terrorism, for example, but there's obviously a much broader series of offences—child pornography users, traffickers and so on. I just wanted to put that on the record. ACLEI noted that in the 2017-18 and 2018-19 financial years you paid approximately $84,000 to telecommunications providers to obtain data in support of investigations. Is that an imposition as a cost, or is that part of your standard operating overheads?

Ms Marshall: We do have regard to the cost of conducting our operations, which is why we will always take the least intrusive and most cost-effective means of investigating a matter, but we accept the operational costs of doing this business.

Senator FAWCETT: Mr Butler, you've talked about, in your oral evidence, modifying or amending section 182(2) of the T(IA) Act to allow you to pass information to the New South Wales Police Force for disciplinary or other actions. Have you had occurrences in the past where the act has actually prevented you providing information such that people have gone unpunished, uncorrected or not held to account for poor behaviour?

Mr Butler: We conducted a recent investigation where we did, in fact, have an officer who had quite a number of social links to known criminals. We were prevented in providing that to the police. I think that investigation had a satisfactory outcome. But, yes, that's the most recent case where we would have liked to have provided that information to the police commissioner.

Senator FAWCETT: If you had been able to provide that, what would have been different in terms of how the New South Wales Police Force were able to deal with that officer?

Mr Butler: It is standard practice for us, when we finish an investigation, that we would advise the police. In many cases when we aren't going to criminal prosecution, there are still issues that the police commissioner may consider, and that is the police's decision. But that may allow them to manage certain issues, or it may allow them to assess the suitability of that officer. It is problematic when, in many of our investigations, telecommunications data has been accessed and it is part of the information within the reports that we produce. So it is problematic to exclude those aspects of the investigation when we advise police of the outcomes.

Senator FAWCETT: I'm just trying to understand exactly the scope of amendments you're seeking. If we take that example—you've done an investigation, you've found an officer has a bunch of links with organised-crime characters and you report that to the police—can I make the assumption that the act prevents you providing the actual data to the police, but it doesn't prevent you issuing a report saying, 'Officer X has had these associations with organised crime,' such that, on the strength of your investigation and your report, they can still take action against the officer?

Mr Butler: I would agree with you that that is probably, in many cases, the case, because the telecommunications data may not be the only corroborating evidence that we are providing. There would be occasions where it is the primary evidence, and we would be prevented in those cases, I would think—

Senator FAWCETT: Sure, but I'm just trying to understand the relationship between your body and the weight of authority of one of your reports. Do you need to disclose the actual evidence to the police or, having done the investigation, is your report sufficient, without the physical evidence being in it, for the police to take action or do they need that evidence to act on your report?
Mr Butler: It's case by case, but, yes, in many cases we are able to exercise our functions without that restriction. But, for example, in a hypothetical situation, it's not uncommon for us to be investigating allegations of, say, police providing information to criminals, such as tipping them off before the execution of a search warrant—things of that nature. An investigation of that type would certainly rely on scrutinising the phone records if we had alleged officers' names or certainly the criminals involved. In a simple case like that, if we were to uncover certain communications through those phone records, that would be very strong evidence that we would provide to police. In that case, you could think that there's criminal conduct, and so that would still be permissible under the act. But, but in less clear, more vague, cases, we couldn't provide that. Sorry to ramble on a bit, but I think to answer your question: we are able to exercise our functions without that explicit power, but there would certainly be some instances where we would be hampered.

Senator FAWCETT: Sure. I'm just trying to think through what you need so that, if there were to be an amendment, the amendment would be practical. So, if you discover conduct that is serious enough that you are going to go to court, you'll obviously tender that as evidence?

Mr Butler: Yes.

Senator FAWCETT: So you can communicate the data if a judicial process is underway, but, if it's a disciplinary process within the department, you are prohibited from making that data available?

Mr Butler: Exactly right, yes.

Senator FAWCETT: If the act were amended such that you could publish, so to speak, the data for a judicial process or a disciplinary process but you couldn't just provide it because you thought Harry might be interested to see it, would that achieve the outcome that you are after?

Mr Butler: Yes. We believe the provisions under 68(d)(ii,iiia) and (iii) are written exactly for that purpose, for all telecommunications interception product. We believe similar provisions under 182 would fit the bill for us.

Senator FAWCETT: Sure. Ms Marshall, I just want to put on the record the comment I made before we started; that is, that the inclusion of case studies in your evidence is very useful. It makes it very clear to the committee and to members of the public who are looking to us to try to find that balance between privacy and protecting the rights of Australians but giving agencies the powers they need. Those worked examples demonstrating the serious nature of the crime as well as the time frames, the role this information provides and that percentage in a graph are very useful to help us as we weigh up those two things. So for any other witnesses reading the Hansard or hearing this, please include more worked examples.

CHAIR: The gold standard. Can we talk about over the top communications services and how that is impacting your operations? Obviously it makes accessing metadata difficult, especially when used with a VPN. Can you just give the public a sense of how that's changing the way you do business?

Mr Butler: We have an appreciation of the use of over-the-top services through our interception activity. Through the interception activity we are able not to access the content of those communications but we get an appreciation for the use. It is absolutely true that many of our targets use over-the-top services, particularly I think with our crime types. Law enforcement officials are very surveillance aware; so they certainly would use encrypted communications to conduct any criminal activity.

CHAIR: By end-to-end encrypted applications we mean WhatsApp, Signal—

Mr Butler: Yes, exactly; WhatsApp, Signal, Facebook Messenger.

CHAIR: Confide and all those?

Mr Butler: Yes. I would say that access to telecommunications data has been a fundamental tool ever since I've been in law enforcement—so over 20 years. There's obviously a degradation of the effectiveness through the use of over-the-top services; however, I would say that, at this current point in time, we still rely heavily on analysing telecommunications data. Whilst brazen communications over encrypted apps may well be happening, we will still get intelligence value and sometimes evidence through analysing their phone call activity and any text messages that we capture under this regime.

Mr Byrne: The chair was interested in whether or not you use Confide, and we've just been googling what it was.

CHAIR: The old timers to my left have never heard of Confide.

Mr Byrne: We'd never heard of it, but now we've learnt something.

CHAIR: There you go. Welcome to the 21st century!

Mr Byrne: I'm still trying to get there!
CHAIR: Do you have any further questions, Deputy Chair?

Mr BYRNE: Yes. Are you able to shed some light on the level of authorised officer that would be requesting the metadata?

Mr Butler: For our agency, we have two directors. I'm one of them. A director is a senior executive officer. We have two managers who would be equivalent to, in the Commonwealth, an executive level 2. They are the levels of officer.

Mr BYRNE: So they are the only people who are then authorised to request metadata from the telecommunications?

Mr Butler: Request?

Mr BYRNE: Yes.

Mr Butler: Oh, sorry. No, they're the authorised officer, so that level of officer would approve a request. The requesting officers are generally intelligence analysts or investigators.

Mr BYRNE: But the process is that, instead of them going directly to the telecommunications providers, they've got to get authorisation from the authorising officer before they would?

Mr Butler: That's correct.

Mr BYRNE: Is there a record kept of that?

Mr Butler: Yes. When the regime commenced—our agency was actually the Police Integrity Commission at that stage—we augmented our case management system, so there are dedicated modules and a platform for these requests to be made. We give full access to the Commonwealth Ombudsman to see everything that occurred when the request was made. For example, there are two fields that the requesting officer must fill out. There's the purpose: 'What is the investigation about? What offence are you investigating? What are you asking for?' Then there's another field: 'What is the purpose that you will use this data for?' Then we require the requesting officer to consider the same test under 180F—the proportionality test and interference with privacy. They put that request into the system. An authorised officer, who is a senior officer of the agency, will then review that request. They may reject it or they may approve it. They will then be required under law to apply that test.

Mr BYRNE: Were you going to say something to supplement that?

Ms Marshall: I was just going to say that, similarly, at ACLEI a request for metadata can be made by any ACLEI investigator or intelligence officer. The request is then considered by one of six officers who have been granted the authority under the T(IA) Act to request information from the carriers to authorise the requests, so to speak. Those officers are me as executive director of operations—a Senior Executive Service band 1—and five operational directors at executive level 2.

Mr BYRNE: Do you have experience, or have things been brought to your attention, where, when some of the data comes to you, you've been provided with more information than you've sought?

Ms Marshall: There have, on occasion, been instances where, for example, carriers have returned metadata that's outside the date range. In those instances, where the returned data is outside the parameters of a request, before any data is released to the requesting officer it is checked very carefully by one of two officers in ACLEI—we're quite small; we don't have an automated process—to see what data has been returned. If it is outside the parameters, we quarantine that material. We report it to the Ombudsman.

Mr BYRNE: Thank you. What length of time would you keep the metadata for? Do you have within your organisation some prescribed or regulated period of time where you would keep metadata for investigative purposes?

Ms Marshall: We keep metadata indefinitely, as there are no destruction requirements under chapter 4, for the purposes of remaining accountable to the Ombudsman and so that it's available for their inspections. We also have occasions whereby the data that we have looked at for the purposes of one investigation is used again. There are times where other players, for example, come to light. So, instead of reinventing the wheel in some cases where that data would no longer be retained, we use that data again.

Mr BYRNE: Thank you for your frankness.

CHAIR: That makes sense. I understand it completely.

Mr BYRNE: As you can see, it's a thing that our committee is grappling with.

Ms Marshall: Yes, certainly.

Mr BYRNE: Thank you.
Senator FAWCETT: For LECC, do you have similar practices—no guidelines as to when you destroy data?

Mr Butler: It's very similar. No, we don't destroy. We do retain. It generally won't be accessed unless there's another investigative need, similar to the ACLEI.

CHAIR: For the purposes of an Ombudsman's spot check, do you have every bit of data that you've ever requested?

Ms Marshall: We do.

Mr BYRNE: How many years would that go back, just roughly? This is not a trick question; it's more just for general interest.

Ms Marshall: Indeed. Bear with me and I can probably tell you. I think if we go back to 2015-16 we can identify metadata checks, so to speak.

Mr BYRNE: Obviously, there will be a discussion about the destruction of data. I take it from what you're saying that you would want to keep that data, as you do, indefinitely rather than have a mandate where invariably you would be required to destroy it after a period of time?

Ms Marshall: It certainly would be useful for other investigative purposes.

Mr BYRNE: Sure. Again, it's something that the committee is probably going to have to look at in terms of the other agencies and their length of time, so it's just useful to get.

CHAIR: Thank you very much for your submission and for your evidence today. We appreciate it. We'll get a transcript of your evidence for you so you can make any corrections. If there's anything further you want to add, forward it to the secretariat by 19 February, please.

Proceedings suspended from 13:47 to 14:11
Evidence was taken via teleconference—

CHAIR: I now welcome representatives of the Law Council of Australia to give evidence. 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 contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. Would you like to make an opening statement?

Dr Neal: I thank the committee for the opportunity to provide evidence on the mandatory data retention regime. The Law Council welcomes the opportunity to speak to its submission made in relation to the operation of this legislation. The Law Council acknowledges that the mandatory data retention scheme seeks to pursue the legitimate objective of addressing and preventing serious crime and threats to national security; however, the mandatory data retention scheme can significantly impact on the privacy of all Australians, not just those suspected of crime or people of national security interest.

In the five years since the mandatory data retention scheme has been enacted there have been significant technological developments and today more can be gleaned about an individual than ever before through the telecommunications data and the application of data analytics, which takes advantage of real advances in artificial intelligence. With that, we note that these possibilities are going to magnify with the advent of 5G technology.

Despite the scheme not permitting access to the content of communications, a certain amount of metadata about an individual may provide sufficient information to construct a complete profile of that individual, particularly if it is matched with publicly-available records. Indeed, the Court of Justice of the European Union held in Tele2 Sverige that access to traffic and location data can 'allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained'. The court found the relevant data may provide a means 'of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.' The mandatory data regime can also expose the extent of otherwise confidential communications between journalists and their sources or lawyers and their clients. Access to telecommunications data by law enforcement and intelligence agencies must, therefore, be governed by a robust legislative regime that safeguards data security and only places necessary and proportionate limitations on the right to privacy and communications where the community has an expectation of confidentiality. To this end, the Law Council considers that serious questions remain regarding the scheme's proportionality. If the mandatory data retention scheme is to be maintained, significant amendment is required.

The detail of the recommendations that we are making is contained in our submissions, but, in summary, the recommendations include as follows: that the data retention period should be reduced from two years to no longer than the minimum period required by law enforcement and security agencies, that the primary legislation should expressly list the agencies which can access the stored communications and telecommunications data, that an independent court or tribunal should authorise by a warrant access to the retained telecommunications data, that the ambiguity around when a journalist information warrant is required should be addressed, and that, lastly, standards for the security of telecommunications data should be developed and compliance with such standards, monitored by the Australian Communications and Media Authority. Those are the main points in summary. We now welcome questions from members of the committee.

CHAIR: Thank you, Dr Neal. Going straight to the recommendation that we amend the act so that the retention of metadata is only for the minimal period required by law enforcement agencies, how would you respond to law enforcement who would argue that retaining it for longer than that would potentially help with legacy cold cases—for example, missing children or, indeed, the trafficking of people—

Senator FAWCETT: Ongoing cases.

CHAIR: ongoing cases of significant public interest beyond the usual discussion around terrorism.
Dr Neal: The real issue that you're raising is a question of how one balances the right of the whole population to privacy versus what appears from the data to be a relatively small number of such cases and with questions about whether or not this information is particularly useful in those respects. It has to be conceded that collecting almost whole-of-population data on the whole of the Australian population plus the access to that information by something in excess it would seem of 20 agencies—although there are also other agencies wanting to get access to this data—there comes a time when you say that the demands of law enforcement need to give way to the individual citizens' liberty. We would say that the demonstrated data in what's been provided so far demonstrates that the vast amount of these inquiries pertain to data which is accessed within three months. It would always be possible to say it should be infinitely available, but I don't think that is acceptable either, therefore, to the question about the balance, that's the basis on which we would say the balance should be struck.

CHAIR: Okay. Thank you. Did you have a follow-up on that, Senator Fawcett?

Senator FAWCETT: I have couple of questions for you. I don't know if you had a look at the table in the chart of the law enforcement integrity commission that was showing that in the last financial year something like 47 per cent of their authorisations for metadata were for requests in excess of two years old. You've made the comment that many of them seem to be small and I think that was based on Home Affairs data. But there are other agencies that deal with serious issues such as crime and corruption by law enforcement agencies and officials where the rate, or the percentage, of requests that are in excess of two years are quite substantial. I was wondering if that would influence your view that the period of retention should be dropped to mandatorily to less than two years?

Dr Neal: I don't know whether the other members of our group would want to comment on this but it's still the same issue. The research about the utility of this information is there is nothing that would satisfy a reasonable burden of proof to establish that this data is necessary to achieve those objectives. But if you then compare us with, basically, the five Eyes countries, or the other countries that do in fact have these schemes, two years seems to be the limit that they set too, which would indicate that they strike the balance in the way that we would suggest. I don't know whether Olga or Peter would want to comment on that?

Prof. Leonard: Yes. When you look at the international comparisons, I believe, as the Home Affairs submission notes, that Australia has the longest retention period out of the 28 countries that are listed there except for three jurisdictions—being Belgium, Ireland and Italy. When we look to our Five Eyes counterparts the retention period is, I believe, 12 months for the UK and a voluntary retention period for the US. When we look at two years quite a number of jurisdictions are two years but, interestingly, the two jurisdictions with whom we most closely compare ourselves are, in fact, either shorter or voluntary.

Dr Neal: I would add to this that when you add to the equation, or to this balance, the fact that the access to this data is warrantless—that is, it is not supervised by any independent authority—and as a number of the submissions, we notice, have pointed out the operation of the safeguards that currently exist, which are internal, seem to be a patchy quality to say the most, that, too, affects the balance. If you were having agencies which would have to justify access to that data to an independent body then some of these questions would be quite different. But at the present we don't have that.

Senator FAWCETT: Could you expand on that comment that the internal mechanisms are patchy? The view that we seem to have had from the ombudsman and IGIS, for example, is that the agencies work quite diligently in terms of their handling of their processes.

Dr Neal: They are two agencies. I have in mind what the AFP problem was, and that's to say nothing of the other 20 or more agencies—whatever that particular number is—where we don't have any information. But such a decentralised scheme of accountability—when it seems that even one of the central agencies like the AFP had not sufficiently trained their operatives to know what the requirements were causes a concern. But quite apart from that it's inconsistent with our usual search and seizure type provisions which require warrants.

Senator FAWCETT: I want to go to a different issue. Your submission says that there's a need for greater clarity as to when retained data will be considered personal information under section 187LA of the TIA Act. I wonder if you could expand on that?

Dr Neal: I'm probably not the best technical person about that, but even I, as a relatively untechnical person, think that the idea that the ability to track me through my mobile phone calls, including this one, about what I'm doing in my daily life is quite personal, and it identifies me exactly. I think that the distinction between content and metadata—others have had difficulty explaining that distinction before and I'm not going to attempt it now. I, frankly, think that the idea that the information can track your movements on a day-to-day basis is, obviously, at a common-sense level, personal, and its content.
**Senator FAWCETT:** Would you anyone else like to add to what was written in the submission?

**Ms Ganopolsky:** Are you asking for clarification on paragraph 49 onwards of the Law Council's submissions, in terms of the operation of section 187LA?

**Senator FAWCETT:** That's correct.

**Ms Ganopolsky:** The issue that's stated in paragraphs 49 to 55 of the submission deal with an unusual set of circumstances produced by the difference in the definition of 'personal information' as regulated under the Privacy Act. The concessions that were made to bring all information into the regulatory regime, under the Privacy Act, and compensate for the fact that the definition of 'personal information' in section 6 of the Privacy Act is substantially narrower than many of the counterpart definitions. It sought to cure that deficiency. By doing that, it introduced an element of confusion in that the case law on the point, which is also referenced in the submission—specifically, in paragraph 50—references the definition by reference to information that's about an individual. Whereas here, in the amending legislation, we have language that deals with 'relating to the individual' and, as has already been stated, there then creates confusion as to what information is being handled, especially that there is difficulty in distinguishing between content or otherwise of self-communication style of data that's collected through their activity. There is a technical complexity there with misalignment of definitions.

**Mr BYRNE:** This is not directed to anyone specifically. One of the things that has become quite apparent, and particularly with respect to the evidence this morning, is the issue of data that has been acquired that has been retained by the agencies, and there seems to be no mandated period for when it should be destroyed. Does the Law Council have a perspective that they would wish to share with respect to that or a proposal, in terms of a time frame, or a protocol that it might want to suggest, in terms of the keeping or destruction of the metadata?

**Dr Neal:** I noticed that in the material, and I don't believe our submission covers that aspect, there should—perhaps that's one we should take on notice. In particular, if there's some form of protocol or time limitation, I think we might take that on notice and provide a written submission to supplement what we have said.

**Mr BYRNE:** Could you, please?

**Dr Neal:** I say that without having first asked permission from Dr Molt, who has to do these things, but I hope she would be in agreement with that.

**Dr Molt:** I think we can certainly do that.

**Mr BYRNE:** I think it's an issue that's becoming increasingly pertinent given that initially, when this scheme was mooted, there was some discussion about how long that data would be kept for and what would happen to that data when the agencies had finished with it. Effectively, as the pertinent legislation is drafted, there appears to be no time frame and thus this data can be kept, basically, definitely.

**Dr Neal:** Similar issues arise in other aspects of police work, and we'd probably like to think about what happens in those instances to object to things which have been seized under warrant and the like and try and draw some analogy there.

**Mr BYRNE:** Sure. Thank you for that.

**Prof. Leonard:** It might be worth mentioning the analogy from the privacy space. The federal Privacy Act has a concept that information that is collected for a particular purpose must only be retained for that purpose or otherwise as mandated by law—that is, applying statutory retention requirements where necessary—and must only be used during that period for that purpose. The issue here is a combination of how long that information may be retained and the circumstances in which it is retained, including what notices, if any, are appended to that information and how that information is isolated or otherwise subject to controls and safeguards for such period as it is retained. I think a good reason for us to take this on notice and come back to you is that, as David suggested, the controls and safeguards in relation to the retention of evidence relevant to criminal prosecutions is, I think, relatively well developed, but in this area we would need to consider, together, the issues of how long the information is retained and how clear it is to someone picking up the files, or having access to that information down the time line, that the information is, or should be, appropriately protected.

**Mr BYRNE:** To amplify that, we took some evidence from one of the organisations this afternoon that referred to data being kept and then potentially used by other agencies for other purposes. I thought that was interesting and probably something that I would encourage you to have a look at.

**Dr Neal:** Again, there are analogies with subpoenas and the like and also the taking of body samples and their retention—the idea that they're only allowed to be used for the original purpose and that any other use would have to be separately justified under the standard criteria. So there are some complexities, but there are also some analogies that we can draw on to respond to that question.
Mr BYRNE: Without belabouring the point, I think it's going to become pretty important. It's an area that concerned me, listening to the evidence this morning. I think it's something the committee is going to have to look at. Of course, we'll take evidence from the law enforcement bodies and security agencies, but it's something that has leapt out in particular with the evidence that's been presented.

Dr Neal: Yes, I noticed it in the submissions. I think it is a real issue, so we'd be happy to do some work on it and provide a further submission.

Mr BYRNE: Thank you.

Dr Molt: I might just note that, when the mandatory data retention scheme was first introduced and the Law Council commented on it, we made a recommendation that the legislation should be amended to require law enforcement and security agencies to de-identify or put beyond use in a timely manner data containing personal information obtained by the agencies. I think, from the Law Council's positioning, that would be our principal starting point.

Mr BYRNE: I'm sorry—you were fading a bit, Dr Molt. I think that's been taken on notice, but I would certainly look forward to the Law Council's additional submission and guidance and view on that, particularly given that it's something that is arising. I would certainly be interested in a consolidated viewpoint and a suggestion for the committee to look at, in terms of a way forward, in terms of the data.

Dr Neal: We'd be happy to do that, and we think your point is right.

Mr BYRNE: One of the other issues that came up in evidence which again concerns me is: it is my understanding that the telecommunications companies that were required to provide the metadata had the capacity to store it separately—which was something that our committee looked at previously—or at least to access it. One of the things that concerned me was that the privacy commissioner wasn't in a position to be able to say where the data was stored. We've taken evidence in other fora where there was more detail provided about that which has led some of our committee to be concerned. Does the Law Council have any concerns about that? Something that bothers me is that we just don't know where this data is, and—

Dr Neal: How it's kept?

Mr BYRNE: Yes.

Prof. Leonard: Perhaps I might comment on that. The legislation was intended to create an obligation on telecommunications carriers to supplement their existing data retention practices, and many telecommunications providers already retain relevant categories of data for a period of some years, and the legislation then added that obligation by effectively requiring a superset of data to be retained, and some of that data therefore has been added to existing databases and data warehouses of telecommunications carriers, and other data is retained in the normal course of either customer relationship management or network management. The problem is that, if we endeavour to deal with this data in a different way from the other retained data, effectively that will require telecommunications carriers—those responsive to this legislation—to establish two different sets of data, which, as I say, is a superset of data that otherwise is retained in their system. I'm not aware of issues that have arisen in respect of the carrier side of retention of this data. Such issues as have been referred to in cases in the submissions have related to the handling of data by law enforcement agencies following the access to that data. I just note for the committee's consideration that, if it were to mandate that this data be separately held, that may increase the cost of administration of this scheme and the complexity of data handling for at least some telecommunications carriers.

Mr BYRNE: I thought that, when the scheme was originally conceived, that was something required of the telecommunications providers. It's something that I'm going to need to check separately. This conversation has precipitated me to do so. I'm looking at the secretariat as I'm talking about this, but I do recall and I believe that some of the carriers were offering or were required to provide that specific subset of metadata. When we looked at this from a technical perspective, it wasn't too challenging for some of the major service providers to do that. I think the concern was that, if they did do that, it would have the honey pot effect of letting people know that there was some aggregated data that was held by companies that then could be accessed that was effectively metadata. But it's something that I think the committee needs to look at in terms of—

Dr Neal: I think there was also the issue that the requirement to encrypt the data meant that carriers did need to treat this set of data in a different way to the way some carriers had dealt with retained, amongst other things, metadata separately. My recollection is that the issues that you refer to were around compliance with the requirement to encrypt.

Mr BYRNE: No worries. Thank you for that.
CHAIR: I have nothing further for the Law Council. I thank you once again for a very comprehensive, detailed and clear submission. As always, it helps us in our deliberations. Thank you on behalf of the committee. Mr Dreyfus, Senator McAllister and Senator Keneally send their apologies. They are in a shadow cabinet meeting today on the South Coast. If there is anything further you would like to add, please get it to the secretariat by 5 pm on 19 February. As always, we will get you a copy of the transcript so you can make corrections. Thank you very much.

Dr Neal: Thank you, Chair, and committee members. We welcome the opportunity and we'll follow up with the supplementary submission.

CHAIR: I now declare this public hearing closed.

Committee adjourned at 14:41