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
Members in attendance: Senators Abetz, Fawcett, Keneally and Mr Byrne, Mr Dreyfus, Mr Hastie, Dr Mike Kelly, Mr Tim Wilson.

Terms of Reference for the Inquiry:
To inquire into and report on:

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

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

- the continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill;
- the appropriateness of the dataset and retention period;
- costs, including ongoing costs borne by service providers for compliance with the regime;
- any potential improvements to oversight, including in relation to journalist information warrants;
- any regulations and determinations made under the regime;
- the number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security;
- security requirements in relation to data stored under the regime, including in relation to data stored offshore;
- any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the Telecommunications Act 1997; and
- developments in international jurisdictions since the passage of the Bill.
<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHURCHES, Ms Genna,</td>
<td>Private capacity</td>
<td>22</td>
</tr>
<tr>
<td>DRURY, Ms Alice,</td>
<td>Senior Lawyer, Human Rights Law Centre</td>
<td>10</td>
</tr>
<tr>
<td>FAIR, Ms Bridget,</td>
<td>Chief Executive Officer, Free TV Australia</td>
<td>16</td>
</tr>
<tr>
<td>GILLESPIE-JONES, Ms Christiane,</td>
<td>Director, Program Management, Communications Alliance</td>
<td>27</td>
</tr>
<tr>
<td>McGUIRE, Ms Tess,</td>
<td>Secondee Lawyer, Human Rights Law Centre</td>
<td>10</td>
</tr>
<tr>
<td>SCHUBERT, Ms Georgia-Kate,</td>
<td>Head of Policy and Government Affairs, News Corp Australia</td>
<td>16</td>
</tr>
<tr>
<td>STANTON, Mr John,</td>
<td>Chief Executive Officer, Communications Alliance</td>
<td>27</td>
</tr>
<tr>
<td>ZALNIERIUTE, Dr Monika,</td>
<td>Private capacity</td>
<td>22</td>
</tr>
<tr>
<td>ZIRNSAK, Dr Mark,</td>
<td>Senior Social Justice Advocate, Synod of Victoria and Tasmania, Uniting Church in Australia</td>
<td>1</td>
</tr>
</tbody>
</table>
ZIRNSAK, Dr Mark, Senior Social Justice Advocate, Synod of Victoria and Tasmania, Uniting Church in Australia

Committee met at 08:44

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 the 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 now welcome a representative from the Uniting Church Synod of Victoria and Tasmania 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 evidence given today will be recorded by Hansard and attracts parliamentary privilege. I invite you to make an opening statement before we proceed to discussion.

Dr Zirnsak: Our interest in this particular issue stems from the work we do around human trafficking and also in relation to online child sexual abuse. Our experience in working in this area is that access to metadata is absolutely essential for law enforcement agencies in the pursuit of dealing with online child sexual abuse and the facilitation of that. Overwhelmingly, it is for very serious matters of human rights violations that law enforcement agencies access metadata. That's where we've been a bit surprised with some of the submissions this committee has received, where one would assume the only human rights that matter are the rights to freedom of expression and rights to privacy, and there is an ignoring of other basic human rights, such as the right to be protected from child sexual abuse, as outlined in article 34 of the Convention on the Rights of the Child. Australia also has obligations under the UN Convention against Transnational Organized Crime to prevent crime types including child sexual abuse, and there is the optional protocol on the sale of children, child pornography and child prostitution. There's a need to talk about the balancing of these human rights.

Our understanding, though, with this access to metadata is it helps law enforcement agencies identify networks of people. In the child sexual abuse area, paedophiles often work in large networks. They assist each other. They will help each other target victims and to continue to extort—on that, we also know that, if they know they're under investigation, they may intimidate the victims. They may also try and pay bribes to families to try and make prosecutions go away. So, being able to identify the networks they work in, and disrupt that, becomes very important. Metadata can also help law enforcement understand the travel patterns of these people. Sometimes, if a child sex offender is involved in live webcam child sexual abuse, they may also travel to locations and engage in direct contact offences as well. Having access to metadata might reveal that.

As an example of an investigation, it might be that a bank reports to AUSTRAC examples of a person engaging in suspicious payment patterns that indicate they're likely to be involved in online live web-streaming child sexual abuse, but having the metadata also then will assist in furthering that investigation—identifying whether the person is engaging in and using live web-streaming, and also whether they've travelled to the location where the offences may be occurring and whether they may be engaging in contact offences. The scale of this is quite large. An example of an offender in another jurisdiction we were aware of—in the US—is an offender who spent $175,000 over a five-year period engaging in live web-streaming sexual abuse. Now a session of live streaming sex abuse of children is about US$20 a session. If you calculate that, it's 5,000 to 6,000 sessions that this person engaged in.

Even under our regime that only allows data to be retained for two years, it also then affects the case when you come to think about sentencing such a person when they get caught if police don't have access to data to establish that. You can only put before the court the evidence for the data you've been able to retain. So any suggestion of reducing the data retention period has an impact on the ability of police to gather information when it comes to a prosecution, and therefore impacts on sentencing.

I also find that in this area I'm deeply puzzled and I struggle to get my head around the differences in how we treat different corporate entities in this. If we think about the recent, understandable, critique of Westpac for its failure to scan its users and report that information actively to law enforcement—about child sexual abuse—and yet when it comes to online technology companies, there is no similar regime where they are required to do that.
And, in fact, *The Cleaners*, the German documentary from last year, showed subcontracted content managers who were claiming that they actively see evidence of child sexual abuse and are simply told to delete it without reporting it.

So we have this completely different standard. In the community, if a bank turned up here and said, 'Look, we want to delete all our users' data and only keep three months worth of transactional data,' that would be seen as completely unacceptable, whereas, in the online world, for tech companies and telecommunication companies to turn up and say, 'We want to be able to delete data and only have data available for law enforcement for three months,' is somehow seen as championing free speech and the right to privacy. I do not understand why we treat these entities so differently in terms of that. For the companies, obviously, there is a cost saving in being able to remove and delete data and also not having to assist law enforcement agencies in the first place. Again, as I said, financial institutions and other reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act pick up those costs.

I would urge you as a committee to have empathy for the victims of these serious human rights abuses: children who are raped, tortured and subjected to other sexual abuse; people who are murdered; and people who are subjected to rape threats, death threats, ransomware and sexual extortion online. These are all people subjected to human rights abuses, and that's where the committee's empathy, I think, should strongly lie. Obviously, in dealing with that and giving law enforcement the appropriate powers to deal with that, there need to be safeguards that protect people's legitimate right to freedom of expression and privacy and proper oversight of those powers, but that should not come at the expense of allowing those ongoing human rights abuses to occur without having those powers.

Further, I'm horrified at any suggestion that potential offenders should be tipped off at the point at which an investigation starts—that law enforcement agencies should be required to go to a court to get a warrant and then the offender is tipped off that they're under investigation. Firstly, law enforcement at an early stage may not know all the platforms that a user is using. On my own phone, I'm using the social media platforms Messenger and WhatsApp, LINE and Slack. Law enforcement may know of only one or two of those, so I have the ability to destroy evidence on other platforms I'm in. It also may allow me to contact other people in my network to, as I said before, intimidate witnesses, bribe them or target victims for further abuse. So I think the committee should absolutely reject any suggestion of tipping-off provisions.

I further would argue that anything the committee does that makes it more difficult for law enforcement to access this data will slow the ability of law enforcement to pursue cases and therefore reduce the number of cases that can be pursued. That means, given that the high-tech unit in the Australian Federal Police prioritise their work by the number of children they can rescue and they prioritise those cases where they can rescue children, that anything the committee does that impedes that work means fewer children get rescued and more children get subjected to ongoing child sexual abuse. We've already seen this. The Virtual Global Taskforce's latest report indicates that in Canada, where law enforcement now has more difficulty in getting warrants to access metadata, they have been able to pursue fewer cases to rescue children from child sexual abuse. That is a consequence of making life more difficult for law enforcement.

With regard to the issue of media, from my point of view, the primary issue here is about what the parliament decides should be the parameters around what a whistleblower should be allowed to provide to journalists, and whether our whistleblower legislation is the correct legislation. I do not believe it should be the role of the owners or managers of media companies to decide what information a public servant is permitted to leak to a journalist and then have published. I notice there appears to be a bit of a double standard for some of these companies, because when you look at media reports you see what they themselves do when one of their employees leaks information. For example, in the case of the leaking of Janet Albrechtsen's pay, News Corp mounted an internal investigation to punish the person who leaked that information. So clearly there are parameters by which a company says in your work contract, 'You can't leak information,' and in some cases—for example, with Apple—when workers leak information, they are prosecuted. Apple seeks their prosecution. So I think that whistleblower laws made by parliament need to ensure that public servants can make appropriate disclosures when perhaps a government or a department is engaged in unlawful activity or maladministration—things that are definitely in the public interest—but it shouldn't be a free-for-all where a public servant can simply decide to leak information and it's the media company that decides whether that was in the public interest.

Finally, I also think that, in that space of the media, there are risks that journalists themselves can be offenders, and we did cite a couple of examples of that. It's very rare; I'm not going to suggest that's a huge risk. And, obviously, there is the concern around the media corporation itself not being tipped off or having too many powers if it itself has engaged in criminal activity. The *News of the World* case is a classic example of that. We
had 13 prosecutions—very serious offences—out of that. We had bribery of police—in this case, by a news outlet whose head corporation operates, obviously, here in Australia. So there are issues here about the committee needing to seek the right balance about media corporations also not being above the law. I'm happy to take questions at that point.

**CHAIR:** Thank you, Dr Zirnsak. We'll go straight to Senator Abetz.

**Senator ABETZ:** I have two very quick questions. I note that you appear on behalf of the Synod of Victoria and Tasmania. But would it be fair to say that if you were to start talking about this issue most people amongst your membership and congregations would draw a blank? Would that be a fair assessment? So, really, you're coming from a higher level within your organisation, not on the basis of all the congregations in Victoria and Tasmania supporting this particular submission.

**Dr Zirnsak:** No, I wouldn't agree with that at all. When the previous government introduced access disruption to child sexual abuse material through section 313 of the Telecommunications Act, we ran petitions and we did work around online child sexual abuse, and it was one of the issues we had the strongest engagement from our members around.

**Senator ABETZ:** On child sexual abuse, without doubt. But my question was in relation to the specific of retention of metadata.

**Dr Zirnsak:** I think that our members would understand that law enforcement need appropriate tools to be able to pursue that and I think—

**Senator ABETZ:** Yes. But the specifics of metadata is what I'm trying to get at. But it's not a—

**Mr BYRNE:** I'm trying to work out what the basis of this question is.

**Mr TIM WILSON:** I think the point is who he is representing; isn't it?

**Senator ABETZ:** Yes. When an organisation comes to us saying—and they're quite right to say—they represent a large group of people—

**Dr Zirnsak:** Sure.

**Senator ABETZ:** I just want to drill down to the membership base and their understanding of the issues. That is why I gave the get-out, if you like, and I think it's a fair point, that this is of a higher level within the Uniting Church. And I would accept that, because I would not expect the average punter in the Liberal Party, for example, to understand all this metadata issue—

**Mr TIM WILSON:** Maybe in Tasmania!

**Dr Zirnsak:** My comment on that would be that, in our submission, we provided the resolutions of the church, as you correctly identified. But, obviously, yes, for high level principles, the members of the church leave the intricate detail of the specifics of the legislation to the staff they employ, who pursue the high-level principles that they have passed.

**Senator ABETZ:** So are you happy with the current law as it is?

**Dr Zirnsak:** I would argue that the issues raised by the Commonwealth Ombudsman are certainly worthy of this committee exploring and addressing—those issues of being able to clarify operation of the law, around when data destruction could occur, the greyness about verbal approvals. All those things that the Commonwealth Ombudsman's submission raises I think are definitely worthy of the committee's decision. They weren't raised in our submission because, at the time, we weren't aware that they were issues that, obviously, the Commonwealth Ombudsman was coming to.

**Senator ABETZ:** But the length of time of retention?

**Dr Zirnsak:** As we mentioned in our submission, we actually think that, for the reasons I outlined, the time should, if anything, be longer. Often, particularly when it comes to child sex abuse offenders, because they work in networks, the further back you can go the more you can see who they've interacted with and what their relationships are, and you'll be able to identify more and more both other offenders and also who they have interacted with in terms of suppliers of victims. So, in live webcam child sex abuse, it is an adult—often a relative of the child—who is facilitating that. Now, if an offender has done that over a period of five years, they don't just go to one family to commit this abuse; they make multiple payments across many, many families. Being able to get that history will allow more children to be identified and potentially rescued. That is very important. Obviously, the committee needs to weigh up the benefits of the ability to do that and of being able to rescue those children versus what the additional cost to the companies would be in having to retain data for longer. But we certainly would not wish to see any reduction in the two-year period, which is also the position of Home Affairs, I
note. And I note that Home Affairs' submission also did indicate that law enforcement agencies indicated the benefits of being able to extend the period of data retention.

Senator ABETZ: Thank you.

CHAIR: Just for the avoidance of doubt, but without getting into the intricacies of church polity, you're here representing the congregant members and parishioners of the Uniting Church of Tasmania and Victoria.

Dr Zirnsak: Correct.

Senator FAWCETT: Thank you firstly for the work you do but also for your evidence to the committee. We've had other submissions to this inquiry, and I refer here to the submission by the Allens Hub, who argue that the scheme has not demonstrated its effectiveness and that there has been 'no robust, independent evidence-based scrutiny of claims and assumptions about the necessity of the scheme, its proportionality or its effectiveness'. Now, you mentioned at least one report, I think it was a global report, and it referred to Canada and the fact that they've been able to—

Dr Zirnsak: The Virtual Global Taskforce report—I'm happy to provide you with that.

Senator FAWCETT: Are there other reports, case studies or things in the broader global community, other than from law enforcement agencies, who tell us how vital it is to their work, highlighting the efficacy of metadata as a law enforcement tool that you can actually point to as evidence so that we can put them on the record?

Dr Zirnsak: Yes. Certainly the Canadian Centre for Child Protection work would verify their importance in this space. But, by and large, it is space that law enforcement get the access to and—

Senator FAWCETT: But people are very sceptical, though, about law enforcement seeking more powers—

Dr Zirnsak: I understand that.

Senator FAWCETT: which is why your evidence, as a civil society advocate, is powerful in this space.

Dr Zirnsak: I think the issue there is obviously that law enforcement, for very obvious reasons, are very careful about what they put in the public arena because, every time they reveal a capability or a technique they use, offenders can play to that. They can play to a skill that law enforcement has. I have sat with law enforcement and listened to some of the things they have to do and the amount of time they have to spend on certain things. Also, because they have to worry that tech companies will tip off offenders and because of the amount of resources they have to waste in certain techniques, they don't necessarily want to put those out in the public arena, so it does tie their hands. And I think, on this issue, we are running very much into this big problem that we face around trust in government and trust in public institutions.

I would have expected more of the submissions to actually wrestle with the questions of how you balance the basic human rights of the state needing to protect children from being sexually abused and exploited versus the right to freedom of speech and privacy. Yet from what we saw in the submissions it was almost as if privacy and freedom of expression were the only human rights that mattered and these other human rights abuses got confined to being just crimes. So, if you abuse a child—if you rape a child or torture a child—it's not a human rights abuse; it's merely a crime. I mean, it is a human rights abuse. Let's be really clear about this: we are talking about balancing human rights.

But, in terms of going back to your original question of whether there are other sources, I can have a look at the reports we've reviewed. I would point out that obviously there are lots of other human rights bodies. Again, there is very selective presentation of evidence here. The UN special rapporteur on freedom of expression has made comments, clearly, more towards what is their purview: freedom of expression and privacy. But, if you look at comments by the UN Office on Drugs and Crime, UNICEF, UNESCO, the UN special rapporteur on protecting women human rights defenders, they all see a far more nuanced balance to be struck here and that the state does have obligations to prevent these other human rights abuses while having regard to the freedom of expression and privacy rights.

Senator FAWCETT: I want to clarify one thing. You mentioned journalists before, and you're aware that there's a large degree of concern about accessing metadata to trace down journalists' sources. In recent history journalists at Channel 9 and ABC have been convicted of offences to do with children. If there's a suspicion that the journalist has committed a crime such as this, then your argument is that there should be not a law that exempts them from authorities being able to use whatever means necessary to pursue them, but you're comfortable that, if it's about accessing their sources, then some limitation is warranted.

Dr Zirnsak: I would probably frame it slightly differently. I would say: if a journalist themselves is being investigated for a crime, they should be treated like any other citizen if they've committed that ordinary crime.
we're talking about sources, my point here was more—and I haven't looked at the two cases; I'm only aware of the media reporting—that, assuming the AFP are pursuing these cases because they actually believe there has been a breach of the law, the question becomes: was it appropriate that the information that was provided to the journalist shouldn't have been provided? That goes back to the whistleblower laws. That's what I was trying to say earlier. In other words, the parliament should address that by making sure that public servants have an appropriate opportunity to supply journalists with information when there has been something serious. But, even there, I think the balance has been that being able to supply information to journalists is normally only after internal channels have failed to address a problem. You can imagine that, if a public servant goes to a journalist as the first point of call, there is a danger that that actually tips off people who have been involved in wrongdoing and, again, allows them to destroy evidence and undermine an investigation. It actually allows them to escape prosecution, which is not in the public interest in that sort of circumstance. So my view would be that what needs to be fixed here is any deficiencies in the existing whistleblower legislation that covers the Public Service—the Public Interest Disclosure Act—rather than saying that the way we fix this is to try and stifle law enforcement's access to metadata, which they use for dealing with many other very serious human rights abuses.

Senator FAWCETT: Thank you.

Senator KENEALLY: I have a few questions, but I might just pick up on Senator Fawcett's point. It seems, Dr Zirnsak, if I'm correct in understanding you, that when it comes to journalists—would it be fair to say this?—your contention is that the decision about whether or not to apply for a journalist information warrant should be determined not because of the profession of the person—that is, that they are a journalist—but based more on the type of crime that is being investigated—

Dr Zirnsak: Correct.

Senator KENEALLY: and whether or not it relates to their activity as a journalist or indeed, to put it in other terms, is a crime committed by them outside of their profession.

Dr Zirnsak: I would share the concern that I do not want to see a regime where law enforcement pursue whistleblowers in order to stifle public servants from seeking lawful pursuit of government activity and proper administration in government.

Senator KENEALLY: Yes, I understand that. Thank you. I will just return very briefly to the point that Senator Abetz raised earlier regarding religious organisations and their submissions, because I think it is an important point for us, in this vexed discussion about the role of religious organisations in the public square, to clarify. You have been in this capacity for how many years?

Dr Zirnsak: Twenty years.

Senator KENEALLY: So you've participated in a number of these types of inquiries or submissions, I presume. You said earlier that churches tend to leave to the professional staff they employ the finer details of providing submissions like this, based on the principles and beliefs of the church. Is that a fair assessment of what you said?

Dr Zirnsak: Yes, that would be a fair assessment.

Senator KENEALLY: I'm assuming over that 20 years you've had the opportunity to work in an ecumenical fashion with other religions. Is that correct?

Dr Zirnsak: Yes, that's correct.

Senator KENEALLY: That would have been on similar issues of public policy. Would it be fair to say that other religions also operate in a similar way, broadly speaking.

Dr Zirnsak: Within the Australian context?

Senator KENEALLY: Yes, within the Australian context.

Dr Zirnsak: Other churches do. I think that for some of the non-Christian religions, because they are much smaller groupings, the amount of their resources, and therefore the level of staffing they have at the central level, often stifles their ability to engage in these broader issues. They tend to be more focused on the issues that very directly affect their members, very understandably, for the reasons of—

Senator KENEALLY: Sure, but, on broad issues of public policy where comment has been sought, when major religious denominations make submissions, they tend to operate in a similar fashion to that of the Uniting Church?

Dr Zirnsak: That would be true, but certainly, if members disagree with what we've written, we hear about it.
Senator KENEALLY: I'm sure. In relation to the religious discrimination bills, has the Uniting Church made a submission?

Dr Zirnsak: Yes.

Senator KENEALLY: I am aware that other religious organisations have made submissions to that consultation as well. Would it be fair to say that the Uniting Church's submission there also was done in a similar fashion—that is, largely compiled by the professional staff of the church?

Dr Zirnsak: That is correct—again, guided by existing resolutions of the membership.

Senator KENEALLY: And it's probably fair to say that the other religious organisations have operated in a similar fashion?

Dr Zirnsak: The polity of other religious groups might be a bit different. We are very much driven by the view that God and the Holy Spirit connect with our membership at a base level. We certainly would have had conversations with other denominations where they might hold a view that those who hold more positions of leadership should be setting more the direction of their denomination as opposed to the grassroots membership doing so.

Senator KENEALLY: If I understand you correctly, you're making the point that the Uniting Church has perhaps a more democratic grassroots organisation than, say, some of the other major Christian religions in Australia?

Dr Zirnsak: Yes. I think that would be a fair comment.

CHAIR: And non-conformist too, by the way.

Senator KENEALLY: Thank you. It's very helpful to understand the way religious organisations participate in this public policy conversation. Can I turn quickly to your point about the importance of using the metadata retention requirements to investigate serious crime such as child sexual abuse. I think you provided a strong argument for the usefulness of this regime in terms of addressing and prosecuting serious crime, such as child sexual abuse. We have had a number of submissions to this inquiry—and indeed the public reporting of the way the metadata laws have been used would also show—that there are a number of circumstances where local government are using metadata retention in order to prosecute crimes such as parking violations. Has the church turned its mind towards that broader use of the metadata? Have you considered whether or not this legislation should be restricted to serious crime or not?

Dr Zirnsak: Certainly, we have been very supportive in this legislation being used for serious crime. Whether it is used for other offences—I think that goes to the heart—and there was a quote that the Human Rights Commission provided you with, but they left off the last two sentences that were actually in that paragraph. It was the report of the Office of the United Nations High Commissioner for Human Rights on privacy in the digital age document, which said:

... capture of communications data is potentially an interference with privacy. ... Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.

The two sentences that followed were:

The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.

To my mind, that is the test that actually needs to be applied: is what's going on here arbitrary and is it lawful but also is it necessary and proportionate. If the reason this data was being kept was in order to pursue parking fines, there'd be a really strong argument to say this feels like a disproportionate use of resources—a cost on the industry in order to pursue parking fines. That just strikes me as disproportionate. Whereas, obviously, if we're talking about children being raped and tortured, if we're talking about investigating murders, preventing terrorism, I think the case is very strong that the data is both necessary and proportionate and its use is neither arbitrary nor unlawful.

Mr Tim Wilson interjecting—

Senator KENEALLY: Sorry, Mr Wilson?

Dr Zirnsak: He said, 'It's not a mass surveillance program.' And I would agree with that as well. In the same way that we don't say that the banks keeping all our financial details under the Anti-Money Laundering and Counter-Terrorism Financing Act and running analysis over it to report suspicious transaction patterns—people don't talk about that as a mass surveillance campaign. I don't understand why. If they regard this as surveillance, why is that not mass surveillance?
Mr BYRNE: Could I just jump in. I wanted to commend you for your evidence and remind the committee that they are intrusive powers. What attracts me about your evidence is that you're talking about the purpose that was put to us by the agencies when they asked for this power to be mandated, which was to use metadata to pursue those who committed horrible crimes, like the ones you've been talking about and that you have been advocating for the victims of. I thank you on behalf of this committee for the work that you have done for many years. The concern I have is that we are talking about the most horrendous crimes. Committee members have spoken to the investigators about the effect it has on the Australian Federal Police. At the very same time we become aware that local councils or some other organisations can access those very same incredibly intrusive powers to pursue matters like parking fines. It's horrific that we've created a data set to protect against the very darkest elements of society, and yet a local council can access this. We're talking about social justice. It's one of the most incongruous things I've heard and something that vexes me as a committee member and other committee members. Your evidence to me is amplifying that very issue as to why we need these powers for these crimes, but it also highlights the absurdity of how any organisation doesn't pursue the most serious crimes. You've just given us incredibly powerful evidence about why a local council can access these powers. It bothers me. I know it's a long statement, but I'd like to know if you want to comment on that from that perspective. I see your evidence is being provided to the committee on that basis. You're asking for metadata to be kept for these most heinous crimes, including terrorism, but the evidence you're talking about is the absurd incongruity you have when you talk about perversion of democracy, that a council that can access this for bloody parking fines and stuff like that.

Dr Zirnsak: I would agree. You would certainly not be putting this regime in place in order to pursue parking fines.

Mr BYRNE: This committee and its predecessor committees were given an assurance when we first looked at this. In the iteration in 2011 and 2012 the same arguments were put to me. What would you say? Can I put it back to you: who should have access to this data? Do you think councils should have access to this data?

Dr Zirnsak: It's outside the remit of the resolutions I have here for the church. I'd be expressing a personal view. In part, simply because the whole regime is being called into question because of that, I think there is definitely a case to say that it should be restricted for the most part for these serious crimes. But where there's a grey zone and where I would disagree with some of the other colleagues in this, is that where they're wanting to say that it should only be serious crimes, I would draw a different line as to where serious crime is. In my mind, large scale tax evasion is a serious crime. Some of these submissions say that stealing millions or tens of millions of dollars from the public purse is not a serious crime. Really? I'm sorry, but I'm struggling to agree with that kind of position. Maybe I'm misreading their position. They have this blanket view about stealing money from the government.

Mr BYRNE: Proportionality is the point you're making.

Dr Zirnsak: I am. The use of the power, because it is impacting on the right to privacy and the right to freedom of speech, there is a need to balance it against the other human rights abuses that need to be addressed. What kind of human rights abuse is being carried out when someone parks illegally versus when they torture a child? I think we can understand they are very different human rights. In fact, you might say someone parking in a disabled spot possibly engages in some inappropriate impacts on another member, but it's certainly not the same.

Mr BYRNE: On proportionality, even hearing some of the evidence you've provided makes the committee members feel ill. We can justify the use of this, but the thing that really vexes me as a committee member that's been involved for a long time is that the scheme was created to ensure that there was mandated access to it on the strictest possible basis; and then we've heard accounts about local councils. To me there is no comparison between rescuing a child and prosecuting child sex offenders verses someone issuing a parking fine. I think it's absurd. Where it ties into what Mr Wilson has been saying is that it weakens public confidence in the regime. These organisations that are accessing it when there is no proportionality have no right to access it, in my view. That weakens public confidence and creates a perspective that I have read in the media, which Mr Wilson has read too, about this surveillance state. What we can do to restore public confidence—in my mind, without prejudging other committee members—is to limit who can access and go back to those first principles about who can, so that the good people of the AFP can focus on a regime that they and the public have confidence in, to pursue these serious sex offenders and not allow a parking inspector to chase up someone for an unpaid parking fine.

Dr Zirnsak: A pet violation.

Mr BYRNE: Absolutely.

Dr Zirnsak: I would agree.
Mr BYRNE: There ends the rant. Thank you.

Dr MIKE KELLY: There are two things marrying up—the evil you're seeking to prevent, but also in this case the nature of the way that evil is perpetrated and the technical dimensions to this, which is why metadata is so relevant to it and, as you pointed out too, the time-line aspects of this, which relate to the retention period we're talking about and how these things are constructed over lengthy periods of time using that technology. That marriage of those two things is a big driver here, isn't it?

Dr Zirnsak: Absolutely. To emphasise this point, you can imagine when a financial institution reports to AUSTRAC the suspicious pattern of someone engaging in child sex offences, that's not enough for a court. It's in the public arena, so I can talk about it. The pattern is small payments—$20 to 40 a pop—to various locations. Someone who is making regular payments to a family member in the Philippines will pay in larger amounts because they want to reduce transaction fees, and they pay to the same person regularly. That pattern is very different to a person engaged in a live child sex webcam. But if law enforcement go to a court with that data and say, 'This is the basis on which we want to proceed', the court may say, 'Those payments might be for school books or donations or whatever—that's not evidence.' Law enforcement on the one hand may get all this retained data in transactional detail, but when they go to the tech company to try and match it up against what's been going on in the online world, the data is completely absent. You can't make the case. You're making it really hard for them to be able to build the evidence base they need to put an end to the harm and rescue the children from further abuse.

Dr MIKE KELLY: That is also relevant in sentencing in terms of the magnitude of sentences.

Dr Zirnsak: Absolutely.

Mr TIM WILSON: I'm conscious that Mr Byrne probably slightly verballed me there in his diatribe, but I didn't feel I could necessarily interfere and say that I was disagreeing with him on everything. But I suspect there would be some nuance between him and me. Accepting the fact that there's a challenge around how data is accessed depending on the scope and scale of the legislation, you talk specifically about the issue of warrants and whether warrants should be permissible around accessing data because it could trigger and give prior information, particularly for people who have committed child sex offences and the like. Do you believe there is a threshold test around where warrants should apply? Say the existing system stays as it is, anything below a certain level of crime that would be permissible to get a warrant, but for it to be reversed when it was a very serious crime because of the nature of the crime?

Dr Zirnsak: Particularly with the high-volume crime in the child sex abuse area, my sense would be that if you suddenly required a warrant every time the people in the hi-tech crime unit needed to get metadata, you would greatly curtail the number of cases you could do. That's my greatest concern. There is a concern about tipping off, which is when an offender might be early warned they're under investigation, but even without that, if you said that they had to go to a court and get a warrant every time they want metadata, talking to law enforcement, who have to do that, it's a huge impediment and reduces the number of cases they can work on. The proposition you were putting to me was, let's say that that regime continues to exist for the very serious crime, but for minor crimes you introduce a warrant regime—

Mr TIM WILSON: A parking offence is not a crime; it's a civil penalty, but that's what I mean.

Dr Zirnsak: Possibly that could be a way to do it. I think it's neater to simply say there is a level of threshold not to do it. If you're going to tie up a court having to deal with lots of warrants on fairly minor matters, that's a use of government revenue. That revenue could be used for much better purposes. We need more money for mental health services.

Mr TIM WILSON: That's a very a dangerous argument to use. I'm not disagreeing with you, but the efficiency of the state doesn't necessarily lead us to better outcomes. There are lots of safeguards we could remove to improve efficiency, where the resources could be used for seemingly better public services, but it removes safeguards.

Dr Zirnsak: What I was suggesting about the safeguard was that a neater and more efficient safeguard is simply to say that there are certain offences that you can't access the data for. So, rather than saying, 'For a parking fine, you have to go to a court and get a warrant, and we're going to use up resources doing it,' you just say, 'You just can't get access to the data for a parking fine.' It's protecting the right of privacy and freedom of expression, and it's actually doing it in a way that's more efficient than going through a court process to get a warrant.

Mr TIM WILSON: I think the point would be that it would be disproportionate, rather than it protecting people's freedom of expression or privacy. I'll leave it there; you've answered my question. Thank you.
CHAIR: Dr Zirnsak, we're out of time, but thank you for the moral argument you've brought to this issue this morning. I do appreciate it. Thank you for your evidence. If you have anything that you'd like to add, could you please forward it to the secretariat by next Wednesday 19 February.

Dr Zirnsak: Sure. I will endeavour to send you some references for effectiveness of metadata from other sources that weren't covered in my submission.

CHAIR: Thank you. You'll also get a copy of your transcript to make corrections. Thank you for your time.

Proceedings suspended from 09:25 to 09:35
DRURY, Ms Alice, Senior Lawyer, Human Rights Law Centre

McGUIRE, Ms Tess, Secondee Lawyer, Human Rights Law Centre

Evidence was taken via teleconference—

CHAIR: I now welcome representatives of the Human Rights Law Centre. Access Now and Digital Rights Watch to give evidence. Although the committee does not require 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 before we proceed to discussion.

Ms Drury: Thank you very much to the committee for the opportunity to appear today, just noting that it is just the Human Rights Law Centre appearing today, but speaking to the joint submission.

CHAIR: Yes.

Ms Drury: We all want to live in a country in a democracy where we have the freedom to live our lives without feeling watched, where the government respects our privacy and treats us as citizens, not suspects. There was a shift in this dynamic when parliament passed the mandatory metadata regime. Before 2015, you could call a friend, text your mum or go for a long drive without fear of being watched. Now every single time every one of us does this, this information is stored and kept on a database somewhere for two years or more. That data can tell a government your daily habits and who you know and can trace your movements. The metadata retention regime effectively turns all mobile phones into potential tracking devices for government agencies. ABC journalist Will Ockenden was reporting on his own metadata, which he managed to obtain, and he found that, on average, his phone logged his whereabouts every 20 minutes. That information is currently available to 87-plus non-law-enforcement government agencies including, as this committee has noted, local councils. They make 300,000-odd applications for our data each year. We will never know who has accessed it because, under the act, it is illegal to disclose when an authorisation has been made. This information is powerful. It's the kind of information that should only be made accessible to law enforcement agencies for the purposes of investigating serious crimes and with a warrant—not at will by local councils chasing down parking fines.

Ms McGuire: The risk that the metadata retention regime poses to a free press has also made headlines this past year. Police have been using the regime to trawl through journalists’ data to find their sources. Democracy requires the free flow of information from government to the public. Sometimes we also rely on brave whistleblowers to come forward with stories in the public interest. The relationship of trust between journalists and their sources is the foundation for investigative journalists to uncover and reveal the truth. This is all the more important given that currently our laws do not adequately protect whistleblowers from criminal prosecution. The journalist information warrants are flawed and are a weak attempt at protecting what is a fundamental part of our democracy. This law should prohibit access to metadata of whistleblowers, journalists and human rights defenders who, in the legitimate course of their work, disclose government wrongdoing in the public interest. Of course the police should be able to use metadata to solve serious crimes, but that doesn't require a system of mass surveillance over all of us.

The committee has an opportunity to fix the flaws with this regime. You could achieve this by: limiting access to metadata to the original 22 law enforcement agencies contemplated by this committee in 2015 for the purposes of investigating serious crimes only; requiring a warrant before those agencies can access metadata; and prohibiting access to journalists and public interest whistleblower metadata except in limited circumstances. These changes are necessary to ensure our democratic rights and freedoms are adequately safeguarded. We now welcome questions from members of the committee.

CHAIR: Thank you. You might have heard the evidence from the Uniting Church earlier. Dr Zirnsak made a moral case for retaining the existing metadata regime. I would be interested to hear your thoughts on his evidence.

Ms Drury: The question really always comes down to one of proportionality when we're talking about human rights. As was noted by this committee in its report in 2015 and consistent with the European Court of Justice's findings in two cases, keeping everybody's metadata, regardless of whether or not there's a link to a crime, is disproportionate to the investigation and fighting of serious crimes. We would say the same thing is very much the case here. Australia is already completely out of step with similar jurisdictions overseas in terms of its metadata retention regime. I'd also note that Dr Zirnsak referred to findings in Canada of how useful metadata has been for combating child abuse. Canada doesn't have a metadata retention regime. So whatever policing has been so effective in Canada could presumably be done here without the incredibly onerous metadata retention regime that we have.
Mr TIM WILSON: You raised that you think the maintenance or collection of the metadata of every Australian regardless of whether they are under investigation or not is disproportionate. I'm just wondering if you could clarify for me your thinking on that. In the physical world, with the retention of any object or fingerprint or anything else that's retained on a surface, regardless of whether somebody has been investigated or not, when you go back and look at it you establish whether there is evidence there or not if you're completing an investigation. If the metadata is retained only for people who are under suspicion then you're essentially denying yourself access to an incredibly large amount of information that you wouldn't ordinarily deny yourself in the physical world. Why do you think the online world should be different?

Ms Drury: With respect, I think the metadata regime is more akin to if the police followed us and collected every single one of our fingerprints wherever we went just in case it was useful to a crime and stored them on a database.

Mr TIM WILSON: That would be true if it were the government, but it's not the government doing it; it is those who have already voluntarily provided that information into systems.

Ms Drury: I would query whether or not people are actually mindfully voluntarily providing that information to the system. They want to call a friend. They want to go from A to B and carry their phone on them. They're not saying each time, 'I consent to my personal information being provided to the telco and being stored for two years by the telco, which can then be accessed by 87 government agencies, plus 22 law enforcement agencies.' If you were to ask people if that is what they were consenting to each time they used their phone or carried their phone, there would be a resounding no. They think—

Mr TIM WILSON: Let's just follow this through. This is the challenge I have with the whole structure of the system. If I, as a private citizen, don't take my phone, get into a car and somebody witnesses me getting in the car at point A, I drive to point B and, say, it's a public place and somebody witnesses me there, I haven't consented to it but the information is still available if it can be established and I can be identified and it can then be used for an investigation, even though I'm not under investigation.

Ms Drury: Let's say there were cameras around in public and everywhere we went was logged, tracked and kept for two years. I think people would have a huge issue with that; we're seeing that currently with the proposal for facial recognition. I think—and this has been found by the European Court of Justice—that just the very fact of recording this information makes people feel watched, which will make them censor themselves. The retention and the gathering of this information is massively compounded by the lack of a warrant system, the extremely long period for which it is retained and the number of agencies which have access. I think the truth of the matter that we're facing at the moment is it's not just the gathering and storing of this information that's the issue; it is also the access of it.

Mr TIM WILSON: I don't think you'd find any argument from me around the access point. Can I just clarify: is the starting point of the Human Rights Law Centre that there should be no regime in place, that there should be but it should only be that information should be retained for those people under active investigation or that the current system should be operational but there should be a limitation on who can access it based primarily on the seriousness of the offence and the agency seeking the information?

Ms Drury: That's right.

Mr TIM WILSON: No, I gave three different propositions. I am trying to clarify which one it is.

Ms Drury: They build on one another. Our first submission is that, consistent with the right to privacy and freedom of expression, there should be some connection—not necessarily suspicion but some connection—to a crime in order for that metadata to be retained. If there is a very brief period for which metadata needs to be retained in order for police to determine what is connected to a serious crime, then we would certainly find that palatable and more reasonable than this two-year retention period for everybody across the board.

Mr TIM WILSON: Thank you.

Mr DREYFUS: Thanks very much, Ms Drury and Ms McGuire, for appearing before the committee. I want to ask some basic questions. When we talk about metadata or telecommunications data, what is it that we're talking about?

Ms Drury: What we're talking about is information that can build a profile of a person. I think part of the difficulty we have in this area, and in getting public engagement in this area, is nobody really knows how to describe metadata. It's better to talk about it in terms of the picture that it gives you about a person. We note that the Inspector-General of Intelligence and Security, Margaret Stone, said that this tells you a lot about a person. You can track their movements, you can track their social networks and you can also match this data with other data that is publicly available to build a very accurate picture of a person.
Mr DREYFUS: Just to clarify: metadata, you've said, can reveal about a person where they've been, their movements and their social networks. What else can metadata reveal about a person?

Ms Drury: I think that's quite a lot about a person.

Mr DREYFUS: Put another way: is there a meaningful distinction that can be drawn between metadata on the one hand and content on the other?

Ms Drury: I think we're increasingly seeing that there isn't a meaningful distinction between the two. Data analysis is becoming increasingly sophisticated. I think that these trends of data being located to a particular person can tell you enough about them, without actually having to see the content of the data; that's consistent with the European Court of Justice's ruling on this. It's on that basis that we say that if you need a warrant to access the content of a communication, you should likewise need a warrant to access all of the metadata or information surrounding that communication.

Mr DREYFUS: I might come back to that point. You've noted in your submission, at paragraph 80, that state and local government agencies are accessing metadata using sections 280(1B) and 313(3) of the Telecommunications Act. That's a different act, of course, to the Telecommunications (Interception and Access) Act, which contains the mandatory data retention scheme. Can you explain how that legal mechanism, the one under the Telecommunications Act, sections 280 and 313, works?

Ms Drury: Certainly. Section 280(1B) allows the disclosure or use of information or a document if the disclosure or use is required or authorised under law. Essentially it means that, despite the TIA bill—as it then was—being heralded as a limiting act on those agencies that can access metadata, in fact, because of the retention of 280(1B) under the Telecommunications Act, metadata can still be accessed by basically any government agency when it has a sufficient purpose at law.

Mr DREYFUS: Just following on from that, why do you say in your submission:
The reality of how the metadata retention regime operates now bears little resemblance to the context in which this Committee reviewed the scheme in 2015.

That's at paragraph 35. How was the scheme supposed to operate?

Ms Drury: The scheme was supposed to operate so that it was only those agencies that investigate serious crime that have access. That's consistent with this committee's recommendation in a May 2013 report as well, I might add. Because it was assumed that only those few agencies—22 agencies—would get access, other safeguards such as warrants were regarded to be unnecessary. Another really important safeguard in terms of reaching a threshold of the seriousness of crime was regarded as unnecessary. What we've seen is that in fact the safeguard of access only by those 22 agencies doesn't apply, and nor do we have those other two safeguards as a result.

Mr DREYFUS: Could you elaborate on your submission at paragraph 32, where you say:

There is no proper threshold relating to the seriousness or nature of the offence to limit access to data.

Ms Drury: That's right. We would say that this law was justified by Minister Turnbull at the time on the basis that it was needed to investigate serious crimes such as murder, terrorism, national security offences. That wasn't actually written into the law itself, so law enforcement can access our metadata in order to protect public revenue, for instance, and, as we just discussed, of course access is not just limited to law enforcement.

Mr DREYFUS: If I can understand with precision what you're saying, it is that, when this committee, in its 2015 report, recommended restricting to a defined, limited set of named agencies, there was, if you like, an implication—in restricting it to effectively a set of state and federal police agencies plus ASIO plus a couple of other agencies that are charged with investigating serious offences—that that would operate as the threshold, because it was only these crime-fighting agencies that would have access, and that was an implied threshold. But that hasn't proved to be the case in practice?

Ms Drury: That's exactly right. We say that both are necessary in terms of amending the act now. We think that only those 22 agencies should have access, but there should also be a threshold introduced.

Mr DREYFUS: Why do you say that there should be a higher threshold so that agencies can only access telecommunications data for the purpose of investigating the commission of serious crimes?

Ms McGuire: We accept that metadata can be an incredibly important tool for investigating serious crimes, but we know that, in order for metadata access to be proportionate, it needs to be limited to those serious crimes. That's just in keeping with human rights principles, freedom of speech and privacy. To us it seems that, if the government justified this law publicly on the basis of investigating serious crimes, it ought to be limited to investigating serious crimes.
Mr DREYFUS: In relation to the other suggestion or recommendation you've made in your submission, which is about requiring agencies to obtain warrants, you've submitted that judicial warrants should be required for access to metadata. We have a submission from the Department of Home Affairs that sets out why, in its view, warrants should not be required. I'm wondering if I can get you to respond to the various arguments put forward by the department. At paragraph 99 of the department's submission, first of all, they've said:

Warrant applications are resource intensive, and can take days, if not weeks, to prepare, review and issue.

For this reason, coupled with 'the current number of authorisations issued to access telecommunications data'—298,691 in 2018-19 alone—they say:

... a warrant application process would become an investigative bottleneck. Can you respond to that?

Ms McGuire: Of course. We agree that the volume of requests being made is incredibly high, as the Department of Home Affairs has pointed out. But we actually see this as a reason for the committee to have concern, not a reason to prevent a warrant mechanism being introduced. A warrant is a simple safeguard to ensure that there is a reasonable basis for the request to access this personal information. The fact that they're pointing to this being resource intensive or taking, potentially, a mere few days or weeks is not a good enough reason, in our eyes, why the process of simply providing a reasonable basis as to why the request for a person's metadata is legitimate should not be introduced in this legislation. Police require a warrant to search someone's home or to gain access to their calendar or diary. As a society, we accept that this mechanism is necessary to protect our right to privacy, and we should extend this protection to metadata.

Mr DREYFUS: Thank you. I will just go on to a further reason that the department advances against a warrant requirement. They say:

It may also have a perverse effect by having agencies jump straight to seeking a warrant for more intrusive powers, rather than the current process whereby agencies use telecommunications data prior to seeking a warrant for ... stored communications and telecommunications intercept—for example. Can you respond to that?

Ms McGuire: Yes. It's an interesting argument to make that law enforcement, if they were to require a warrant, would then want to actually request a warrant for more intrusive data on a person. If they truly needed that data then they could be obtaining a warrant to have access to that in the first place. But we do not see that as a reason that, within this legislative regime, there should not be a simple threshold that the police or law enforcement agencies point to a reasonable basis for the request to access. The fact that in the 2018-19 period there were nearly 300,000 requests for people's metadata is a reason to introduce a basic threshold in this process.

Ms Drury: I have two things to say as well. If the threshold of investigation were reduced to serious crimes only, presumably the enormous volume of requests would reduce in any case. In addition, just to echo what my colleague has said, what this point made by the Department of Home Affairs indicates to us is that metadata is currently being used as a fishing exercise to see whether or not a warrant for the content of communications or otherwise is required. We think that that is inappropriate given the sensitivity of the nature of metadata.

Mr DREYFUS: Finally, the department's advanced this reason. I'm paraphrasing. They say that a warrant requirement could 'fundamentally change the way investigations are conducted', and they give examples of telecommunications data providing vital evidence for agencies to satisfy the legal test to obtain a warrant, such as a telecommunications interception warrant or law enforcement using metadata to rule out innocent parties from suspicion, without having to resort to more privacy-intrusive and costly investigative measures. Are you able to respond to that last reason that's being advanced by the department as to why a warrant requirement shouldn't be imposed?

Ms Drury: I think it's always dangerous to say, 'Unless you let us do this without a proper safeguard in place, we're going to come down even harder.' To me that doesn't sound like a very comforting or convincing argument. I will also just add that warrants are part of common practice in policing, and they don't necessarily take weeks; they can be granted quite quickly. I think this is a case where we now have an enormous amount of new information that is being provided to police. Traditionally, policing practices didn't have access to this kind of data and presumably they were able to prosecute crimes then. We haven't yet seen the case for the number of arrests and prosecutions that this data has led to and how important this data has been to those prosecutions.

Mr DREYFUS: I don't ask for you to have a comprehensive knowledge of the law of the United States but, as I understand it, in the United States warrants are a requirement for the obtaining of this kind of metadata by police and law enforcement agencies.
Ms McGuire: That's right; in both the United States and in the UK now as well. I should also note that the United States doesn't have the comprehensive metadata retention regime that we have here.

ACTING CHAIR (Mr Byrne): Sorry; did you say the United Kingdom as well?

Ms McGuire: That's right.

ACTING CHAIR: So there are two comparable jurisdictions that basically require warrants to access metadata?

Ms McGuire: That's correct.

ACTING CHAIR: Thank you.

Mr DREYFUS: Finally, Ms Drury and Ms McGuire, I have a couple of questions about access to journalists' metadata. For the benefit of those who may be listening to this hearing, can you elaborate on why you believe that the current journalist information warrant regime is ineffective?

Ms McGuire: Of course, and thank you for the question. The current regime is ineffective because it's conducted in secret and without the journalists or their media organisations knowing or having a chance to respond and without adequate protection of sources and whistleblowers of those journalists. We've put forward the recommendation, though, that there should actually be a prohibition on the access of the metadata of whistleblowers, journalists and human rights defenders who, in the legitimate course of their work, disclose government wrongdoing in the public interest. An exception to this could allow law enforcement agencies to access their metadata with a warrant if necessary to prevent or mitigate an immediate threat to a person's safety. But if this current process for obtaining a journalist information warrant is to be retained, then we think there needs to be key amendments made to ensure that there is a notification to the journalist or the media organisation and that there is a contested hearing, that it is public and less necessary for there to be a suppression order, to ensure that this is a transparent and accountable process.

Mr DREYFUS: As the chair did for the previous witness, I would like to thank you for the moral arguments that you've made before the committee today.

Dr MIKE KELLY: In relation to the 'seriousness of offence' barrier that you are advocating, how would that practically be done? What mechanism would you attach that to in terms of defining the seriousness of the offence, just as a practical matter?

Ms Drury: 'Serious offence' is already defined in the act under section 5(d) quite comprehensively. It lists a number of offences and goes on to say that a serious offence is one with a sentence of seven years or more. We're aware of the Law Council's submission that three years or more to be regarded as a serious offence in this instance. One of those two options would seem reasonable to us.

Dr MIKE KELLY: So which one are you advocating—the act definition or the Law Council's submission?

Ms Drury: Given that it's already in the act, that would seem to be the smoother option. We also have some concerns that some offences attract inappropriately high sentences. For instance, under the rule of law, making a prank call can attract a three-year sentence. But we are also sympathetic to the position that some offences—for instance, corruption offences—may not attract a seven-year sentence, and yet, in keeping with public expectation, metadata should be accessible for those sorts of offences.

Dr MIKE KELLY: But you'd be comfortable with the definition for the time being.

Ms Drury: That's right, yes.

Dr MIKE KELLY: In relation to retention periods, you're talking about the shortest period possible, noting that various crimes relate to different time frames. What sort of suggestion have you got to make in relation to the retention period?

Ms Drury: In keeping with jurisdictions in Europe, in those jurisdictions that have a mandatory metadata retention regime, most typically it's six months; some have 12 months. We believe six months is reasonable, particularly given that that's when the vast majority of authorisations for access are made.

Dr MIKE KELLY: So, in accordance with overseas practice, six months is what you're recommending.

Ms Drury: That's right. To add to that, if law enforcement did decide that they required a particular person's metadata for longer because of a suspected connection to a crime, there should be a mechanism by which they apply to a court to have a warrant to have that metadata retained for longer.

Dr MIKE KELLY: So you'd have a mechanism to account for those longer time line offences where tracking is more difficult over an extended period?

Ms Drury: Yes.
Dr MIKE KELLY: Obviously there are a lot of issues associated with the requirement to notify the person who has their metadata accessed, in terms of the impact on the investigation. Is there a point at which you believe a person should be notified, or is that an aspect that could also have some flexibility around it, depending on the nature of the investigation and the offence?

Ms Drury: I think it's certainly an area that can have some flexibility around it. Of course we would never advocate for anything to happen that would undermine an investigation. For instance, if there's a risk of somebody destroying evidence, having been notified of their metadata being accessed, then, as is very common already in criminal procedures, we would say that those would be circumstances justifying not notifying the person, at least not immediately. But, particularly after an investigation has been completed, there seems to be no risk of that, and often, I imagine, there would be times when people could be notified where there's no risk of undermining the investigation.

Dr MIKE KELLY: In relation to warrant regimes, there are obviously ways and means by which warrant regimes can be streamlined very effectively—having duty magistrates and processes by which things can be expedited. Have you looked at templates for that kind of process?

Ms Drury: We are, unfortunately, not experts in criminal law. I've been speaking about this to one of my colleagues who is, and we understand that there are many examples across the different state and territory jurisdictions in criminal law where warrants can be expedited. Warrants can be received over the phone if they're urgently required; I think it's uncontroversial to say that they're a standard part of policing procedure.

ACTING CHAIR: On behalf of the committee, thank you for your evidence here today, Ms McGuire and Ms Drury. If you've been asked to provide any additional information, please forward it to the secretariat by 5 pm on Wednesday 19 February. You'll be sent a copy of a transcript of your evidence and will have an opportunity to request corrections of transcription errors. We will suspend the hearing; we are trying to track down a witness.

Proceedings suspended from 10:08 to 10:15
FAIR, Ms Bridge, Chief Executive Officer, Free TV Australia

SCHUBERT, Ms Georgia-Kate, Head of Policy and Government Affairs, News Corp Australia

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

**Ms Schubert:** Thank you. The Australia's Right to Know coalition of media organisations thanks the Parliamentary Joint Committee on Intelligence and Security for the opportunity to provide evidence today regarding the review of the mandatory data retention regime in the Telecommunications (Interception and Access) Act 1979. Our submission to this review is confined to the operation of the journalist information warrant scheme at division 4C of the TIA Act. We note that, when the journalist information warrant scheme was introduced, it was with bipartisan support in response to our concerns regarding protection of sources, access to journalists' metadata and the ability of journalists to do their work. We thank those members of parliament, from both the government and the opposition, including Mr Dreyfus, who is here today, who were involved in the development of the scheme, which was undertaken in less than ideal circumstances including a very tight time frame and without being able to consult media organisations in any transparent manner.

It was acknowledged then that 'democracy depends absolutely, fundamentally on a free press and journalists being able to do their work'. As we've outlined in our submission to the committee for this review, the good intentions of the journalist information warrant scheme fall short for a range of reasons outlined in our submission, including that the scheme is cloaked in secrecy and does nothing to address concerns relating to the identification of journalists' sources. In our view, the journalist information warrant scheme, and other legislation relating to access to journalists' records more broadly, requires fundamental reconsideration and immediate amendments.

As we put forward in our submission, our starting position is that an exemption from the law for public interest reporting should be enacted. We also said that, if this was not successful, the scheme must be overhauled, and we outlined key aspects of what this should incorporate. For the purposes of this hearing, we focused on the following recommended amendments to the journalist information warrant scheme: (1) a journalist information warrant scheme is required for all warrants sought under the TIA Act when the subject of the warrant is a journalist or media organisation or the material and how it relates to operating in those professional capacities; (2) an application for a journalist information warrant must be contestable by the parties to a higher authority and authorised only if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in not granting access; (3) the journalist information warrant scheme must apply consistently to ASIO and all other enforcement agencies; and (4) there must be transparency across all elements of the journalist information warrant scheme.

We acknowledge that we have amended our position regarding our original recommendation in our submission of 4 July that the journalist information warrant scheme must first be approved by the Attorney-General before applying to an independent third party. We have made that change since engaging in further consideration about how a contestable warrant scheme to a higher authority should apply to the application for all warrants concerning a journalist or media company and not just to the journalist information warrant scheme.

To that end, we note that, in December last year, the Australia's Right to Know coalition of media organisations made a detailed supplementary submission to the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the media. That submission includes a framework for contestable warrants to apply to all warrants issued under Commonwealth law, noting the importance of balancing the public interest in a free media and the legitimate interests of law enforcement. We look forward to engaging with the PJCIS inquiry regarding the details of our supplementary submission to that inquiry at a suitable time. Today we welcome the committee's questions regarding our submission to this inquiry: the review of the data retention laws regarding the journalist information warrant scheme.

**ACTING CHAIR:** Thank you very much.

**Mr Dreyfus:** Thanks very much, Ms Schubert and Ms Fair, for appearing. As you've just pointed out in your introduction, there's a direct overlap between the committee's inquiry into the mandatory data retention scheme and the committee's still-current inquiry into press freedom. We had hoped that the press freedom inquiry would have been completed by now but we're still waiting on two submissions from the government, which is
why that inquiry has been paused. We're in the somewhat unusual position of you not having the committee's report on the press freedom matter at all and we're here embarked on what is a statutory review, which we are due to report on by 13 April and we will do so. I say that by the way of introduction to my questions, because it may very well be that we report first on the questions raised in respect of the mandatory data retention scheme and are not at that point in the position of having reported on the press freedom inquiry.

With that preliminary out of the way, has the introduction of this mandatory data retention scheme in the telecommunications interception and access act of 2015 affected the practice of public interest journalism in Australia?

Ms Fair: I think all our newsrooms have reported that the combination of the range of laws that impact on freedom of reporting has had a chilling effect on the way that they go about their activities. Certainly this particular piece of legislation, which enables widespread access of metadata information, is something that journalists have regard to in communicating with sources and has made their job much more difficult.

Mr Dreyfus: To put it in broad terms, has it become harder to practice public interest journalism in Australia since 2015?

Ms Fair: Yes.

Mr Dreyfus: What are the key challenges that are faced by journalists engaging in public interest reporting today and where does the current metadata retention regime fit into that list of challenges?

Ms Fair: There's a range of challenges. We've seen very public demonstrations of some of the challenges. The raids conducted on ABC and News Corp journalists are a very clear demonstration of factors that journalists take into account in pursing their practice. The potential for that activity to take place is something that makes many people pause before pursuing particular stories.

Specifically in relation to the mandatory data retention scheme, it is increasingly the case that metadata and other types of information collected in relation to telecommunications are extremely telling, both about people's personal and professional activities. This regime allows information around journalists to be collected in quite an unfettered manner. Whilst we have some limits in the journalist information warrant scheme, there isn't much transparency and it only relates to a very limited subset of information that might be sought, which is information aimed at uncovering sources. If, for instance, you were interested in trying to put together a trove of information about a particular journalist and stories that they're pursuing, that wouldn't necessarily fall within the limited protections that the legislation currently provides. We say those limited protections need to be reviewed and expanded.

Mr Dreyfus: You noted in your submission that there's very little detailed information that is provided about how the journalist information warrant scheme has operated in practice. For the benefit of those listening, could you elaborate on what you do know, or what is known, about the journalist information warrant scheme? To the best of your knowledge, when have authorities used that? I think you gave a couple of examples in your earlier answer.

Ms Schubert: It's fair to say, I think, that our knowledge of the operation of the journalist information warrant scheme—it has come to our attention only through the reporting of that and through the information that has been brought to the fore. The things that we've outlined in our submission include the breach of the journalist information warrant scheme by the Australian Federal Police, when they announced that, because there are no reporting requirements under the journalist information warrant scheme under the annual report for the Telecommunications (Interception and Access) Act. So any reporting of the occurrence of journalist information warrants being issued only occurs through the review mechanisms, the compliance mechanisms, and that would either be through IGIS, I think, for ASIO, or the Commonwealth Ombudsman for the other law enforcement agencies. I think it's been reported as well that there were public interest advocates actually put into those positions. If I'm correct, that is pretty much the limit of what we understand about the operation of the public interest advocates, and the journalist information warrant scheme more broadly, because there are no reporting requirements.

Mr Dreyfus: I will go to the suggestions that the Right to Know coalition have put to this committee. One of your options is that journalists who are reporting in the public interest should be altogether exempt from the operation of this legislation. I want to see if we could tease out how that could work in practice and what the exemption would actually look like. The reason I ask is that it's not, with respect, completely clear what the Right to Know coalition is suggesting here.

Ms Schubert: Our option 1, to put it in short terms, is for journalists to be exempted from the operation of the scheme, which actually wouldn't say, 'You don't have to get a warrant.' It would say that journalists' metadata
should not be able to be accessed, particularly for the purpose of identifying sources. So journalists' metadata would be out of bounds, off limits, for those purposes, in the capacity that they are undertaking their professional undertakings and outputs. It is limited in that way.

Mr DREYFUS: Would the exception that you have in mind—some suggest that 'exception' is a better term than 'exemption', but, either way—provide that authorities can't authorise the disclosure of telecommunications data of a journalist for the purpose of investigating an unauthorised disclosure offence or a leak?

Ms Schubert: Yes. That would be correct, yes. I think the other point to note is that an exemption or an exception would operate in the same way, so that would be correct.

Mr DREYFUS: Say the committee were minded not to accept the suggestion, or the first option, if you like, of an outright exception. You've suggested in your submission that the journalist information warrant scheme should be improved and you've suggested a few improvements; I want to see if I can tease out some details of that too. You've argued that the Attorney-General should have to approve every application for a journalist information warrant. Why do you see that as an improvement? In other words, why is the Attorney-General an appropriate gatekeeper? I'm not suggesting that she or he is not; I'm just asking you to elaborate.

Ms Schubert: I think it's fair to say that our thinking has evolved since this submission and the other activities and circumstances arose last year, and other government responses to that. This is where we have a bit of an overlapping issue with the two inquiries and the timing of the two inquiries. At the moment it is the case under the journalist information warrant scheme that ASIO and other enforcement agencies have different processes to seek a journalist information warrant. The journalist information warrant for ASIO is issued by the Attorney-General, and the issuing authority for all other journalist information warrants is someone that's nominated by the government. It's lodged in the legislation. It talks about who and how that may be done. It could be a judge at the lower court, it could be a magistrate, it could be a member of the AAT.

When we were devising the submission, we thought it would be appropriate that the issuing authority would be consistent across all of the authorising agencies and that the Attorney-General may well be someone who should actually have knowledge of each and every one of the requests for journalist information warrants and tick them off before they go to an issuing authority for consideration and the public interest advocate for input. I think it is appropriate to say that our thinking has changed on that. Our thinking hasn't changed to the extent that the issuing authority should be consistent, but the role of the Attorney-General should not be across each and every one of those. In fact, it probably should be outside of that, because, if you go to point 2 in our recommendations, we believe that the issuing of the warrants must be a contestable process in front of a judge of a higher order and that both parties, both the government agency and the media organisation, should be heard in a court about whether or not the warrant should be granted, and there should be a public interest test in that.

Ms Fair: Some of the evolution of our thinking takes into account the role of the Attorney-General if there's a contested warrant process. Obviously, it would not necessarily be appropriate that they were also involved at the earlier stage. It could create the potential for conflict of interest. It would be more appropriate to have the Attorney-General as the first law officer involved at that contested stage.

Mr DREYFUS: It might be stated for the record that the involvement of the Attorney-General in ASIO's warrant processes has been there since the inception of those warrant processes, perhaps recognising the distinction between ASIO as an investigative agency and an intelligence agency and not a law enforcement agency. It's always occupied a different role in Australia.

Ms Schubert: That's right.

Mr DREYFUS: You suggested also in the submission that, once the Attorney-General has approved an application—so you've got some possibility; it's just at the first stage—the application should then go to a judge as the issuing authority. I take it by implication that you don't think magistrates or Administrative Appeals Tribunal members should be the issuing authorities? Why do you say that?

Ms Fair: We mean no disrespect to any of those people, who perform a very important function.

Mr DREYFUS: No, and none is taken, I'm sure.

Ms Fair: However, these are very weighty matters, dealing with the public interest and our right to know certain things, and presumably there's a government's view or an agency's view that there's some importance in uncovering certain information, and we think that's something that really should be considered by a senior judicial officer. They're very important considerations. There's also been some history of search warrants and other documents being issued without very much evidence, so I guess our position reflects the need for some greater scrutiny of this type of information being uncovered.
Mr DREYFUS: Warrants generally, not just in relation to journalist information warrants, have come up already in the context of this inquiry and have been referred to in a whole range of submissions. One of the department's objections to warrants generally—we've already got a warrants scheme of a sort for journalists—was simply about volume. Just to give context to this consideration of journalist information warrants, not much is known, but we do know that a very small number indeed of journalist information warrants have been sought since they were created. Is that right—in the order of 10 or so per year, or not even that many?

Ms Schubert: From the Commonwealth Ombudsman's reports we could assume, from that piece of information, that the number is relatively small.

Mr DREYFUS: Yes, in the—

Ms Schubert: In the scheme of things.

Mr DREYFUS: That's right. In the 10 a year type scale rather than the 300,000 a year type scale for information requests under the TIA Act?

Ms Schubert: Correct, yes.

Mr DREYFUS: I mention that only because it's relevant to considering what would be the resources implications of any warrant scheme. You've also argued that the journalist information warrants should be contested. The scheme as it exists now allows for a public interest advocate to be involved in the issuing process for a warrant and that the public interest advocate's role is, at least to an extent, to contest, albeit in secret, the issue of a warrant. What's wrong with that public interest advocate scheme from the point of view of the Right to Know coalition?

Ms Schubert: A significant issue is that the public interest advocate doesn't necessarily have to contest. So they don't actually have to stand in the shoes of the contradicter. There are also some limitations about what the public interest advocate would be given access to in relation to the information being put forward by the requester for the warrant. There being no requirement for the public interest advocate to actually contest the warrant, to argue against the issuing of the warrant, is a significant issue. We have raised that from the very beginning of this process in correspondence with the then Attorney-General because we see that as a significant limitation in the effective and efficient operation of the journalist information warrant scheme as it's currently structured.

Mr DREYFUS: The last point, and I'm happy if you take this on notice, is in relation to this question of whether or not journalist information warrants should be contestable and whether or not there should be notification to journalists or their employers if a warrant is sought. Are there any relevant overseas models that could provide guidance to the committee?

Ms Schubert: We'll take that on notice and come back to you. I think we may have also answered that had in our other submission to the other inquiry. We will come back to this committee on that particular point.

Mr DREYFUS: It will be easy for you to provide us with some further submission on that.

Ms Schubert: Yes, we will.

Mr DREYFUS: Thanks very much.

Senator FAWCETT: I note your submission doesn't go to any of the broader aspects of the metadata regime, such as the length of time to retain data et cetera. We had evidence this morning from one civil society group particularly looking at child exploitation and they were saying two years wasn't long enough in those serious cases. Broadly speaking, other than the access issues and the journalist information warrants and things we have just been talking about, do you have any comment on the length of time that the data is retained under the scheme? Are you broadly comfortable that those founding elements are reasonable if we address the other concerns you have?

Ms Schubert: We've made no comment about the length of retention and those sorts of requirements under the scheme and have focused very specifically on the journalist information warrant scheme. I would note though in reviewing other evidence that's been given to the committee, and I think at last week's hearing in particular, it is concerning that there was potentially a broader range of data that has been provided. I make no comment on who's at fault there at all or anything like that. But reading about the breadth of the information required; or the length of time; or that there is no time limit on the retention of the data at the recipient's end, if I could put it that way, as opposed to the telecommunications companies end, does increase our concern in relation to the journalist information warrant scheme, and potentially just the information that may be held about journalists—the metadata of journalists held by any of the law enforcement or national security and intelligence agencies—for what seems to be an unlimited duration of time. I have nothing other than that to say, other than to say it does raise additional concerns for us in what we've heard of in some of those hearings.
Senator FAWCETT: I'll just note we had contradictory evidence on that last week. Some of the oversight bodies saying it wasn't held long enough and other oversight bodies saying it was held too long. I think the outflow of that was more consistent guidance, which perhaps we'll look at. I note the current regime around journalist information warrants is in the context of them pursuing their professional occupation, but, for clarity and to put it on the record, for the incidents that were raised by previous witnesses where a journalist is suspected of committing a crime of whatever nature—in this case it was child exploitation—you have no objections to their metadata being accessed if they have committed a crime independent of their professional conduct?

Ms Fair: That's correct. A journalist who's a criminal is no different to any other criminal. I think the point you raise is important, because the scope of the requirement to obtain a journalist information warrant for other purposes is very severely limited to where you're trying to identify the source of a story. There may be a range of other reasons why intelligence or other law enforcement agencies may choose to investigate a journalist that may not be in relation to a criminal offence or that may possibly loosely be characterised as something that may be potentially—there are a range of criminal offences, right, so there are under various pieces of legislation issues about not being able to disclose information and certain other things, but for journalists that's part of what they do. They uncover information. When I say a journalist who's a criminal is like any other journalist, of course if someone's involved in child exploitation or something like that there is no difference, but some people argue that some of what journalists do does involve contravention of the law, and journalists argue that in those instances they're pursuing something which is a matter of public interest. So there is a little bit of a conflict in viewing those two areas.

Ms Schubert: Perhaps this is where the inquiries of this committee and the inquiries of the—I know the PICIS has a number of inquiries, but the 'press freedom inquiry' that the PJCIS is undertaking. Is the relevance of our discussions and arguments in that forum about exemptions for journalists from the criminal activities that would apply to them as they are discharging their jobs—of which we've put into that submission from December last year quite a weighty and detailed response too. I think there is a discussion that follows on from Bridget's which probably has a place to play out in the other committee as well.

Senator FAWCETT: Sure. As you know, we've had extensive discussions about the efficacy of public interest disclosure schemes to try and obviate the need for a public servant who has classified information to feel the need to go to a journalist, but that's a different topic.

ACTING CHAIR: Before I go to Senator Keneally, a point that I think is moot here and why Mr Dreyfus is pursuing this is that there has been a delay with respect to the committee's intent to report on the matter of press freedom. It may well be—we don't know at this point in time—that this committee might report on metadata prior to the press freedom inquiry, which is why Mr Dreyfus and probably now Senator Keneally will be asking you questions. As I said, we may be reporting on this before the press freedom inquiry report, and so that's why we're exhaustively asking you questions that you might have addressed in the other inquiry, That having been said, I'll throw to Senator Keneally.

Senator KENEALLY: Thank you to you both for being here today. I would like to probe a bit further the idea of an exception for a journalist to the information warrant. Would an exception create a protected class of citizens—that is, journalists being exempt—given that almost all other professions are subject to the metadata regime?

Ms Schubert: We would say there was some good reason to consider journalists differently to other classes of profession, and that's because of the very important role that the media plays in our democracy in reporting on matters that we all should be able to know about. That's very different to the work that's done by other types of professions, and so there is some good reason to consider journalists and the work that they perform in public interest journalism to be different to most other people.

Senator KENEALLY: To play devils advocate and flesh this out a bit further, I'm thinking that some people might say that there are other professions which are already accorded a form of privilege: lawyers; clergy; people who can receive a protected disclosure, including parliamentarians. I'm wondering if you've turned your mind to whether or not those professions could also make a claim to a form of protection or exemption from metadata retention and investigation?

Ms Schubert: I guess potentially they could make that claim. I think we make the point around option 1 being for an exemption because the operation of the journalist information warrant scheme falls wildly short of its intentions and so, unless it is significantly renovated, we will continue to have those issues. We also talk about an exemption because, as it is currently structured in legislation, although its operation may well fall short—and we're not clear about that, because we don't have any data about it—the legislation says that a journalist
information warrant only has to be applied for if the purpose for doing that is to find and identify a journalist's source. If it's not for that purpose then a warrant is actually not required.

That leaves the gate wide open on potentially the application being perhaps wilfully blind to it being a journalist or wilfully blind to whether or not it's about a source, in which case the journalist information warrant scheme doesn't have to apply; hence an exemption would be the only way of actually providing that protection for journalist sources, particularly under Australian law, in which, as everyone here is very well aware of, there is no constitutional right to freedom of the media and free speech in that regard. When we suggest some of these things, it's necessary in the context because other limitations do not exist that would apply thresholds that need to be considered in the application of these laws.

**Senator KENEALLY:** Thank you. The other issue that has been raised in some submissions and, it is fair to say, in the inquiry on media freedom is the possibility that an exception for journalists could have an unintended consequence of protecting the bad behaviour of rogue individuals—that is, someone could pose as a journalist, operating as a bad actor in plain sight, so to speak, or indeed could cultivate a relationship with a journalist for the purpose of interference or other malicious intent. How do you respond to that concern?

**Ms Schubert:** If I were to reframe that, the concern has been suggested that journalism is a great cover for espionage activities. I think that is what has been put in other forums and other inquiries. We would say that journalism is probably no more or less likely a cover for espionage than a range of other professions. Even in one of the submissions to the PJCIS's inquiry into press freedom—it was the evidence of one of the intelligence agencies or law enforcement agencies that businesspeople could also be a significant foil for people being bad actors and so therefore journalism was only one of a number, including probably the range of people that are walking in the streets in any of the cities or towns in which we live. There is no evidence. I think there's been a story pointed to that someone tried to cultivate someone as a source, and I think that journalist put that to rest in a following article at the end of last year.

**Senator KENEALLY:** If I could perhaps draw this out a bit further, I think the concern that has been raised is that granting an exemption would make it more attractive as well for foreign interference and espionage to be conducted under the cloak of journalism. It's not so much whether or not it is happening on a wide scale now but that you might actually create the conditions that make it conducive or attractive to do that.

**Ms Schubert:** I think our submissions to the other inquiry—it almost feels like we shouldn't share those submissions with this inquiry—and I'm happy to do that if the committee so wishes—

**Senator KENEALLY:** I think we have them.

**Ms Schubert:** I'm sorry—same people but different inquiry. That's why it's a bit funny—not funny, strange.

**ACTING CHAIR:** We find the same.

**Ms Schubert:** I'm pleased. In those submissions, we've gone into much detail and have posited our views about that, which is that an exemption does not put anyone outside the scope of the law. It does actually carefully retain you within the law. So you still have to abide by the same thresholds. It's actually that you won't necessarily have to be put in front of a judge and have to defend yourself. It means you would still have to meet those thresholds, but it begins at the beginning of a process rather than at the end of a process. When we talk about exemptions, exceptions and other things, it's not someone writing a blank cheque and saying, 'You don't have to comply.' It actually means you do have to comply. It just puts it in a different process. So, rather than having to mount a defence, the onus of proof is shifted in those processes. Sorry, I'm not sure if I've answered your question completely.

**Senator KENEALLY:** Thank you. I appreciate your time today.

**ACTING CHAIR:** Thank you very much for your attendance and thank you for your evidence. Just on formalities, if you have been asked to provide any additional information, please forward it to the secretariat by 5 pm on Wednesday the 19th. You will be sent a copy of the transcript for your evidence, and you will have an opportunity to request corrections to transcription errors. Again, thank you for your evidence today.
CHURCHES, Ms Genna, Private capacity

ZALNIERIUTE, Dr Monika, Private capacity

Evidence from Dr Zalnieriute was taken via teleconference—[10:53]

ACTING CHAIR: I welcome representatives from the Allens Hub for Technology, Law and Innovation: Ms Genna Churches, and, via telephone, Dr Monika Zalnieriute. Do you have any comment to make on the capacity in which you appear?

Ms Churches: I am appearing in a private capacity.

Dr Zalnieriute: I am appearing in a private capacity.

ACTING CHAIR: 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. I now invite you to make a brief opening statement before we proceed to discussions and questions.

Ms Churches: We welcome the opportunity to give evidence before the committee today. To clarify, we represent two submissions, Nos 4 and 28. Please refer questions of international comparative law to Dr Zalnieriute, as she is an expert in transatlantic privacy law and data privacy policy, whereas I specialise in Australian communications interception law. The importance of these public hearings and the assessment of the regime by the PJCIS cannot be underestimated. Australian law, juxtaposed with technology, stands at a precipice. If we continue to ignore the importance of metadata and to permit unwarranted access to it, there may be serious ramifications for the rule of law and our broader democracy. Metadata will only increase in production, as will the capacity to store it, creating a greater potential for misuse.

Internationally, jurisdictions such as the US are ensuring the protection of metadata, particularly location data. The Court of Justice of the European Union held that blanket data retention schemes are incompatible with European law. We take this opportunity to mention the very recent Opinion of the Advocate General on the UK, French and Belgian data retention schemes. The advocate general suggests that the UK and French retention schemes are inconsistent with European law, particularly in light of the Tele2 Sverige and Watson judgement. The opinion provides further guidance on the proportionality of data retention and access and should be kept in mind when reading the list of international comparisons in the Home Affairs submission. We suggest that the proportionality, as judged by the CJEU, should be used as an example for Australia, as it would ensure the rights of the individual are carefully balanced against the societal objectives of investigating serious crime and the protection of national security.

We note serious issues with the proportionality of the current data retention and access scheme. These include no prior review of access through a warrant system; blanket metadata retention, including the likely retention and access of content, such as URLs; indefinite retention of data accessed by agencies; no deletion time frame for telcos or agencies; secondary disclosures being broadly permitted and not reported in annual reports; no protections for roles which require professional secrecy, such as lawyers; and access being permitted by a wide range of agencies. Proportionality may be returned to the regime by a combination of reducing the scope of metadata retained, reducing the agencies with access, reducing the retention period, implementing a judicial warrants system or only permitting access for the investigation of serious crime.

As our submissions show, the current metadata retention and access regime is undermined by older provisions, suggesting that amendments to the act may be ineffective. Instead, we suggest that the Telecommunications (Interception and Access) Act and the Telecommunications Act be completely revised. This review should be wide ranging and include the review of similar technologies regulated by the Surveillance Devices Act. Only with complete revision can legislators be sure that the protections they envisaged are not weakened through external legislation or existing instances of broad drafting. In closing, we urge the PJCIS to recognise that metadata can be more pervasive than content and to appropriately adjust the proportionality of the scheme.

ACTING CHAIR: Thank you. Is there an additional comment by Dr Zalnieriute at all or not?

Ms Churches: No, not at this stage.
you elaborate on why location data specifically should be taken away from the subset of metadata that would be required to be held?

**Ms Churches:** Understood. There is a strong argument that location data is, in fact, content. Because of the ability of data points to be received from mobile phones and other internet connected devices, there is an ability to track an individual from location to location. Obviously, I can see the advantages for law enforcement agencies, and I also note that there was an attempt in the dataset enacted in 2015 to limit the scope of those location points. Nevertheless, I would argue that the attempt to reduce them is perhaps becoming less effective—if it was effective at all—as we become more connected to the internet and carry more devices with us.

Location data is highly sensitive data. Think of the scandalous instances where someone might be caught going somewhere they're not supposed to, like a brothel or what have you; those kinds of things can be detrimental to the individual. That's why we say that the location data should not be part of the retained dataset, and that access to it should be at a higher threshold, just as in the US a general warrant is required to access location data there. That's the highest threshold of warrant that they have.

**Senator KENEALLY:** Just quickly—and I apologise for my lack of technical knowledge—but is it actually possible to separate location data?

**Ms Churches:** Definitely; it would be. For instance, mobile phones—that's the easiest one to describe. Under the retained dataset and when we go from cell tower to cell tower, when that communication occurs that will be logged in a cell tower. In ordinary circumstances that data may be of little use to the telco, or they may retain it for other business purposes. But that data is something that they would have to analyse for those business purposes, or of course retain under the dataset.

**Senator KENEALLY:** If I understand you correctly, if the fact is that I make a phone call to Mr Dreyfus then that is metadata which is retained—

**Ms Churches:** Yes.

**Senator KENEALLY:** and could be known under what you seem to be suggesting. But the fact that I am in Adelaide and Mr Dreyfus is in Darwin at that particular time, then that should not be available?

**Ms Churches:** It depends. If we can work out a way for it to be proportional and if the police were investigating a serious crime, then, under a warrant system, I can understand why that would be a proportional response. But at the moment that is not the case, and this is what we're arguing. Right now, it is not proportional because that data, that you were in Adelaide and Darwin, is available even for minor crime.

**ACTING CHAIR:** Including local councils!

**Ms Churches:** Potentially, under section—

**Senator KENEALLY:** But I'm just trying to understand why it's okay to know that I called Mr Dreyfus but not okay to know where Mr Dreyfus and I were when the call took place?

**Ms Churches:** You're right: we could extrapolate this further. But the problem is that we've got to draw a line somewhere as to where that proportionality lies. And it is pervasive: we now know that you and Mr Dreyfus have had telephone conversations, so there's a connection. Where does that lead—

**Senator KENEALLY:** Shock! Horror!

**Mr DREYFUS:** I think we would presume that! It's already not a secret.

**ACTING CHAIR:** On an ongoing basis, it's the time of night that I'm more interested in!

**Ms Churches:** There you go! That's available too.

**Senator KENEALLY:** It's just because I texted you last night to ask what your coffee order was!

**ACTING CHAIR:** Exactly! I didn't want to put it on the Hansard, but now you've raised it!
Senator FAWCETT: You've consistently talked about the threshold for serious crime. Can I just clarify that you would also be comfortable if, for example, the police were involved in a missing person case—so, not a serious crime but a serious incident—with them accessing locatedal data as part of a missing person case?

Ms Churches: Yes. And that would be a proportional response to that particular crime—if it's a crime—or that particular situation at hand. There is scope to mould the law to be proportionate in ways like that—to protect the public and to make sure that missing persons are located as quickly as possible. So the scope is there, it's just not there in its current form.

Senator FAWCETT: That's fine, I just wanted to clarify that you were happy about those exceptions to the serious crime aspect.

Ms Churches: Definitely.

Mr TIM WILSON: Would you deem the best way to achieve that is to define the nature of the crime in the act, and the agencies that can use the said power, or is there a different way that you would seek to do that?

Ms Churches: Obviously I'd love a fresh review so we can look at this in its entirety, but right now there is a regime within the telecommunications interception act, and that is the one for stored communications and the interception of live telephone calls. I can see that we've already got a regime there that sets a threshold that would be able to be used in these circumstances.

Senator FAWCETT: On that point, from a previous report of this committee, the telecommunications interception act is relatively tight. It's the Telecommunications Act and state and territory legislation that actually enables many of the very low-level accesses. It's a related issue that needs to be dealt with. It's not the TIA necessarily that causes some of the problems that you're discussing. I just wanted to put that on the record.

Ms Churches: I would beg to differ. Remember this is federal legislation, so where there is inconsistency the state legislation should fall away. But the issue is that the TIA, in my opinion—no disrespect meant—is not sufficiently tight and its interactions with the Telecommunications Act itself cause conflict. Of course, there is confusion between those two acts, and then we have the Surveillance Devices Act as well which regulates tracking devices, and you could argue that the mobile phone has now become a tracking device, so how do we regain consistency over this area? The only way I can see that happening in its entirety is a full review.

Senator FAWCETT: Sure. My comment was in relation to traffic offences and those sorts of issues, which is a different set of legislation.

Ms Churches: Apologies.

Senator FAWCETT: I want to come back to the opening paragraph in your submission. Essentially you challenge the effectiveness of metadata as a tool and you argue that there is not sufficient reporting or evidence, even as a starting point, to say it's a valid or useful tool. I'd be interested to know what you think would be a sufficient evidence base. Certainly, evidence that we received from previous witnesses today and from law enforcement agencies has given us many case examples and seems to demonstrate that it is a very important tool in being able to identify key players in a crime, particularly in organised crime, and then actually target their resources to gain more evidence that enables people to be held to account through a court. So what would be reasonable evidence in your view?

Ms Churches: You're referring to submission 28—is that correct?

Senator FAWCETT: Yes.

Ms Churches: There has been some research, which my colleagues have cited in that particular part of the report, which has suggested that some use of metadata may not be as effective as we'd like to think. I think that the last hearing also heard evidence from a gentleman specialising in antiterrorism regimes and those kinds of things who suggested that there may also be ineffectiveness in what we're doing currently.

Senator FAWCETT: Could I just clarify: that was about counter-radicalisation as opposed to pursuing an actual terror threat—two different things.

Ms Churches: That is right. We would agree: definitely, telecommunications data is a tool which can be used because of its 'pervasivity'.

Senator FAWCETT: Is that a word?

Ms Churches: It's a difficult—

ACTING CHAIR: Well, it's now going to be in the Hansard. You've created a new word!

Ms Churches: Essentially, what we're saying is that there is research to suggest that it might not be as effective as we think it is and perhaps there should be more research done into that area, but we can definitely see
that, for a period of two years, when someone's metadata is retained from start to finish, it is a very useful tool to see who they interact with, where they've been, who their friends are, whether they connect to the internet, and whether they've even got a mobile phone. There's a whole raft of information, which of course can provide evidence for someone likely to commit a crime or otherwise.

**ACTING CHAIR:** Does your colleague have anything to add? I'm mindful of the fact that she's on the telephone at the moment.

**Ms Churches:** Yes, she's on the telephone at the moment. She is prepared to speak to you about international comparative law if there are any questions.

**Dr Zalnieriute:** I'm here. Unless the question is directed to me I will not intervene, because my colleague Genna Churches is an expert in the area.

**ACTING CHAIR:** I am not criticising or questioning that. I'm just offering you the opportunity.

**Dr Zalnieriute:** I will draw your attention to what Genna mentioned in our opening statement, which is the very recent opinion of the Advocate General of the European Union, delivered on 16 January, concerning the metadata retention schemes in the UK, France and Belgium. The judgement of the Court of Justice of the European Union is now expected within a month, or maximum two. We would advise the committee to keep an eye on that. In essence, the Advocate General at least recommended that you build up on the previous case law of the Court of Justice of the European Union and reiterated three main points about the retention and access and duty to inform the affected party within the regime.

But on your questions to Genna and the discussion you just had, for example you pointed to the investigation of serious crimes and so forth. I think it all points to one tendency. You were talking about targeted data retention and targeted access to particular individuals, particular cases about missing individuals and so on. Genna Churches and I are arguing against the blanket and indiscriminate retention of the data and access to the data, which is not independently authorised as it currently stands; it is internally authorised within the agency. So we would like to emphasise the recent Advocate General's opinion that the access needs to be accessed independently by the judiciary or administrative authority which is independent of the agency accessing the data. I leave the rest of the discussion between you and Genna. Thank you for this opportunity.

**Mr DREYFUS:** In the Allens Hub submission, on pages 6 and 7 there is an interesting passage about cost as a means of assessing data retention schemes. The submission makes the point that a cost-benefit calculation made in the United States in 2018 resulted in a similar retention team to the one we have in Australia being terminated. It notes that the European Court of Justice, in the data retention directive case, referred to costs. Later in the submission you refer to a piece written by Richard Chirgwin, 'Australia's metadata retention scheme costs telcos $500k per cuffing'. That article simply made the point about the 334,000 requests in 2015-16, almost all of which were related to criminal investigations, the 334,000 requests and the $200 million cost yielded 366 arrests and 195 convictions, a unit cost of more than $500,000 per arrest and $1 million per conviction. They are pretty startling statistics. Do you agree with them?

**Ms Churches:** I have to say that I didn't write that part of the submission. I haven't checked that myself, but I can take that on notice to confirm those figures.

**Mr DREYFUS:** We'd like you to do that. By way of follow-up, why is cost an appropriate matter to take into account in considering the social efficacy of the scheme like this?

**Ms Churches:** Understood. I can actually tie this back to the Home Affairs submissions, where they're discussing that implementing a warrant process would be an undue burden, it would blow out costs, those kinds of things. When we look at any of these regimes, cost is in the back of our mind. When we look at data retention, does the cost of implementing result in something tangible at the end? What is that cost? Is there some overall societal benefit? Have we achieved those objectives? I think that cost always plays a part in anything that we do.

**Dr MIKE KELLY:** Perhaps this is directed more at Dr Zalnieriute in relation to the international experience. Perhaps she might want to speculate on what directions the European decision may go, particularly looking at the sorts of regimes that have been in place overseas. What observations or summaries could she make about the experience of the practical application of the frameworks that have been in existence, and what steps are agencies similar to ours taking to seek reforms or looking at our experience here? In terms of the practical enforcement experience that they have had, has she got any observations to make in respect of that and where there may be attempts being made to address any deficiencies in other European or overseas examples of this type of legislation?

**Dr Zalnieriute:** Thank you for this question. We have two points. One is the practical issues that the agencies are facing in trying to enforce or keep data retention regimes in place. Another one is the potential direction of the
upcoming judgement of the Court of Justice of the European Union. In terms of the practical issues, I have to say that in Europe the situation has been very tricky since the original 2014 judgement, called Digital Rights Ireland, when the European data retention directive was invalidated, leaving the member state countries confused about how to proceed with their national systems. The Tele2 Sverige judgement then also applied the same standards of EU law to the national regimes. It turns out that in many countries the regimes are in place and the other ones are invalidating and trying to comply with the court of justice judgement.

The situation is definitely very complicated and the activists, especially after the Snowden revelations, are taking every opportunity to take legal challenges against the national data retention regimes. I would say that law enforcements agencies are encountering big challenges, and they are only increasing again, also again after the Cambridge Analytica scandal and so on. So each big event in the mainstream psyche would contribute to more legal challenges against the national data retention schemes. It puts a lot of pressure on the law enforcement agencies.

In terms of the practical issues, I wouldn't know about them, because my expertise is more on constitutional and privacy law rather than the practical issues of the law enforcement agencies trying to deal with that. But the pressure on the agencies are very big.

Coming to the second point, the potential direction of the judgement, I'm pretty certain that the Court of Justice of the European Union will follow a non-binding opinion by the Advocate General, because that's been the tendency since the Snowden revelations and the first big judgement in Digital Rights Ireland; also because this opinion and the case in question really concerns the same issue and it is pretty much same legal matters, except that it would prove yet again that the national frameworks that were still left in place after these big judgements delivered between the period of 2014 and 2016, or 2018 will no longer be able to remain as they were in the past. So the expected judgement, in my opinion, will confirm what the Advocate General has said, that the parent regimes are compliant with the three basic principles: that the retention must be targeted, access needs to be authorised and there must be duty to inform the affected parties. So I think that the pressure on the national regimes on the blanket, indiscriminate retention, as well as the access, will keep growing with the political and current legal and political climate in the EU and beyond.

**ACTING CHAIR:** Thank you for your evidence and for your attendance here today and by phone. If you've been asked to provide any additional information, please forward it to the secretariat by 5 pm on Wednesday 19 February 2020. You'll be sent a copy of a transcript of your evidence and will have an opportunity to request corrections of transcription errors.
GILLESPIE-JONES, Ms Christiane, Director, Program Management, Communications Alliance

STANTON, Mr John, Chief Executive Officer, Communications Alliance

**ACTING CHAIR:** Welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I'd like to throw it open to you to make an opening statement before we proceed to questions and/or discussion.

**Mr Stanton:** Thank you to the committee for the opportunity to appear before you today. The telecommunications industry does share the government's desire to protect national security, to fight terrorism and crime, to enforce law and, specifically, to enable relevant agencies to do their jobs effectively in a digital environment. Our members, the carriage service providers and carriers of Australia, do cooperate with law enforcement agencies. The most recent annual report on the Telecommunications (Interception and Access) Act highlighted that carriage service providers receive on average more than 1,100 requests for metadata per business day during the course of the year. So, while the data retention legislation is certainly effective from a throughput perspective, there are nonetheless a number of problematic elements that we think need to be addressed. There is also one expansionary risk that we think ought to be explicitly avoided.

The concerns that we've outlined in our submission include what we would see as the unintended consequence of section 280 of the Telecommunications Act being used by a broad range of agencies to access data without a warrant. This is outside the 22 criminal law enforcement agencies as per the TIA Act. We've provided a non-exhaustive list of some of those agencies, mainly state based, that are getting access to data. The fact that they are doing so through the telco act and don't need to comply with the relevant sections of the TIA Act is problematic. It leads to a lack of reporting around those requests and to fewer considerations around privacy. It leads to disputes over compensation for the work that's undertaken by the telcos. It also presents complexities for the service providers when they receive requests from these agencies, because they feel an obligation to try to figure out whether the agency that's making the request is actually entitled to make that request and, indeed, what sorts of data the service provider is entitled to release to them.

We have some longstanding questions as to whether it's appropriate for metadata to be released for use in civil proceedings and about the lack of protections that are associated with those disclosures. We've always had a question around the two-year duration of the retention period, in the light of international experience but also, as we see in the annual reports of the TIA Act, due to the fact that the vast majority of the data being stored is three months old or younger and more than 90 per cent is 12 months old or younger.

We also have a concern around the scope of the services to which the legislation may apply, and this is around whether it can be construed to capture machine-to-machine communication. IoT networks are burgeoning across Australia and the world at the moment. We believe it could be interpreted that machine-to-machine communication is covered by the act, and, were that to be the case, we're talking about the addition of literally many, many billions of additional data points during the course of each year that would need to be retained. These are things like the salinity level of water in oyster leases, the moisture content in orchards and wheat fields, and the condition of pipes in sewerage networks. We would argue that this data is not relevant to agencies—unless they're perhaps contemplating writing a novel about the secret life of parking meters!—but it would add very substantially to the cost of this scheme to industry, which is significant. Net of the grants and net of the compensation to carriage service providers by agencies, the scheme still does cost around $37 million a year to industry.

We're a little disappointed in agencies failing to meet their reporting requirements and the length of time it takes for those reports to make their way to parliament. I'll pause there, if I may. Christiane and I would be very happy to try to answer any questions that the committee may have for us.

**ACTING CHAIR:** I am extremely interested to have a conversation with you about a couple of matters. You just said that the $37 million cost is borne by the telecommunications industry. Can you elaborate on that?

**Mr Stanton:** Yes. The figure, which was out of the annual report, comes from a figure of $229 million a year over a five-year period. That's excluding the initial grants. The cost recovery over that time from agencies was $46 million—that is, about 20 per cent of the cost. So, when you do that subtraction and divide it by five, you get a figure of around $37 million a year in net cost to industry.

**ACTING CHAIR:** So their out-of-pocket costs are being absorbed by the telecommunications companies. Is that what you're saying?
Mr Stanton: Correct.

Senator FAWCETT: I want to ask a quick follow-up on that. You gave a figure before about the very large number of requests that were received each day. Of that $37 million, how many of those come as a result of requests under the metadata regime that this committee supported and recommended in 2015 and how many of them come through the plethora of agencies that access data through section 280 of the Telecommunications Act? What percentage of that cost would be deferred if we were to close that?

Mr Stanton: We don't have precise numbers around that, because they're not reported, so they don't form part of official reporting, and, typically, the service providers deal with them but don't necessarily log them all individually.

Senator FAWCETT: Is that something you can get an indication of?

ACTING CHAIR: Could you take it on notice? Is that possible?

Mr Stanton: I've tried before and failed, but I will try again to see if we can get some better metrics around that, but it is tricky.

ACTING CHAIR: One of the key points that I'm interested in is what I call mission creep. We've seen mission creep in terms of what we found when this committee first looked at who could access this data and the circumstances in which they could access it and, then, what we now find is occurring, which vexes all of the committee members, I think.

The second issue is then, of course, what is being accessed. Right from the inception of this from 2011-12, we were very specific about, given the intrusive nature of the powers, exactly what it was that could be accessed. In your submission you're talking about, again, the potential broadening of what could be categorised as metadata and then what the agencies might seek to obtain. I also note that in the Home Affairs submission they talk about not being overly prescriptive in terms of what metadata could be retained. Have you had any discussions with the Department of Home Affairs, agencies or anyone else that would lead you to believe that they might be seeking to extend what is currently being collected as metadata?

Mr Stanton: Personally, no, I haven't had that discussion with Home Affairs.

ACTING CHAIR: Are you aware of any.

Ms Gillespie-Jones: I'm not aware of any specific data points that Home Affairs would like to seek access to that they're not currently already seeking access to. I must say that some time back I looked at the submissions, and there was talk that potentially IoT data or data that is derived from things might be of interest. I would need to look up exactly where I read that.

ACTING CHAIR: Could you take that on notice? I speak on behalf of the committee and think that would be one thing that would concern the committee a great deal. We're observing a set of very clear guidelines that were established by the committee that appear not to have been actuated in a functioning law which has then been utilised to others to access beyond the scope of the scheme and certainly what we were told would occur with the scheme.

Ms Gillespie-Jones: The question's not only whether agencies have sought or will seek to have access to such data. The problem, of course, for carriers would be the legal certainty as to whether or not they need to retain that data. As long as the legislation does not create that legal certainty, that already in itself constitutes a massive problem for our industry.

ACTING CHAIR: Would you say, on that note, that the telecommunications companies, service providers etc are keeping more data than they normally would in expectation that this might be a request that might come by some form of government agency or government in the future?

Mr Stanton: No, I don't believe so.

Ms Gillespie-Jones: I don't believe so.

Mr Stanton: They have a clear understanding of the requirements and the categories of information that are named in the act. To my knowledge, they operate to that list. One of the difficulties they say that they often encounter when agencies outside the 22 CLEAs make data requests is that those requests can be imprecise. Sometimes these agencies don't know exactly what they're looking for or what they're trying to find. Often they also have difficulty interpreting the data that they receive, come back to the service provider and try to work their way through it.
**ACTING CHAIR:** From our perspective, we would expect, we're told and we've got forms that say that, when a metadata request is lodged, they're actually quite specific. Are you saying that that's not the case in some circumstances?

**Mr Stanton:** I think that in the case of the CLEAs it's a pretty-well-organised system with good knowledge on both sides. What we hear from service providers is that the interaction with those many entities outside is not as neat a process.

**ACTING CHAIR:** So in a sense they could be providing content inadvertently to organisations like councils et cetera because of the unspecific nature of the request?

**Mr Stanton:** I can't make that extrapolation. They're aware that it is not about providing content. At the same time, as I think other submissions or testimony have said, sometimes a URL may be disclosed. Sometimes that will provide no guidance as to contents; potentially sometimes it could. As the testimonies made the point, it's incumbent on every agency to ensure that the data that it receives is authorised to be provided to them.

**ACTING CHAIR:** In essence, I'm hearing you say we don't really know whether or not inadvertently—because you might have a local government, Fines Victoria or something that's after information and that could inadvertently get someone's URLs as a consequence of the lack of specificity in what they're asking for in terms of metadata?

**Mr Stanton:** It's clearly possible that that could occur. I can't give you—

**ACTING CHAIR:** I'm not seeking to lead you. We as a committee are trying to understand what's happening out there. To be clear about this: we were told that there would be a certain number of defined organisations that would have that data. We gave those organisations the power that basis and now we learn that that's not the case. Even worse, in terms of your testimony here today, what I'm hearing is that you could have an organisation that I clearly think should not have those powers then having the potential to get content of someone's communications, which disturbs me a very great deal. We're seeking to understand the scope of the problem given what we expect and what we're now learning, so we can take remedial action, if the committee so determines, to give public confidence in the sense of who's accessing that information and what they might be doing with it.

**Mr Stanton:** We would agree that there are options to try and put better controls around that. Those other agencies could be required to go through a CLEA like the AFP, which is an option for them, and make their request that way, which brings it within the system. There could be a requirement that they comply with all those elements of the TIA Act which are specifically designed to give greater surety around this process.

**ACTING CHAIR:** To come back to the point, previous iterations of this committee and this committee provided access to the power for defined agencies. We did not envisage that anyone else would access that. I think this is the point that's causing great concern, along with the scope, the nature of what's been aggregated by this and the sheer number of requests. I think committee members on both sides are perturbed about this, to provide you with some form of reassurance. It's good to hear from you about the extent of this, because, as I said, from my perspective I'm quite horrified by what I'm now hearing about who has access to this data. It's not the intention of the scheme. Having finished that, I will throw to Mr Wilson and then Senator Keneally.

**Mr TIM WILSON:** I was essentially going to raise the same issues. What I'm really after is how you think this, shall we say, loophole can be closed. We have a current situation where the act is supposed to stipulate that certain information should only be available and accessible in certain circumstances for certain agencies for certain purposes, and now other acts are being used to circumvent that. Do you have a suggestion about how that loophole can be closed?

**Mr Stanton:** We could amend the Telecommunications Act to make it clear that, if requests for metadata are being made under section 280, they should be directed through an existing CLEA and/or the requesting agency ought to be subject to the relevant sections of the TIA Act which govern the way that those metadata requests are handled.

**Mr TIM WILSON:** For clarity, you're confident that, if we went down that path, it would address the fundamental issue that you've raised in your submission?

**Ms Gillespie-Jones:** Parts of it.

**Mr TIM WILSON:** That is not the whole of the substance but on this particular issue around circumventing the law?

**Ms Gillespie-Jones:** It would arrest the number of agencies and which agencies make requests. We still face the issues around the categories of data and whether data is being sought in civil proceedings, for example, and whereby then the protections that the Telecommunications Act would offer providers who make that data
available would no longer told. Under the Telecommunications Act, section 313(3), under which providers currently make that data available if it's being sought under 280, only applies to criminal legislation and to laws with a pecuniary penalty. It doesn't apply to civil proceedings. Providers currently are not protected. There are no liability protections for the providers when they make such data available for civil proceedings and there is also no cost reimbursement for that purpose.

**Mr TIM WILSON:** What would you see as the best way to address that issue as well?

**Ms Gillespie-Jones:** That would be more substantial change, I would assume, because it is currently, I think, section 280 that allows the disclosure of information if it is not purely maintained for the purpose of the data retention regime. That is the thing that creates the complexity. In essence, that means any data that has been retained prior to the regime can be made available and any data that has been retained for the purpose of the regime but not solely for the purpose of the regime can be made available, but only for the period of time that it hasn't been retained solely for the purpose of the regime.

**Mr TIM WILSON:** This is why it's good that it's all transcribed in *Hansard*!

**Ms Gillespie-Jones:** Exactly! You can imagine the difficulty for a provider to assess whether or not that data can be made available.

**Mr TIM WILSON:** Whether that data can be made available?

**Ms Gillespie-Jones:** Yes, because they take the data, retain the data and ingest it in a certain system. Sometimes that may be separate systems for data retention or it might be one big system. They first need to take their own processes apart and see whether that data has been retained only for data retention purposes or whether it has also been retained for any other purpose, and for which period it has been retained for that other purpose.

**Mr TIM WILSON:** Thank you.

**Senator KENEALLY:** I have a few questions. You may wish to take some of them on notice, because I seek your opinion on some issues that are raised in a supplementary submission we have just received from the Department of Home Affairs; it will be published shortly. Can I turn, first, to your submission, where you note the exorbitant costs that would result for CSPs if 'Internet of Things' was included in the definition of relevant services and communications under the TIA Act. The submission we've received from the Department of Home Affairs makes the point:

… machine-to-machine communications are increasingly taking place on applications that run 'over-the-top' of a carrier or carriage service …

They say:

'Over-the-top' providers are not captured by the data retention obligations meaning that an increasing volume of data may not be retained. It would therefore be premature to state that 5G—

and these machine-to-machine communications—

will necessarily increase the amount of data captured …

I don't know if you have a response to that statement from Home Affairs here or if you'd like to take that away, but I would be interested in your response to that observation they're making.

**Mr Stanton:** Thank you. We may do both. We will certainly take it away and come back to the committee. I guess I would make the point that there are many different types of machine-to-machine applications and, for many categories—a traffic meter reporting back to base, a farmer keeping an eye on a connected cow as it wanders around the field, all of these agricultural applications and so forth—I think it is very hard to construe that they would ever be useful to an enforcement agency. Similarly, it's hard to predict all the applications for which M-to-M can or will be used in the future. I take the point that there could be systems that would generate data that would potentially be of interest for agencies. The question that confronts us all now, I guess, is: how do you separate everything which can never be useful while leaving open the possibility of being able to request data on M-to-M systems that are of interest? We will talk to members and try and give you a more cogent response than that.

**Senator KENEALLY:** Thank you.

**Ms Gillespie-Jones:** Just so I understand you correctly: I understood from what you just said and from the submission that the department wanted to say that in fact the amount of data that would need to be retained, even if machine-to-machine communications were included, wouldn't be that high because a lot of it would go over the top and would not be captured. Is that what you wanted to—

**Senator KENEALLY:** That seems to be the implication of their submission to us, yes.
Mr Stanton: We disagree with that.

Ms Gillespie-Jones: We would disagree with that. Surely there is IT data that will go over the top, but surely there's also a huge amount that will not. Just because not the entire amount of IoT or machine-to-machine data will be dealt with over mobile networks—or fixed networks, for that matter—it doesn't mean that the amounts will not be exorbitant.

Senator KENEALLY: Just so I am clear: it appears that there is a lack of clarity as to whether or not this data will be retained under the metadata legislation.

Mr Stanton: Yes, because 'communications' is not defined in the TIA Act. 'Communication services' is defined under the data retention legislation. If you look at the telco act and its definition of communications it explicitly includes 'machine-to-machine'. So there is some greyness there, but I think it's possible that it can be interpreted to include those types of data.

Senator KENEALLY: So from your members' perspective, there is an open question as to what they are to retain as the introduction of machine-to-machine and Internet of Things expands in our society?

Mr Stanton: Yes. They've not been asked to, but they fear that that can happen and blow out the costs very significantly, potentially for no benefit.

Senator KENEALLY: In another matter that arises from your submission: you made the point that 94 per cent of the requests that you received for metadata were for data that was retained within 12 months or fewer before the request. This goes to the issue we've heard a fair bit about in terms of the length of time the data should be retained. The Department of Home Affairs' submission and the previous report of this committee in 2015 made the observation that perhaps it is not surprising that most metadata requests were for information that was stored fewer than 12 months. However, the observation was also made that even though those that were longer than 12 months might be small in number, they tended to relate to the most serious categories of crime—antiterrorism, online sexual abuse et cetera. Do you want to comment on that observation here now, as to whether or not that changes your view regarding the period of time in which the data should be retained, or go back and have a look at the submission that's about to be published from Home Affairs?

Mr Stanton: In terms of the categories or the crimes pertaining to the request for older data, Home Affairs is in a better position than us to comment on that. What I would say is that investments have been made in storage capacity by service providers in order to be able to comply with the two-year period, but we have seen suggestions that that two-year period ought to be extended further. We wouldn't support that. Secondly, it relates back to the previous issue: if you suddenly introduce enormous new categories and numbers of data points that have to be retained then perhaps the investment already made by providers is no longer adequate and they've got to go into a fresh round of filling up data centres.

Senator KENEALLY: My last question relates to an issue we heard about in a previous submission. A number of submissions have expressed the increased sensitivity of location information, and have suggested that access to location information should require a warrant or be excluded from the mandatory retained dataset altogether. I wanted to ask you if, in terms of the technical requirements, that were a change that was introduced to the system, what would that mean from the CSP's point of view in terms of the ease with which you could separate out that data, the changes you might need to make in storage or the changes you might need to make in responding to requests from the CSP's members? The previous issue then if you suddenly introduce enormous new categories and numbers of data points that have to be retained then perhaps the investment already made by providers is no longer adequate and they've got to go into a fresh round of filling up data centres.

Mr Stanton: There are already location requirements within the datasets that can be sought. I guess the argument here is: to what level? If the request is for AML data that's not retained today, then that would require changes to systems and additional costs. But, again, if I may take that one on notice and get some better advice from the mobile operators, we would be happy to provide a response.

Senator KENEALLY: That would be helpful. Thank you.

Ms Gillespie-Jones: Just to be clear: are you also asking about the costs to systems not to make this data available?

Senator KENEALLY: That's right. The suggestion has been made that we should remove location data, or that location data only be provided—

Ms Gillespie-Jones: Under warrant.

Senator KENEALLY: If a warrant has been issued. So I'm trying to understand the impact that would have on CSPs, both in practicality and in cost, and what the changes you might need to make would be if such a change were introduced into the law.
Ms Gillespie-Jones: Let us take that on notice. We would assume, though, that the data would still be allowed to be retained, because it would need to be allowed to be retained. So, just about the disclosure part of the information—

Senator KENEALLY: Yes, that is correct.

Ms Gillespie-Jones: It goes back a bit to the question that we had before: could it be the case that content is being made available—and you specifically referred to URL information. I will come to the question of the way that they relate to each other. URL information is not clearly content information, but it might go in that direction. It is sometimes, but not always by far, being provided by providers because of the difficulty of separating out specific data points. I suspect that the same might be the case with location data, and that it is difficult to say, ‘You can have that big dataset but you cannot have the specific location data that's contained in the dataset.’ I would suspect that there is some cost in removing such data. The additional complication, potentially, to provide it only under warrant might add to the picture.

Senator KENEALLY: That's exactly the point I'm trying to get at. I gave another example earlier: if I called Mr Dreyfus, and the request were made for the details of that call, then if such a change were made you might report that a call was made between two people but not that I was in Adelaide and he was in Darwin. What does that mean from a CSP point of view? Is it technically possible to sort that data out to remove the location information? What would it cost you? How would you need to change your storage? Would you need to change your storage? Would it make it more complicated?

Mr Stanton: The fact that landline numbers are still geographically based in their configuration means that just providing the number—

Senator KENEALLY: Itself.

Mr Stanton: Shows that you're in Adelaide. The number called is one of the requirements.

Senator FAWCETT: You've mentioned in the submission and in your oral evidence both the complexity of the legislation and the uncertainty around civil cases. Coming back to the metadata retention regime as this committee approved it in 2015, civil cases were never envisaged under the parameters we had placed around that. Can you confirm for us that providers are providing metadata for civil cases and questioning whether it's right for them to do it, or is it just a concern that you're raising that they may be asked?

Ms Gillespie-Jones: My understanding is that they're providing that data—under subpoena, for example. The problem that has been raised with us—and I can't tell you whether it is a very common problem, but it certainly does occur—which does come with such provision under subpoena, is that a court that typically subpoenas information does not necessarily have regard to proportionality and the effects on the privacy of the individual. It might also subpoena information of an individual who is not part of the proceedings. The provider might therefore disclose that information, and another individual might not even know about it—the individual whose information is being disclosed.

Mr Stanton: And section 280 is quite broad, because it simply requires the CSPs to respond to requests where disclosure or use is required or authorised by or under law. So it doesn't do a great job of differentiating between different types of legal issues.

Senator FAWCETT: My second question goes to your evidence that around 94 per cent of all requests are less than 12 months old. We had evidence from anticorruption bodies at the last hearing, particularly from New South Wales, that 47 per cent of their authorised access to metadata was at the two-year point or beyond in terms of their pursuit. They said that quite often corruption takes time to uncover. Again, if we wrapped around the appropriate accesses, as we envisaged in our 2015 report, are you happy to accept the fact that there is a legitimate case for retaining at least that two years worth of data?

Mr Stanton: We said in our submission that our preference would be for it to be a shorter period, but we recognise the investments that have been made in storage capacity. What we're more concerned about is that it not be expanded in terms of duration or in terms of the types of data that have to be retained.

Dr MIKE KELLY: A quick technical chase-up, with the fundamentals behind this, in relation to the liability it imposes in data storage: you're talking about the new expansionary regime that could apply because of the definitional problem. What are we actually talking about in terms of the volume? What are your arrangements now in relation to data centres? Are you being required to add significantly to your data centre capability?

Mr Stanton: Different carriers responded in different ways when the legislation came in. Some of the larger ones had to make major investments in internal systems because they had, in one case, more than a dozen different databases within the company that needed to be integrated so a single request could be pulled from
those. That varied depending on the number of systems. Often the players had more than one billing system because they had acquired other entities. There were those sets of internal system and process investments. The simpler piece is buying more rack space in more data centres to be able to hold the data.

Dr MIKE KELLY: So that is happening—buying more data space. How is that happening? Are the telcos using in-house solutions to that, or are they leasing or outsourcing that data space?

Mr Stanton: The majority tend to outsource to data centres. That is standard practice across the industry. Some databases will be held internally for whatever reasons, maybe commercial, may be sensitivity; but there's a thriving data centre industry in Australia, and by and large you go and buy more rack space and put more servers in.

Dr MIKE KELLY: So the majority of what is going on, in terms of getting that extra space, is the outsourcing?

Mr Stanton: That's right. That is what happens now. The initial investments in internal changes were largely made a number of years ago.

Dr MIKE KELLY: In one sense, that can potentially open up greater vulnerabilities from a security point of view. We had the experience of Global Switch taking a majority controlling interest in data centre space, so that, for example, Defence was leasing in centres that stored highly sensitive information, both Australian and allied information. In terms of the ownership of those data centres and the regimes in which they're managed, there could be quite an array of international and other global companies involved in running those data centres.

Mr Stanton: All the service providers have obligations under the TSSR legislation to protect the integrity of their systems and their data storage. Yes, that's a risk for any system anywhere around the world, but I think it's pretty well managed in Australia.

Dr MIKE KELLY: We've had recent experience with China and, prosecutions in the United States, where they're basically hoovering up billions of data points on US citizens across a range of debt, medical and other spectrums in order to utilise that in targeting individuals and creating pressure points et cetera. They have a much greater global concept of their use of data and personal data now. We're seeing the Russians, of course, doing that and using it in different ways. Creating more and more data storage is going to be a real issue in terms of ensuring that data sources are not vulnerable and protecting them and ensuring that the data centres we're leasing out to are secure as well. There is going to be a big liability associated with that as well, isn't there?

Mr Stanton: There's always been the fear that you create a honey pot of data that becomes very attractive to bad actors. Cyberrisks are real. They exist here and elsewhere.

Dr MIKE KELLY: On the cost of doing this so far, can you put a dollar figure on where we might end up if the definitions are tightened up in relation to machine-to-machine and IOT data retention?

Mr Stanton: No, I can't give you an estimate of that today. It would be very hard to predict because the use of IOT networks is literally exploding as we speak. It's the next massive disruptor. The rate at which it will grow over the next five years is very hard to predict, but on current trajectories it's huge.

Dr MIKE KELLY: I think you were given $131 million initially to assist with this. How has that panned out in the scheme of meeting the costs of this?

Mr Stanton: There were statistics that the government put out at the time. I need to check this, but from memory I think that they said that 80 per cent of those who applied for grants received 80 per cent on average of what they'd asked for. The majority of players who looked for capital support at that time got most of what they asked for. I know that in the case of some of the larger ones it was more like 50 per cent of their internal costs of capital changes at that time.

Dr MIKE KELLY: So that $131 million was meant to be for the initial three years, and there was nothing more coming behind it?

Mr Stanton: That's right. It wasn't an operational grant. It was for capital investment to be able to comply.

Dr MIKE KELLY: That will pale then, in relation to some of the further burdens that might be coming downstream. I guess you would look to pass that on to consumers.

Mr Stanton: For the service providers it's a cost of doing business at the moment. It's $37 million or thereabouts spread across the industry. Compliance with all manner of regulation and legislation for these companies is a very significant cost of doing business. It's one of the more heavily regulated sectors in Australia.

Dr MIKE KELLY: Do you utilise any attempt at tax minimisation associated with those extra costs? Do you attempt to claim those in tax minimisation, or is that not a valid source of tax deduction?
Mr Stanton: I'm not running a service provider these days, so I can't comment on the financial practices or accounting procedures within individual members.

Mr DREYFUS: Thanks for attending here today and assisting the committee. Mr Wilson's questions touched on this to some extent already. Many of us thought after 2015 that only the 22 agencies listed in section 110A of the Telecommunications (Interception and Access) Act would be able to access retained telecommunications data. Your submission very helpfully gives us a list of 87 agencies that are using means outside the provisions of the data retention legislation. To mention a few: Brisbane City Council; Fairfield City Council in New South Wales; Primary Industries Queensland; the Victorian Institute of Teaching; the Veterinary Surgeons Board of Western Australia; Victorian Fisheries. That's not the whole list, obviously. Do you have any idea or does anyone have any idea why the bodies I've just read out—Brisbane City Council, Fairfield City Council, Victorian Fisheries—need access to a person's telecommunications data?

Mr Stanton: I don't have an exhaustive list of the nature of those requests. We know that some, for example, were looking for information about the location of mobile numbers and whether they were associated with a spot where illegal dumping had taken place. Some of those requests were about trying to track down those who had committed infringements at the local council level. Why the vets and the fisheries and everyone else were looking for the data? I don't have, nor should I have, information about the content of each request.

Mr DREYFUS: On any view, the purpose of those requests is very far from what ordinary Australians would think of as the investigation of serious crime.

Mr Stanton: That's a view we hold, yes.

Mr DREYFUS: I think we can agree that Fairfield City Council or those others are in no sense criminal law enforcement agencies.

Mr Stanton: Yes.

Mr DREYFUS: Would they have had to go through a rigorous approval process to get access to a person's telecommunications data?

Mr Stanton: In each case they would have made the request and presented the service provider with a dilemma: does this council have right-to-produce powers? Am I authorised under this legislation?

Mr DREYFUS: Pausing to get this right, I'm not trying to take you through the full operation of section 280 of the Telecommunications Act. The question is basically, is this agency or body authorised under a state law?

Mr Stanton: That's right. I would imagine that in some cases that would have been furnished up front by the entity making the request. If it wasn't, then the telco is left with the question of how deep they have to dig to try to verify that this is an authorised request. They don't see that as their role. When you look at the volume of the requests coming in, to have to try to go down the investigative track every time is really difficult.

Mr DREYFUS: To take an example—again, I have no personal knowledge of this and you probably don't either—but one of the more unusual bodies in your list is the Victorian Institute of Teaching. I'm guessing, but I don't imagine that the Victorian Institute of Teaching has made thousands of requests for telecommunications data. It may have; but let's say it didn't and it's a fairly unusual event for the Victorian Institute of Teaching to seek telecommunications data. It might be an example of an agency that is required by the telecommunications provider to provide proof that it has in fact got some authorisation under Victorian law that authorises it to compulsorily seek information.

Mr Stanton: Indeed, that may be the case. One of the things it points to is that, if that institute had needed to go through an authorised CLEA to make its request, its right to make such a request could be vetted at that point, rather than leaving it in the hands of the telco to try to decide that.

Ms Gillespie-Jones: It would also mean that there could be greater scrutiny or consideration given, as it currently is the case under the TIA Act, as to whether the request actually pertains to an offence that was envisaged under the act and the effect on privacy of the individual. It would get reported. Mr Wilson asked the question about what is the percentage of those that come through the telco act as opposed to the TIA Act? We don't know, because there is no reporting around it.

Mr DREYFUS: Can you make any estimate of how many times these agencies and organisations that are not listed in section 110 of the Telecommunications (Interception and Access) Act have requested telecommunications data? Or is the answer again 'We don't know'?

Mr Stanton: The answer is we don't know.

Ms Gillespie-Jones: We don't know.
**Mr Stanton:** To try to get the telcos to estimate it is difficult as well. They're not required to keep records of this and they don't necessarily have good data around exactly how many times. You will see two lists that we provided in our submission. The second one was created not that long after the first one, and in that brief space of time an additional 27 entities had popped up. I thought that growth was quite interesting. It was a non-exhaustive list because we weren't able to get data from all of the players in the industry. It came basically from just a few.

**Mr DREYFUS:** It's catching on, you might say?

**Mr Stanton:** Yes.

**Mr DREYFUS:** Just to be clear—because the committee may yet need to examine itself the list of agencies that are using sections 280 and 313 of the Telecommunications Act—can you describe what process you use to create these two lists?

**Mr Stanton:** We have a great number of different working committees and standing groups within Communications Alliance, composed of representatives from our members. There is a group that deals with national security and with these issues. They are operational people dealing with agencies on a daily basis or managing teams that are. We went to those individuals and said, 'What can you say to us about the nature of the agencies? What sort of examples can you give us?' Some were able to pull records from the requests they'd received and dealt with. So it was from the operational parts of the CSPs.

**Mr DREYFUS:** So this is a non-exhaustive list provided by a non-exhaustive list of providers—

**Mr Stanton:** Correct.

**Mr DREYFUS:** of agencies and organisations across Australia that are using sections of the Telecommunications Act to access mandatorily retained data?

**Mr Stanton:** Yes. We don't know the size of the iceberg.

**Mr DREYFUS:** To move to a slightly different topic, do providers ever decline requests for telecommunications data? If they do, how often does that occur?

**Mr Stanton:** I can't answer the second part of that question. We've made the point that these are the agencies that have requested metadata. They haven't necessarily all been furnished with it. Perhaps that's because they were unable to substantiate the basis for their right to seek the data or perhaps the data didn't exist or wasn't required to be retained. Again, I don't have definitive numbers around how often that's occurred.

**Mr DREYFUS:** Let's confine this for a moment to the requests under the Telecommunications (Interception and Access) Act by the agencies that are listed under section 110A. Are there occasions in which providers may refuse requests even from those 22 agencies?

**Mr Stanton:** I can't rule it out, but—

**Ms Gillespie-Jones:** I wouldn't see why.

**Mr DREYFUS:** Hypothetically, it might be because there is no information to provide—in other words, that's a declined request.

**Mr Stanton:** Or if it was a request for data that is outside the categories under the legislation.

**Mr DREYFUS:** What happens if a telecommunications provider declines?

**Mr Stanton:** The data is not provided and there is presumably no compensation for the work done. I'm not aware of what other avenues agencies may use or can use in those circumstances.

**Mr DREYFUS:** Has any telecommunications provider ever been prosecuted for failing to answer a request or failing to provide data?

**Mr Stanton:** Not to my knowledge.

**Mr DREYFUS:** How much time do telecommunications providers spend reviewing requests for telecommunications data?

**Mr Stanton:** As we said, on an average business day there are more than 1,100 of those requests, which suggests that they have to deal with them pretty quickly. With those sorts of volumes, particularly the larger players have to make reasonably rapid decisions about whether or not to respond. Very often there is—

**Mr DREYFUS:** Just on this, what's the process? Do they look at who the requester is and, if it's a very frequent requester, such as the Australian Federal Police or the New South Wales police, that doesn't take much time at all?

**Mr Stanton:** That's right. Often they will have a relationship with the person making the request because it's a well-established channel. During the period when I was running a telecommunications company, the requests
from the AFP were regular. At that time—this is going back more than 10 years—they wanted responses within 24 hours max. Often they will be looking for responses in much shorter time frames than that. So clearly, if you're going to meet the operational expectation behind many of these requests, you don't have extended periods in which to ponder whether it's authorised or not. But on many occasions that will be beyond doubt anyway, particularly if they are one of the 22.

**Mr DREYFUS:** So the main effort will actually be on ensuring you've fully complied with the request by trawling through the necessary data and then packaging that up and sending it back by return email?

**Mr Stanton:** Yes.

**Mr DREYFUS:** Perhaps I could finish with just a general question. What would you say that metadata or telecommunications data can reveal about the person whose data it is?

**Mr Stanton:** It's a very powerful tool. It's often more powerful than content, we would say, because of the way that it can demonstrate patterns of behaviour, relationships and methods of operation. In the right hands, it's an extremely useful analytical tool.

**ACTING CHAIR:** Thank you very much for your attendance. If you've been asked to provide any additional information, can you forward it to the secretariat by five o'clock on Wednesday 19 February. You will be sent a copy of the transcript of the evidence and will have an opportunity to request corrections to transcription errors. Thank you very much for your time. I'll say, on behalf of the committee, your evidence is all incredibly helpful for us in our deliberations on a way forward. Thank you for your time. As there are no further witnesses, I declare this public hearing closed.

**Committee adjourned at 12:20**