COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL AFFAIRS LEGISLATION COMMITTEE

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

(Public)

THURSDAY, 17 NOVEMBER 2022

CANBERRA

BY AUTHORITY OF THE SENATE

[PROOF COPY]

LEGAL AND CONSTITUTIONAL AFFAIRS LEGISLATION COMMITTEE

Thursday, 17 November 2022

Members in attendance: Senators Antic [by audio link], Green, Scarr [by video link] and Shoebridge

Terms of Reference for the Inquiry:

To inquire into and report on the provisions of:
Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

WITNESSES

BAILES, Ms Rachel, Head of Policy, Australian Information Industry Association [by video link] 20

BLACK, Ms Wendy, Head of Policy, Business Council of Australia, [by video link] 20

BRAYSHAW, Ms Elizabeth, Acting First Assistant Secretary, Integrity Frameworks Division, Attorney-General's Department 27

FALK, Ms Angelene, Australian Information Commissioner and Privacy Commissioner, Office of the Australian Information Commissioner 1

FLOREANI, Ms Samantha, Program Lead, Digital Rights Watch [by video link] 8

GALLUCCIO, Ms Julia, Assistant Secretary, Information Law Branch, Attorney-General's Department 27

GHALI, Ms Sarah, Acting Assistant Commissioner, Regulation and Strategy Branch, Office of the Australian Information Commissioner 1

HENNESSY, Ms Isobel, Senior Legal Officer, Information Law Unit, Attorney-General's Department 27

LACEY, Professor David, Managing Director, IDCARE [by video link] 15

LOUIE, Mr Chris, Director, Digital, Cyber and Future Industries, Business Council of Australia [by video link] 20

NGUYEN, Mr Daniel, Acting Director, Information Law Unit, Attorney-General's Department 27

POUNDER, Ms Kate, Chief Executive Officer, Tech Council of Australia [by video link] 20

RAINSFORD, Ms Cathy, General Manager, Content and Consumer Division, Australian Communications and Media Authority 27

VAILE, Mr David, Chair, Australian Privacy Foundation [by video link] 8

WARREN, Mr Justin, Chair, Electronic Frontiers Australia [by video link] 8

FALK, Ms Angelene, Australian Information Commissioner and Privacy Commissioner, Office of the Australian Information Commissioner

GHALI, Ms Sarah, Acting Assistant Commissioner, Regulation and Strategy Branch, Office of the Australian Information Commissioner

Committee met at 08:59

CHAIR (Senator Green): I declare open this public hearing of the Senate Legal and Constitutional Affairs Legislation Committee inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. I acknowledge the traditional custodians of the land on which we meet and the Ngunnawal people and pay my respects to their elders past and present. I also acknowledge and welcome other Aboriginal and Torres Strait Islander people who are participating in today's public hearing.

The committee's proceedings today will follow the program as circulated. These are public proceedings being broadcast live in Parliament House and via the web.

I remind witnesses that in giving evidence to the committee they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to the 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 the committee.

The committee prefers evidence to be in public, but under the Senate's resolutions witnesses have the right to be heard in confidence, described as being in camera. If you are a witness today and intend to request to give evidence in camera, please bring this to the attention of the secretariat as soon as possible.

If a witness objects to answering a question, the witness should state the ground upon which the objection is taken and the committee will determine whether it will insist on an answer having regard to the ground which is claimed. If the committee determines to insist on an answer, a witness may request that the answer be in camera. Such a request may of course also be made at any other time.

With those formalities over, I now welcome representatives of the Office of the Australian Information Commissioner. Thank you for taking some time to speak with the committee today. Information on parliamentary privilege and the protection of witnesses and evidence has been provided to you and is available from the secretariat.

I remind senators and witnesses that the Senate has resolved that an officer of a department of the Commonwealth or a state shall not be asked to give opinions on matters of policy and shall be given reasonable opportunity to refer questions asked of the officer to superior officers or to a minister. This resolution prohibits only questions asking for opinions on matters of policy and does not preclude questions asking for explanations of policies or factual questions about when or how policies were adopted. Would you like to make a brief opening statement before we go to questions?

Ms Falk: I would.

CHAIR: Thank you, Ms Falk.

Ms Falk: The OAIC welcomes the opportunity to appear today and welcomes the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. We see this as a positive step towards updating Australia's privacy law to ensure that we have a regulatory framework that empowers individuals, that ensures entities protect personal information and that best serves the Australian economy.

In a digital world, where data knows no borders, our privacy law must protect Australians' personal information wherever it flows. That's why I support the simplification of the extraterritoriality in section 5B of the Privacy Act as proposed by the bill. It will help ensure that companies that carry on a business in Australia whilst domiciled overseas comply with Australia's privacy law. The simplification mitigates overseas companies avoiding the jurisdiction based on complex structural and technical matters.

Across the world and domestically we see higher penalties for privacy breaches and consumer protection type contraventions. To incentivise investment in compliance with privacy laws in Australia we need a multifaceted approach. This includes the OAIC continuing to provide guidance and advice, conducting assessments and identifying risks. It also includes having the ability to take court action to seek higher penalties in appropriate cases. Any decisions to do so will be proportionate and transparent and in line with our published regulatory action policy and guide.

We also need information-gathering powers and consequences for noncompliance. This ensures we have all relevant information to assess and help mitigate harms to individuals. We support additional information-gathering powers and infringement notices for noncompliance.

Another key feature of our regulatory environment is the need for multiple domestic regulators across content-specific domains to collaborate and coordinate. Recent data breaches have made this all the more apparent. The enhanced information-sharing provisions will ensure we can work together cohesively in the public interest, with clarity and certainty. That's also the case for international cooperation. The enhanced information-sharing provisions will ensure we have a clear framework for joint action and coordination with international regulators to ensure Australians' personal information is protected wherever it flows.

So we say the provisions of the bill together will enhance the OAIC's ability to undertake our regulatory functions in an efficient and effective manner in the interests of the community.

CHAIR: Thank you so much. We appreciate that. I just want to kick off, and then I will hand to the senators here that have questions for you. I have read quite a lot of briefing material on this bill, and it is still quite a complicated piece of legislation in an area of complicated law and policy. So I was wondering whether you could explain to start off with how the changes that are proposed in the bill will operate, particularly the new measures for serious or repeated data breaches.

Ms Falk: There are a number of aspects to the bill, and I am happy to start with the penalties. Currently, under the Privacy Act, there is already the ability for my office to seek a civil penalty through the Federal Court for a serious and/or repeated interference with privacy. So it's an existing power. The current penalty is set at $2.2 million per contravention. The bill proposes to increase that to $50 million, and there are certain other circumstances where the quantum can be assessed. That aligns it with the Australian consumer competition legislation, which has recently also increased penalties to $50 million. The provision is modelled on that law. It also, I think, is an important incentive for businesses across the country.

In terms of how that provision is and would be exercised, for the existing provision, section 13G of the Privacy Act, the only thing matter that's changing is the quantum. It's reserved for matters that warrant a civil penalty in the circumstances, so where it's necessary to send a strong deterrent message. We have published a regulatory action policy and also a guide as to how that power is currently exercised, and we see that the same factors will apply. The seriousness of the conduct is an operable factor, as is whether there has been a history of interference with privacy. I think it's helpful to say that the $50 million threshold is at the upper end of a penalty that can be sought and that there may be lower penalties that a court decides to award, depending on all of the circumstances before it.

CHAIR: One of the questions I had was in regard to the safeguards on sharing information. At the moment, under the current legislation, are they sufficient, how can they be improved and how is this bill addressing some of those shortfalls?

Ms Falk: The bill contains three amendments which would provide greater clarity and certainty for my office in disclosing and sharing information in order to get the best outcome in the public interest. Currently section 29 of the Australian Information Commissioner Act has restrictive non-disclosure provisions where I am prevented from disclosing information through my privacy functions unless it's in relation to the same function that I am exercising. This bill will allow for greater clarity and certainty as to when I can disclose information. Sections 33A and 33B would also allow sharing with other authorities and disclosures in the public interest. I can give a couple of examples.

CHAIR: I think that would be really helpful.

Ms Falk: What we seek to do is to collaborate, to coordinate with other regulators, to make sure that we are joined up, that we're cohesive and that we are not duplicating effort. We are able to achieve that currently, but not without having to turn our minds very carefully to this very restrictive nondisclosure provision. If we have additional clarity and certainty, I wouldn't envisage the circumstances of disclosing information to be markedly different. But, for example, in the Optus matter it was on the public record that the AFP was looking into the matter and also that I was looking into the matter, and I was able to reach out to the AFP to ensure my investigation would not interfere with their criminal investigation. However, there are many circumstances where neither party is aware of a particular matter before the office, because it's not in the public domain. I'd like to be able to say to the AFP: 'Is this a matter of interest to you? It's a matter of interest to me, and I want to ensure that any action I take does not interfere with any criminal investigation.'

CHAIR: What other types of agencies or bodies will you be able to share information with, in the interest of making the way we deal with these breaches in the future more efficient?

Ms Falk: Bodies such as the Commonwealth Ombudsman. If there are issues that I see arising through my regulatory conduct that I think ought to be brought to the Commonwealth Ombudsman's attention, it would enable that to happen in a more efficient way. Similarly, it would enable another complaint-handling body to deal with a matter where an individual has come to our office, and the matter could be more appropriately dealt with by another body. An example might be someone who has experienced online abuse and has come to my office. It may be much more appropriate for that person to address the eSafety Commissioner. But it would allow us to navigate that for affected individuals.

CHAIR: We've had some submissions and obviously some concerns raised around the extraterritorial provision. I think there is some concession that we need to make that provision as clear as possible. It's probably something that this committee will consider. I'm not pre-empting any recommendations, but it's something that we'll be interested in. For your part, what do you consider is the scope of the proposed extraterritorial provision in the bill? How do you see that operating? Why is it important? Australia is not isolated in the way that we exchange data, so what's the intention behind that?

Ms Falk: Currently, section 5B of the Privacy Act has this notion of having an Australian link in order for the act to apply. That link can manifest by a company being incorporated in Australia, and that's a very clear way that the act would have operation. It also has a concept that a foreign corporation that's domiciled outside of Australia could also be subject to Australian privacy law where it is carrying on a business in Australia. That part of the test is consistent with Australian competition and consumer law and law that's regulated by ASIC. But the current Privacy Act goes on to require two more factors to be proved in order for the jurisdiction to apply. That is not only that they're carrying on a business but that the personal information is collected or held in Australia. My regulatory experience is that that provision doesn't adequately acknowledge or represent the way in which contemporary businesses are structured and the way in which personal information flows across borders. So what I'm seeking is the provision to be simplified so that it's efficient: if a foreign entity is carrying out a business in Australia, they then have to handle Australians' personal information in accordance with our domestic law.

Senator SCARR: I've got some questions in relation to the penalty regime. I've been reflecting on the context in which these increased penalties would apply, and I'm giving you this background so that you have an insight into what my questions are based on. I'm trying to reconcile the fact that this bill, as I understand it, provides a penalty regime which is quite similar to what would apply under the anti-competition legislation, the anti-competitive behaviour legislation—the sort of penalty regime that would provide penalties in relation to cartel-like behaviour and activities by companies where they're colluding together in a conscious way to breach the law for their commercial benefit. In this case, the penalties are potentially applying, as I understand it, where a company may well have been subject to a sophisticated hack. Of course, there's a question as to whether or not they've taken reasonable steps to protect the data.

I want to tease out your understanding of the context in which these penalties apply, because it seems to me—and this is one of the issues I'm grappling with in this regard—that it's one thing for a company to proactively and consciously disclose privacy information or to misuse privacy information for commercial gain and achieve commercial benefit but it's another thing for a company to be subject to the unlawful behaviour of another party without any collusion with that party, any knowledge that that's occurring, and to almost be the victim, if that's the right word, of a hack and then be subject to a penalty regime which is quite similar to that which applies in some contexts to conscious corporate behaviour. I'm wondering if you could speak to that philosophical issue in relation to how this civil penalty regime applies.

Ms Falk: I've appreciated the opportunity to read some of the submissions that have also raised some of these issues. It might be helpful for me to first acknowledge your point about what the civil penalty regime does. The increased amounts would apply in a range of contexts, not only in a data breach context but also where there's a misuse of personal information by an entity, where there has been a secondary disclosure or where there has been a failure to obtain consent and so on. So it's across a broad range of privacy requirements.

There does seem to be some concern manifesting in submissions around the issue you raised—that is, where there has been a malicious actor that has then exfiltrated data. I have a couple of things to say on that. The first is that we need to ensure that Australians' personal information is protected from known risks. Just as we build a car and make sure that it can handle Australian terrain, we know that there are particular risks in our environment at present. One is malicious criminal actors; the other is human error. And these are causes of data breaches that I have brought to the attention of businesses across Australia through my six-monthly reports on data breaches that have occurred. Because they are known risks, we need to ensure that businesses put in place reasonable steps to prevent them. If they have done so, it will not constitute an interference with privacy, and therefore the issue of applying for a penalty doesn't arise. But, for example, if there has been a failure to mitigate known risks—if

there's been a failure, for example, to train staff or to alert them to how to identify phishing emails, or if the information is sensitive and warrants particular protection, such as multifactor authentication, and that's not provided—then they're the situations where I'd be more inclined to investigate a data breach and then consider regulatory options. A civil penalty would be only one regulatory option. The others are seeking an enforceable undertaking for the entity to rectify the problem and ensure it's not repeated; I can also make a determination, which is an administrative decision ordering or declaring that the entity rectify the situation; or, as you say, in more egregious circumstances, I can seek a civil penalty.

Senator SCARR: So you recognise that, as we're looking at this issue, there is some relevance in relation to assessing the intent of the company or the organisation that has the data. There can be breaches, where the privacy principles had been breached—they have not been followed or complied with. There's mens rea, as you'd say in the law; there's an intention not to follow the privacy principles, to obtain some sort of commercial benefit, on the one hand. But, on the other hand, it could be a situation where there's no positive intent to breach the privacy principles, but an assessment is made after the fact that reasonable steps haven't been taken to protect privacy. Is that correct?

Ms Falk: It's already been recognised in my regulatory action policy that the issue of recklessness or wilful disregard would be an aggravating factor that would point more towards seeking a civil penalty than the other circumstances that you've outlined.

Senator SCARR: Okay. Just focusing on that standard of recklessness or wilful disregard, when I look at that test in this context—to be frank, I find some attraction to that phrase. It's almost like the old concept of gross negligence. What does gross negligence constitute? If you're applying the penalty in those circumstances, where, let's say, there has been recklessness or wilful disregard, how does the mechanism work in terms of assessing the value of the benefit under the clause? In an anticompetitive context, I think you can work that out in terms of the commercial benefit that's been generated through, say, criminal cartel behaviour. In this context, where, say, putting it at its highest, a company has been reckless or has wilfully disregarded its obligations, and that company has been hacked, the benefit has really been realised by the entity that's done the hacking, in terms of accessing the information. The whole scenario is, in fact, a disaster for the company that's been hacked—from a reputational perspective and in terms of compliance costs and all the actions that have be taken flowing from the hack. So I'm trying to work out how the benefit part of the test, in relation to an increase in civil penalties, would actually be applied in practice to a scenario where a company has potentially engaged in recklessness or wilful disregard, because the benefit is actually flowing to a third party, not to the company that's been hacked. Does that make sense?

Ms Falk: Understood. I think that the provision as drafted offers three alternatives for the court to assess the quantum. One is up to $50 million. The second is an assessment of the benefit that flows. The third is related to turnover of the entity. In the circumstance you outline, the ability to assess quantum based on benefit would not arise because there has been no benefit in the scenario you've put that's arisen to the company. It would be more likely that the other two options for assessing quantum would come to bear.

Senator SCARR: Isn't that somewhat perverse? I'm just thinking that through. In a situation where a company has consciously breached the privacy principles and obtained some benefit, when you apply the test three times the value of the benefit would apply; that would be operative in terms of assessing the benefit in a situation. In that case, you've got three options: the $50 million; three times the value of the benefit; or, if the value of the benefit obtained cannot be determined, 30 per cent. You can work out the value of the benefit in that case, where a company has wilfully leaked information for some commercial gain, so you can presumably work out what that is—so it's $50 million or three times the value of the benefit. I would have thought it would be very hard to envisage a scenario where three times the value of the benefit is up into the region of 30 per cent of an entity's domestic turnover. In a situation where a company has been hacked and it hasn't achieved a benefit, it's the greater of $50 million or 30 per cent of an entity's domestic turnover in the relevant period. It's the greater of, so 30 per cent of an entity's domestic turnover in the relevant period is a huge amount.

Let me put it this way: if company X has a turnover of $1 billion in a scenario where it sold private information for $10 million consciously, then three times the benefit of that is $30 million. Now, $50 million is greater than $30 million, so $50 million would be the maximum civil penalty—you don't look at the turnover, right? If the same company had been hacked by an outsider there's no benefit to that company, so the $30 million is not relevant and it becomes a choice between the $50 million and 30 per cent of an entity's domestic turnover. In my example, it's $300 million.

CHAIR: Senator Scarr, I know you're explaining the context of your question but can you put your question. I need to hand the call over in a moment.

Senator SCARR: Commissioner, do you understand my point?

Ms Falk: I do. The point you're making is that the assessment of benefit in a situation where there has been a malicious hack may be difficult to determine, and if that can't be determined then the court might be looking at 30 per cent of the adjusted turnover. I think there are likely to be submissions by the entity that's been breached to say that the concept of benefit doesn't arise in the circumstances you're raising, in which case the maximum of $50 million may be operable. I need to stress: a court needs to assess the amount of penalty to be provided. It doesn't necessarily flow that $50 million will be what's awarded. Currently, section 13G of the Privacy Act is subject to section 80 of the regulatory powers act, which provides that the court must take account of all relevant matters, including the circumstances of the contravention, the nature and extent of any loss or damage suffered because of the contravention and whether the entity has previously been found to have engaged in similar conduct.

CHAIR: Senator Scarr, I'm going to hand the call to Senator Shoebridge. If we have time we will come back to your questions, or you can put them on notice.

Senator SHOEBRIDGE: Thanks to the office for turning up. I'm glad the office turned up, and we have a number of other key stakeholders turning up today, but I want to express my frustration that the committee invited Medibank, Optus, Woolworths and Telstra to come, because they clearly have experience relevant to what we are considering, and they all declined. I think that is a collective failure of that part of corporate Australia to come and clearly explain to this committee right now how this act would work, in light of the experience they're having. So I'm glad you've turned up. I think part of what Senator Scarr was asking was in relation to the tiered penalty regime. The second tier is, if an entity is maliciously sharing data, is consciously, deliberately sharing data, and seeks to obtain a benefit from it, in the example of a corporation with a billion dollar turnover, that benefit they get may be relatively modest; it might be $5 million or $10 million. That's not modest for me, but it would be modest for that entity. They would be consciously and deliberately trying to use data, in breach of privacy rules, to obtain a modest benefit. In that case, that company's maximum penalty wouldn't breach the $50 million, because you could identify the benefit. Let's say it was $10 million. As Senator Scarr says, the maximum penalty under proposed 3(b) of the new penalty provision would be $30 million. Because you can identify the quantum of the benefit, you don't get to (3)(c), so you don't get to what would otherwise be a $300 million maximum. Therefore you've got a more limited penalty of $50 million. Now, that's a company that consciously, deliberately, maliciously breached the privacy laws. But, if that same company had a hack, where they'd been negligent or reckless and the hack had got in and obtained the same information and they hadn't received any benefit from it, the maximum penalty for the sharing of the same information would be $300 million, because there is no benefit; you can't determine the benefit. So it kind of works a bit perversely. Corporations or entities that are intentionally and deliberately seeking to benefit may have a lower cap and a lower penalty than ones that are negligent or reckless. Why was that done?

Ms Falk: The preceding words, where it's intended to insert, after section 13G, (3), it refers to 'an amount not more than the greater of the following'.

Senator SHOEBRIDGE: Correct.

Ms Falk: So I'm not sure that I read that in quite the same way, but it's something that I'll reflect on, and I think the department is also appearing later today and might be able to address that in more detail.

Senator SHOEBRIDGE: Could I ask you about your funding. You were given an additional $5½ million in this budget to deal with the Optus breach.

Ms Falk: Correct.

Senator SHOEBRIDGE: And I assume that reflects the kinds of resources you will have to devote to what is a complex investigation and complex work?

Ms Falk: It does.

Senator SHOEBRIDGE: And that doesn't include the additional powers you are given in this bill, because I assume the budget was done before this bill had been fully ventilated; is that right?

Ms Falk: That is correct, but what I would say is that my view is that this bill will create efficiencies for the office. One of the issues that we face around the extraterritoriality provision is the time and resources that it takes in dealing with multinational, global corporations—and I'm in the High Court at present against Facebook on exactly this issue—to just assert that the Privacy Act has jurisdiction. I made a determination in relation to Uber that took several years because of these complexities around structural—

Senator SHOEBRIDGE: And this is about how the data is shared—

Ms Falk: Correct.

Senator SHOEBRIDGE: globally. I understand that issue and I understand that will create some efficiencies, and I'm sure that's good. But, if it's going to take you something in the order of $5½ million worth of resources to deal with just Optus, and you now have Medibank, MyDeal, Telstra—I don't know what happened this morning, but you've got whatever happened this morning—I can't conceive of how you're going to have the resources that you need to deal with the new powers and to deal with the expanded role you've been given. If it's $5½ million to deal with Optus and you've got about a $30 million budget for all of your obligations, how are you going to deal with Medibank, say?

Ms Falk: We already have the power to seek civil penalties; this is just about the quantum that can be sought. So I don't see that the bill itself creates additional resources imposts. In fact, I think the opposite, for the reasons I also said to the chair in my earlier remarks—it will create efficiencies in working with other regulators, with the ability to share information in a much clearer way.

But the issue that you raise around the resourcing of the office is a separate one. I have welcomed receiving the $5½ million for the Optus data breach. That will assist my office to uplift our capability more broadly, and I am continuing to be in discussions with government around the resourcing requirements of the office into the future, noting the significant issues facing Australian businesses, not only around data breaches but around complexity of information-handling practices.

Senator SHOEBRIDGE: But before you bring proceedings for a $50 million penalty, I assume that is very resource intensive, and it's going to require—I see nodding—a very significant investment from the office before you launch a prosecution with a $50 million maximum penalty?

Ms Falk: Absolutely, and I have said publicly that as part of the Attorney-General Department's more comprehensive review of the Privacy Act then I think that is the optimal time to assess the resourcing needs of the office and to ensure that we are set up in a way that can protect and regulate Australians' data in a way that is expected into the future. If I compare the resources of my counterpart in the UK, the Information Commissioner's Office, where they have nearly tenfold the staff of our office—they have a bigger jurisdictional remit—they have a system where any entity that handles personal information has to pay a very small fee to ensure that that office has the resources it needs. It demonstrates really what is required in a global framework of data flows to ensure that we are protecting Australia's digital economy.

Senator SHOEBRIDGE: That is the levy model that was considered in the privacy discussion paper that you endorsed, I assume, to get some ongoing funding?

Ms Falk: That is correct, yes.

Senator SHOEBRIDGE: Do you have an indication of how many of these kinds of prosecutions you would be able to do given your resources? What is the kind of maximum envelope of the number of prosecutions you could do given your resources?

Ms Falk: In the resourcing of the office, we will always take the regulatory action warranted in the circumstances. On this occasion, I have gone to government, I have sought the funding and it has been provided. I will continue to raise the issue of the need to have access to a funding base that takes account of the need to bring litigation.

Senator SHOEBRIDGE: So do I read it that the $5½ million for Optus is the kind of funding envelope you need to undertake a serious investigation, do the kind of research, back the expert opinions and be in a position, potentially, to prosecute? In a complex case like Optus, is that the kind of envelope we are talking about?

Ms Falk: I would say that is at the upper end because of the complexity of what we are dealing with in the Optus matter.

Senator SHOEBRIDGE: I have to be frank: we give you this new penalty power but you haven't got the resources to do that for Medibank or for Woolworths, because we already know that your office is slammed in other parts of your jurisdiction. Say, on FOI, we give you the penalty but you literally have only got to the resources to have one shot and that is with Optus.

Ms Falk: I welcome conversations about the resourcing of the office and continue to advance those. But as the regulator, I will ensure we take the regulatory action that is required in the circumstances.

Senator SHOEBRIDGE: My final question is: I know that your office has previously supported a privacy tort.

Ms Falk: Yes.

Senator SHOEBRIDGE: Given the resourcing constraints attached to your office bringing penalties, if we are going to hold corporate Australia, and governments as well, to account, that privacy tort is kind of a missing link, isn't it?

Ms Falk: The Attorney-General's Department has raised the issue of a tort of privacy, which I support. The other aspect is to have a direct right of action for individuals to take action through the courts. Currently we don't have a recognised common law right to privacy that can be actionable. There are media reports that certain law firms are looking to contest that in the current environment.

Senator SHOEBRIDGE: Some kind of equitable action.

Ms Falk: But I do see that a direct action for breaches of the Privacy Act is an avenue that would help to address the issue that you've raised.

Senator SHOEBRIDGE: That's, if you like, a privacy enforcement measure that can be done outside of your office.

Ms Falk: That's correct.

CHAIR: There's been a discussion about penalties. I'm right, aren't I, that the court will still have to decide whether a penalty is reasonable, with all the bells and whistles of what is usually considered? And I wondered whether you could speak to the size of the penalty being an incentive for businesses to prevent breaches happening in the first place.

Ms Falk: What we see is a move both domestically and internationally towards regimes with higher penalty provisions. I've mentioned the Australian Consumer Law, and this would align with that. There's also the General Data Protection Regulation in the EU, and there has recently been the Digital Market Acts enacted in the EU, with fines of 10 per cent of gatekeepers' worldwide turnover and up to 25 per cent in certain circumstances. We do need to have an incentive that ensures that corporate Australia invests in the security of Australians' personal information. Ideally the penalties would not need to be utilised, because we'd see an uplift in security posture and a reduction in data breaches.

CHAIR: Thank you. That's all the time we have today. I'm sure we could ask lots of other questions. Thank you very much for taking the time to give evidence today.

Ms Falk: Thank you.

FLOREANI, Ms Samantha, Program Lead, Digital Rights Watch [by video link]

VAILE, Mr David, Chair, Australian Privacy Foundation [by video link]

WARREN, Mr Justin, Chair, Electronic Frontiers Australia [by video link]

[09:41]

CHAIR: I now welcome representatives of the Australian Privacy Foundation, Digital Rights Watch and Electronic Frontiers Australia. Thank you for taking the time to speak with the committee today. Information on parliamentary privilege and the protection of witnesses and evidence has been provided to you and is available from the secretariat. We do have limited time today, but would any of you like to make a very brief opening statement before we go to questions?

Mr Warren: We provided one, in writing, to the senators. We're happy for that to be entered into the record.

CHAIR: Thank you—and we do have submissions. Mr Vaile, would you like to make a short opening statement?

Mr Vaile: Thanks for the opportunity to address the committee. Before looking at the specific amendments, I want to put a question that might give a new context for thinking about these changes, in light of the exploding risk manifested by the Optus, Medibank, Woolworths, Telstra and other incidents: is personal data held online actually an asset, the new gold, or is it bait for cybercriminals?

I see the *Mandarin* said yesterday it was a 'toxic asset', as a global security expert, Bruce Schneier has put it; or uranium, as tax office Second Commissioner Hirschhorn said recently. If it's the latter, as I think is the case, will these new amendments have any impact on the problem of data breaches, especially the ones arising from a custodian's failure to commit enough resources to adequate protection or their failure to adopt what we think is the only strategy likely to have reliable preventative impact on future breaches, which is the most important thing: one-off data minimisation—doing more with less, collecting less, using less, sharing less and storing less—rather than going on with the big data industry's assumption that more is better. 'We have to collect it all. We're all going to be rich. We just want a huge data lake.'

But data protection in Australia has long been a matter of too little too late and, in a sense, often just making theatrical gestures, rather than creating a fast and effective regulatory tool which enables Australians to protect themselves or tools which increase the costs of weak security or data gluttony to a high enough level to incentivise the custodians to no longer treat the risks that they project onto Australians and the feeble or non-existent penalties that they face when things go wrong as merely a cost of doing business and one which is lower than the investment required to do the right thing. I note that Bruce Schneier at the recent World Ethical Data Forum pointed out that one of the main useful things we can do at the moment is increase that level of cost to increase those incentives. It's something I've been saying for a while, like I said.

Onto the specific amendments, yes, we support the increases. We do say that you should remove or replace the 'serious or repeated' limitation on these penalties and leave it up to the courts to decide how to assess the proper penalties. We have heard from the previous discussion that there are a lot of existing factors which are to be taken into account. I would prefer to leave it up to them. There are too many examples of Australian privacy law giving with one hand and taking back with the other quietly. Legislators have often seemed to want to put in loopholes, exceptions, back doors and limitations, all apparently to avoid scaring the horses by being seen to be going too far. If not scaring the horses was ever a reasonable thing to do, that day is long past. We say we now need to scare the horses. The horses don't feel any pain if they are lashed with a limp lettuce leaf or can always get away with anything that happens by begging for forgiveness when they choose not to invest to do the right thing when it matters, which is before everything is going wrong. The 'serious and repeated' test is a barrier to letting the regulator and the courts judge how to characterise each instance properly.

We also say you should simplify the calculation of the maximum penalty. I understand the commissioner was raising this issue. It is not possible to calculate the benefit obtained from an interference. In many cases it's just not having to invest enough or not having to trim their sails enough to use data in a safe, minimalist way. If there is going to be a limit, it should be much higher than the $100 million there. I said previously in the digital protections inquiry to the ACCC that I agree with the approach [inaudible] of a global turnover. I hear 20 per cent is now on the table. We think it should be up at that sort of level for a massive global corporation. If you have to put a figure on it, it should be somewhere in the $300 million to $500 million range.

CHAIR: I don't want to cut you off, but we have senators who have questions and we do have the benefit of your submission. So if you could just wrap up we will get to some questions where you will probably get to address some of these issues.

Mr Vaile: Then I would just also like to emphasise that we agree with all the submissions saying that the commissioner needs more resources but also resource limitations so far need to be addressed by the other thing that has been recommended, the 30 years for a private right of action, particularly one that enables class actions, which would in appropriate cases take the burden off what would be a massive task.

CHAIR: Digital Rights Watch, did you want to make an opening statement? We do have a submission from you as well.

Ms Floreani: Yes, please. I would like to.

CHAIR: If you could keep it brief, we have senators with questions.

Ms Floreani: Of course. On behalf of Digital Rights Watch, I would like to thank you for inviting us here and for the opportunity to participate in today's hearing. The harms of a data-driven economy and the business models of surveillance capitalism are becoming increasingly obvious. Breaches which make people more vulnerable to identity theft and scams are really just the tip of the iceberg. There are a range of other harms that arise when personal information is inappropriately or unfairly handled. Just some of the other forms of harm include microtargeting, profiling, manipulation, discrimination and exclusion. It is our view that stronger privacy protections have a critically important role to play in minimising the harms of the data-driven economy.

Overall we support this bill and we are glad to see movement in this space after many years of advocating for privacy reform, but we caution that it does not go nearly far enough. It is essential that, should this bill pass—and I hope that it does—it doesn't serve to slow or kill the momentum and motivation for real, comprehensive and meaningful privacy reform. This bill on its own will not achieve the kind of privacy protections that are needed to keep individuals and communities safe in the modern digital economy. That said, I understand that the meaningful reforms are beyond the scope of this particular bill and are to be considered as part of the broader review process, and so I will turn my attention to what's currently in scope.

First, we welcome the increased penalties. However, we do have some concerns regarding how these fines will actually be levied in practice. We believe that some tweaks to the proposed regime could make it more effective. Under the current bill, these penalties would still need to meet the 'serious or repeated' threshold and require the OAIC to apply to the Federal Court to levy them. Not a single penalty has been imposed under the Privacy Act since the provision came into effect in 2014. The OAIC has only sought a penalty in one case, against Facebook, which is ongoing. We do believe that fines can be an important deterrent and encourage executives to prioritise privacy compliance. However, as long as the enforcement regime is limited to serious or repeated conduct and fines can only be levied by the Federal Court, we are concerned that many organisations will continue to ignore their obligations. If the likelihood of being penalised is perceived to be low, then it's unlikely to have that desired deterrent effect, no matter how big those fines are. We're concerned that the maximum fines won't happen often in practice and will be reserved for only the largest companies, who are willing to spend years fighting in court. As such, we suggest that consideration be given to a scalable or tiered penalty regime and to amending that 'serious or repeated' threshold. We would like to see a dynamic system that avoids fines becoming seen as part of doing business but also ensures that they are effective and readily available where organisations do the wrong thing.

My second point is that there is a lack of pathways for meaningful redress for harmed individuals. Millions of people are experiencing severe distress and the threat of scams and identity theft as a result of major data breaches, including Optus, Medibank, Vinomofo and Harcourts real estate—and these are just the breaches that we know about. Breaches are happening all the time, and often they are not newsworthy enough to make it into the media. But the harm caused by privacy infringements is not limited to just breaches, and it is clear that the OAIC cannot handle all of this alone. A direct right of action and a statutory tort for serious invasion of privacy would give people pathways for redress, including the ability to lodge a case without needing to go through the OAIC. It would be an important pathway for people to take their right to privacy into their own hands. It would also—

CHAIR: I'm just going to stop you there. I know that there is a lot to talk about in this space, but we've got some questions about the bill, and I just want to get to those, so, if you could just finish up quickly, thank you.

Ms Floreani: I'm happy to end it there.

Senator SCARR: Thank you to everyone for joining us today, and congratulations to each of you and your organisations for your important advocacy in this space. It is deeply acknowledged. I'd like to ask questions in relation to this penalty regime. You may well have heard some of the discussion we were having in the earlier session. I note the comments made with respect to 'serious or repeated' breaches. To your knowledge, have there been any cases or interpretations with respect to what 'serious or repeated' breach means in this context?

Mr Vaile: There are very few legal precedents in this area, very little court analysis of the meaning of particular provisions, because there is no easy way to get into court. It's a very unusual area because of the lack of a cause of action. So we are left with the commissioner's guidelines or nothing.

One of the other problems is, as Samantha just said, there's no experience of the application of a lot of the more serious penalties and enforcements available to the commissioner—which are a very limited set—because, for whatever reason, they very rarely get levied. So it's impossible, unlike in some other legal areas, to assess what a tariff would be and the likely lower level and the higher level and whatever. You'd just be guessing if you were a counsel trying to advise a client. You wouldn't really understand what the maximum was, and all you could probably say is, 'It's extremely unlikely you will ever face any fine at all.'

Senator SCARR: Ms Floreani, do you have a view in relation to that? And, Mr Warren, what's your view in relation to that?

Ms Floreani: Certainly I would say the threshold is currently too high. I would echo what David has just said in terms of not having any examples to point to because it hasn't gone through the Federal Court, aside from the Facebook case which is currently still happening. I'm reluctant to focus too much just on breaches because, as I said, there are plenty of other harms that can arise. There are plenty of examples of breaches which have caused immense harm to many millions of Australians, and if they're not able to get up to that level of 'serious or repeated'—which maybe they are or maybe they're not—then I think that represents a fundamental flaw in this process.

Senator SCARR: Mr Warren?

Mr Warren: Similarly, we're not aware of any legislative exploration of this particular phrase.

Senator SCARR: Mr Warren, does that mean that one way to approach this would be to actually provide more certainty in the bill around what 'serious or repeated' means?

Mr Warren: That would certainly assist. We would certainly appreciate greater guidance. Otherwise, as we've seen in other regimes, such as around the Freedom of Information Act, there is a large amount of exploration of what the law actually means through case law. That takes time. As others have said, we don't have the case law to base this on, so having greater guidance that's actually in the legislation itself is important. Sometimes parliament attempts to provide guidance through the explanatory memorandums, but they don't actually have the force of law so we would like to see that actually in the legislation itself.

Senator SCARR: Mr Vaile, if I can come back to you, the concern I have, to be open with you, in terms of removing the concept of 'serious or repeated breaches' is that the penalties we're talking about are extraordinarily high. They're a great amount. And when I reflect on this I reflect on the fact that a listed public company can potentially have hundreds of thousands of Australian shareholders who will ultimately pay the economic cost of the fine, but they've got no ability to control what the senior executives are doing to manage these risks in any meaningful way. Do you think that is an alternative? Instead of removing the concept of 'serious or repeated', that the legislation will actually drill down and provide more guidance with respect to what that actually means?

Mr Vaile: I have two different responses to that. One is that I agree that it can be useful to include some indicators or some of the factors that you'd use to assess the seriousness, but I understand from the previous discussion that there are already generic tools available in legislation that point to the appropriate consideration of the number of factors and the severity of those factors. So we're not starting from nothing—it's not a black hole.

The real problem is that there is no experience. There is not a practice of fines being widespread.

Senator SCARR: That may well change.

Mr Vaile: The other problem is, I've been looking at this area for many, many years—for decades—and one of the things that's remarkable is how few determinations the commissioner's office ever made when there was a dedicated privacy commissioner, and how few penalties are ever levied. One of the concerns you have is that there are lots of barriers and lots of disincentives and nudges saying, 'Don't go too far,' or whatever to do this, and they've created an environment and the lack of resources where nothing is going forward. I'm sympathetic with the concerns of shareholders, because controlling rogue executives who've adopted the latest fad of data everywhere—collect it all or whatever—is difficult. On the other hand, there are also millions, or tens of millions, of Australians who are potentially suffering not only the known breaches but the effect that may spread through their entire lifetimes and may affect their families or communities as well as them as individuals. Also, I'm concerned for the good companies, the responsible corporate citizens, of whom there are very many. I've heard from security people, governance people and others saying that everybody looks around at this and sees that there is no penalty, so why not try it? The conscious rule of thumb in some of the bigger operators is 'move fast and break things' or 'try for forgiveness, not permission', which is essentially seeing if they can get away with it.

Senator SCARR: If I can interrupt you—I'm hesitant to do so, but I have limited time. I want to ask you one final question, and then the chair will need to share the call. You're drawing a distinction—and I think it's right to do so—between, say, the rogue operator, the company that may be consciously saying, 'We're moving ahead and a few things are going to be broken along the way', as opposed to the good corporate citizen that is really trying to do the right thing and staying ahead of the game, which I assume is very difficult in this space. Do you think it would be helpful for there to be something like a safe harbour in the bill that says, if you have done the sorts of things we would expect you to do, and the sorts of things that your agencies, your organisations and the people you're advocating for would expect you to do, that should be a safe harbour and you should have confidence that you're not going to have civil penalties levelled against you?

Mr Vaile: I'm not a fan of safe harbours. In the European and US context it was eventually found that there was no basis for that, and it was used to lower the benchmark and lower the standards of protection for half a billion people in Europe. I think the danger is that there's already too much incentive and too much drift within the—

Senator SCARR: Okay. I want to get the views of the other two witnesses on that safe harbour point because it has been raised in some of the submissions. Mr Warren?

Mr Warren: I think changing the incentives to create a positive incentive—so some carrots, not just sticks—viewing this more as a public health issue rather than a policing matter and trying to punish people, is beneficial. However, I do echo Mr Vaile's concerns that often these safe harbour mechanisms are used as a way of avoiding consequences rather than as an incentive towards good behaviour. They would need to be very carefully designed.

Senator SCARR: Ms Floreani?

Ms Floreani: I would echo what Justin and David have said. I would also raise that, if these companies are able to demonstrate they've taken the reasonable steps under the various privacy principles, I would argue that they would be able to make an argument that they have not been in breach of those privacy principles. If they've done the right thing then they shouldn't be penalised.

Senator SCARR: Thank you.

CHAIR: Senator Shoebridge, you have the call.

Senator SHOEBRIDGE: Thank you all for your submissions and your engagement with this, and, in fact, your ongoing engagement with privacy reform, which is a lot more than just this bill. Could I ask about the penalties, first of all? One of the options available would be to have two tiers: one which has the $50 million or turnover basis as proposed in this bill and has the serious or repeated requirement, and the other one which mirrors that provision but removes the serious or repeated requirement, and has an action available, a civil penalty, where there's been interference with the privacy of an individual, and have that set at the existing penalty regime under the existing act so that there's more than one option for the Information Commissioner. What do you think of that as an alternative?

Mr Warren: I'll start with that. We agree that there should be a graduated scheme. However, as during the discussion with the Information Commissioner, we think putting all of the penalties in the hands of one single regulator creates a bottleneck. We've seen this in other regulatory regimes as well. A regulator simply cannot have time to deal with everything, and, particularly for smaller breaches, the harm still occurs to an individual.

With a breach, it is more of a deterrent. That seems to be the structure of the way this legislation is set up. That doesn't actually do anything for you as an individual. Even if they are found to have breached the act, and a fine is levied against them, that doesn't come to the victims. So, as you mentioned, by adding a private right of action to that graduated scheme—so you still have the regulator based penalties and deterrent effect—there is a further constraint on this behaviour from companies that do it en masse or do it a lot. They place themselves at risk, because paying out $500 per person scales up quite quickly. It does actually align a redress scheme to the individuals who are harmed as well.

Senator SHOEBRIDGE: So Electronic Frontiers' preference is to simply bite the bullet and put in place a private tort at this point?

Mr Warren: As well. We're not advocating that we get rid of the Information Commissioner.

Senator SHOEBRIDGE: No, I understand.

Mr Warren: We're saying in addition to certain penalties, and with great power comes great responsibility. If large companies are collecting huge amounts of data, they're in a position to create a serious breach. A ready option available to them is to simply to give up that power and stop collecting that much information.

Senator SHOEBRIDGE: I assume you heard the evidence from the Information Commissioner earlier, which seemed to be that they've got the resources to do one of these. If it costs $5½ million to do Optus—they've got a $33 million total budget for all of their duties. Parliament can pass whatever penalties they like, but there's going to be, at best, one a year or one per season. That's not really a deterrent, is it?

Mr Warren: Not at all. As we put in our opening statement and in submissions, we think there are possibly incentives. Some of the penalties on that sort of scale pose an existential risk for many organisations. So there's an incentive for them to either potentially hide it, which actually makes things worse—it's a perverse incentive—or indeed just slow down the action through prolonged court action, because for them it makes sense that a very small likelihood of success in court means it's worth fighting for a very, very long time. We've seen that in other industries.

Senator SHOEBRIDGE: Ms Floreani?

Ms Floreani: I would echo what Justin has said. We absolutely need a direct right of action and a statutory tort of serious invasion of privacy. My preference would be to have both of those avenues available. I am quite open to the idea of there being some kind of tiered penalty regime, as you've put forward, one where there are more readily available fines that can be levied quickly for interference with privacy that doesn't meet that serious and repeated threshold. I'm also quite in favour of that penalty then being diverted to the harmed individuals as well. I think that there is a lot of room for improvement in this penalty regime to make sure that it is both being an effective deterrent and assisting in creating pathways for redress for harmed individuals.

Senator SHOEBRIDGE: One of the elements of this bill that is counterintuitive is we've got a real problem with data being unlawfully shared—and 'shared' is a polite term for it; there are constant data breaches—yet what this bill does is put in place a whole series of new avenues for data sharing to happen at a government level. Do any of you have any observations about that?

Mr Vaile: Yes. We're very concerned that the cure for data being spread too far is to spread data too far. We think there should be checks and balances that involve things like notice to the affected individuals if it's personal information. If it's not personal information, then we're much less concerned about it. There should be specific limitations on purpose sharing, time limits for retention and time limits for further usage. In a sense, there is a culture both in government and in business that has been spurred on by this data maximalism—the idea that there's no downside, no cost, no risk to keeping and disclosing without consent the information of individuals. It's because the risk is projected entirely onto the data subject. If there's no realistic likelihood of either a commissioner penalty or being sued, then we can just say, 'Oh well, too bad, we're probably not going to be caught.' The most important thing, we think, is by a private right of action and also by cranking up resources and the penalties available to raise the assessment made by rational people saying, 'Will we invest in this or just more marketing?' to say, 'Actually, boss, we have to recognise that there is a real risk here.' I've heard compliance, governance and security specialists in big corporates, in finance and banks, saying, 'We'd like to do the right thing, but if nobody else is doing that, we will just—

Senator SHOEBRIDGE: Follow the herd, yes. Mr Warren, you say this in your tabled opening statement: 'Parliament must also take responsibility for its own role in overcollection.' Are we repeating some of the errors of the past with this bill in data sharing?

Mr Warren: Yes, you are.

Senator SHOEBRIDGE: What's the remedy for that?

Mr Warren: Don't do that. There are two issues. One is that parliament and regulators see themselves as saviours of people: 'We will do it for you.' For example: 'We will share data amongst ourselves. Trust us; we're the elites. We know what we're doing'—despite decades of evidence to the contrary. They do that rather than empowering people to protect themselves.

The most important part here, however, is: you can't lose what you don't have. Removing legislation that requires organisations to overcollect—in many cases this has been passed for law enforcement purposes. Removing that legislation means organisations won't collect the data in the first place. Government also needs to take that same action and stop collecting data on citizens that it can then lose.

Senator SHOEBRIDGE: The safest data is the data that's not collected in the first place; is that right?

Mr Warren: I think the quote is 'three may keep a secret if two of them are dead'. Yes, you can't lose what you don't have—so if you don't collect it the problem goes away. That's really what we need here; we need a systemic change from overcollection of data, particularly personal information. It is impossible to look after it perfectly. The best way to reduce the risk is to not have it in the first place.

Senator SHOEBRIDGE: Ms Floreani?

Ms Floreani: I don't have anything to add to that. I think Justin summed it up very well.

Senator SHOEBRIDGE: Mr Vaile?

Mr Vaile: I'd like to support that but also say that one of the other steps that needs to be taken here—Justin has hinted at it—is to review all the drivers created by parliament, created by law enforcement, created by a profession that is working on the old assumption that it's cost free to collect more, to store more, to use more and to disclose more. When I was on AUSTRAC's privacy consultative panel, which was randomly abolished two years ago, I asked: 'Is there any disincentive for constantly ratcheting up the expectations of more and more data collected? For every small pawnbroker and small business, large business, banks, whatever, there is this FATF international mechanism by which you and your colleagues all ratchet up the standard. Where is the banking secrecy in that? Where is the data protection? Where are the IT security people saying, "This is a risk. This is a problem. This is disproportionate"?' The answer was: 'No, there's none of that. There's no counterinfluence in these schemes. We are just doing what we can do, which is to do what we're doing.' There is no voice going the other way saying: 'Can we revisit? Can we sunset some of those? Can we minimise some of those? Can we start with the awareness that the more we collect, we are making honey pots and we are making problems?' One of the things parliament could do is lead by example, be very cautious about endorsing anything that is not a turnaround and a retraction and look at all the different influences that are going in the wrong direction, that have just been set in concrete and that have an incremental relentless momentum to ever expand the collection. A useful initiative that would come out of this is to explore that. I think it's that sort of cultural change that will be necessary.

Senator SHOEBRIDGE: You'll be pleased to know that we'll very safely keep all of your contact details on file for if we need you for another privacy review.

CHAIR: I thank you all for your contributions today. You have covered off some of what I want to ask about. Your submission seemed to generally welcome the amendments as a starting point. I think you have raised some of the things you would like to see in addition to this bill. I want to take you to the penalty and enforcement regime in the bill. Why do you think that's important as a starting point? I'm happy if you want to add things we should be looking at in addition to that.

Mr Warren: It's useful as a starting point because it is evidence of a change in attitude—that there is willingness within parliament to change the system of incentives. We disagree about some of the nuances of how that's going to be done, but we broadly support the recognition that there is a systemic issue here that will require a systemic change in incentive structures. We would like to see a lot more of that, but, as others have said, there are existing inquiries exploring that in more detail and across a broader range—the existing review into the Privacy Act and the Richardson review's recommendation to review the overall surveillance regime.

CHAIR: I do have a couple of other questions as well, but does anyone else want to jump in on that? No? Okay. This might not be something you've thought about in depth, but there are provisions in the bill that extend the extraterritoriality of the bill. I wonder if you have any opinions or thoughts about those provisions—how they can be improved or made clearer. Something that has been raised through many submissions is that those provisions are needed but we need to consider how we can make them clear.

Ms Floreani: I generally support this proposal to remove that particular paragraph—and I have lost the specific paragraph. I think this represents at least a first step to ensure that the Privacy Act is fit for purpose for a global internet economy. Currently, foreign entities that do business in Australia only have to meet the obligations of the Privacy Act if they have that Australian link, and that includes the condition that they collect or hold information from a source in Australia. This in practice can be hard to establish. For example, a company could collect information that relates to an Australian from a digital platform that doesn't have servers in Australia and it would come up to this situation where it becomes tricky to establish if it meets that threshold. I think removing that paragraph does play an important role in bringing the Privacy Act into the modern economy.

Mr Vaile: This continues the innovation by Australian lawmakers that we see in the Australian consumer law, which has a similar but very interesting extraterritorial impact. It's not framed in the same way but it means that a lot of the terms of use of software and other services offered online globally have a little provision at the end saying: 'By the way, if you're Australian'—I'm not aware of the actual details of the inclusion—'we have to tell you you've still got rights. Whatever you thought were the terms of use, or the contract, that gave away all your rights, they possibly don't apply, and we have to tell you about it.' That is quite unusual. There are not many other countries. The EU has attempted to do that sort of thing, so that's very good.

We think another thing that needs to happen, though, is that the entities that are affected by the extraterritoriality provisions should be obliged to have a local establishment or appoint an Australian representative. I'm reminded of the time I met the global Facebook policy guru. It was at a time when they had five million customers in Australia and no relevant Australian operation. They changed a bit and had a little office, but their subsidiary had virtually no connection here. There's a practice of global entities operating in Australia and putting Australians' data at risk by not engaging properly with our jurisdiction. So something that is a little bit similar to what the EU does—and I understand that Twitter is now at risk of having a representative, a data protection officer and an office, within the jurisdiction—would be a very useful further step down this path.

CHAIR: Thank you. That's really helpful. I apologise that that is where we'll have to leave the discussion today. I know that you are regular contributors to Senate inquiries into legislation of this kind. Thank you for the time you've taken to prepare submissions.

LACEY, Professor David, Managing Director, IDCARE [by video link]

[10:27]

CHAIR: I now welcome the representative from IDCARE. Thank you, Mr Lacey, for joining us and taking the time to speak with the committee today. Information on parliamentary privilege and the protection of witnesses and evidence has been provided to you and is available from the secretariat. Would you like to make a brief opening statement before we go to questions?

Prof. Lacey: Yes, I will. Thanks for the opportunity to speak with you today. For those who are unfamiliar with IDCARE but may well have seen our name bandied about in the media, particularly over the last few months, we are a national support service and community organisation registered as an Australian charity, and we also have a New Zealand charity in operation. Our raison d'etre is to provide practical, behavioural and technical support to members of the community who experience the loss and misuse of personal account and credential information. We were born from the National Identity Security Strategy 2009, which had as a policy priority area the support of victims of identity crimes and other related acts. So we were formed out of a joint government industry initiative—hence the not-for-profit and charitable status.

Since that launch in 2014, we've responded to in excess of half a million community engagements across Australia. Around a quarter of the people that engage IDCARE services and speak with our specialist case managers have no idea how their information was actually compromised or stolen, and they have experienced the exploitation of their details by criminals through, for example, the establishment of accounts with financial institutions, accessing of government services and hacking of social media accounts, email accounts or the like. For that cohort in the community, you can imagine the impact that will have on them emotionally but also financially and, going forward, their participation online in other arrangements that they may have in their lives. Their confidence is certainly dented.

At present, probably around a quarter of the work this calendar year has been devoted to supporting organisations respond to data breaches, and obviously the motivation of the committee in looking at reforms around the Privacy Act is very much welcomed by IDCARE. We do support the provisions that are in the bill in terms of sharpening the focus of organisations on how they are treating personal information and the penalties that might arise as result of it. We think the penalties are quite commensurate with the pain that we see caused across the community when such things happen. But we think the bill also perhaps falls a little short in terms of going directly to the pointed issue as to whether organisations should pay ransom to these criminals and what the penalties for the payment of such ransom should be or should at least be entertained.

For committee members who may not know my background, I come at this as a former director of the Australian Crime Commission, a Commonwealth entity charged with disrupting organised crime. Most of my years working for that organisation were spent targeting groups committing these crimes. For post a decade since, my professional life and career have been focused on supporting community members directly impacted by these organised criminals, through the work of IDCARE across the community. So I come at this from probably a pretty unique perspective, and I don't say lightly that organisations should be prohibited or there should be some type of offence created directly around the payment of ransom, but I do think it's worth this committee exploring that specific point in addition to the raft of other reforms that has been put forward in the bill that's being examined and considered.

Chair, I'm happy to take questions. I hope that's been useful in terms of setting the scene.

CHAIR: Thank you, Mr Lacey, that has been helpful. I've just got a couple of questions. You've outlined what IDCARE does. What services do you offer businesses that might have faced a data breach?

Prof. Lacey: Yes, IDCARE's a bit of a strange model. We're not a public benevolent institution, so we're prohibited from receiving donations—nor, to be honest, would we want to contemplate charging the community or receiving financial benefit. To sustain our business, our charitable work, we have to deliver services that organisations pay for. In the context of breaches, that would include potentially the delivery of a harm assessment. So, where organisations are familiar with what information might be exposed in a particular breach, IDCARE can provide a much more independent and much more rigorous view of what the real risks are to the community and, most importantly, what are the response affordances available to individuals in treating that risk of harm. So harm assessments and response plans are one particular service we provide.

In the case of Optus and Medibank, we've been asked to provide a couple of things to those organisations. One is an online information guide, if you like, for people that have been notified about those breaches, and what IDCARE feels are some response considerations people may wish to take to protect themselves. The other is a point of reference to individuals who are impacted by those breaches who believe that, because of those breaches,

they are experiencing other crimes and exploitation in their name. So it's much more of a specified support service to those customers in that situation.

CHAIR: Thank you. With regard to the breaches themselves, do you think that there's been an increase in data breaches, or is it just that the scale of the people that are impacted has recently increased? Is it that they're high-profile entities that we're talking about, or have we actually seen an increase in this type of behaviour?

Prof. Lacey: We monitor online places for law enforcement and national security agencies and other institutions. One-half of the work that we do is to keep an eye on what criminals are doing and help inform law enforcement and others about where there might be opportunities for intervention. We've observed about an 80 per cent increase in ransomware attacks against Australian entities over the last three months. So, to answer your question, yes, there's been an escalation that we've observed through those online channels and places. That might be a bit counter to the statistical reporting that's provided by the regulator. The Office of the Australian Information Commissioner, as the privacy regulator, produce reports on six-monthly trends around their own regulatory reporting environment and how that might be increasing. We haven't yet seen a greater jump in those reports to the regulator such as we have seen in terms of the activity in those online environments. Those two aren't commensurate at the moment.

CHAIR: You spoke about the measures in this bill. I'm going to pre-empt some of your answers and say that I am interested to know what you would like to see beyond this bill, but if we can just deal with these provisions. The size of the penalty has been discussed by many submissions. The need to have some incentive or disincentive for businesses to actually take preventative measures, I think, is captured by the provisions, but, from your perspective and the experience that you bring to this conversation, are those penalties necessary? How do you think that will actually affect the behaviour of big companies?

Prof. Lacey: I think the penalties certainly are robust enough to sharpen the focus of boards on how they are protecting personal information and how they are assessing, if there are incidents, the harm around those and the remediation and response to those events. If an outcome or an intention of the bill is to achieve that, then I have confidence that the penalties will achieve it. There's a flip side to that argument, which would be that if that's the penalty, maybe there's a disincentive to report to the regulator. I think, from what we're seeing in the environment at the moment, there's perhaps a degree of under-reporting, and that's in the absence of these types of penalties in any case. So we don't necessarily feel as though the increase of penalties or what organisations might be up for will necessarily create that disincentive to report. We think at present there is still a degree of under-reporting going on around these incidents.

Medibank—what its customers are experiencing and what that threat actor is trying to achieve through its information operations and through using the media in the way that it is—is amongst the ugliest breaches we've ever seen. In its own right, certainly what we're seeing is that organisations are increasing their engagement with IDCARE, wanting to know that the way they're going about preparing and planning for these events is consistent with others and is best practice.

The other aspect of all of this is that there's the penalty side but then there's also the response side. There are measures within the bill that talk to the ability for the regulator to understand more about how an organisation has responded or is responding and to make a more informed assessment of that, which I think is also an important addition to the bill.

CHAIR: Beyond this, there's a review around the Privacy Act, and some of our submitters and witnesses today have raised some of the things they'd like to see through that act. I know this is an inquiry into the provisions in front of us, but, extending beyond this particular bill, what are the types of things that you'd like to see introduced?

Prof. Lacey: I think there really needs to be serious consideration of whether paying a ransom is an offence. In my experience of working with organised crime intervention and the disruption landscape it is a business model, and the way to disrupt, effectively, organised crime is to disrupt their business model. There was a report released within the last week by a leading cyberforensics firm, McGrathNicol. They had surveyed 500 Australian businesses on whether they had experienced a ransomware attack. Around, from memory, three-quarters had over the last five years. Seventy-nine per cent had elected to pay the ransom, and the average ransom payment was over a million dollars. So if I'm an organised criminal that commits ransomware, I'm loving Australia. What a great target. Guaranteed a million dollars a hit. That has perpetuated the problem we are seeing impact the community at large now. That's why I make those comments, not lightly but deeply, thinking that one way is to remove that business model through creating a disincentive to pay a ransom.

Regarding the perpetuation of the payment of ransom it would behove the committee and others within parliament perhaps to look at our cyber-insurance industry, its role in this and what's covered within existing policies. Some will publicly say they have a policy, with us we'll pay a ransom. That's worthy of consideration now, we're a few years into the notifiable data breach scheme and the role that may be playing in perpetuating the crime that's impacting our community.

More broadly, there's the question of what are other opportunities here in reviewing the Privacy Act. Our bread and butter at IDCARE is providing citizens with a map of how to navigate a very complex response system across all levels of government and industry. We are the only organisation to do that. The adage within our case management team is that if you're not harmed by the crime, you almost certainly will be by the response. A case in point is that, yes, it's been good in a way that Optus has occurred, and that there's been much more focus and light on the response system and its affordances. But as a by-product of all of that work we now have a twin-track response system. If I'm a citizen in Victoria and my Victorian licence has been exposed—through a scam or through somebody stealing a wallet or another data breach—and I want to get a new licence with a new licence version number, I can't. But if I'm an Optus customer impacted by that breach, I can.

There are hooks within the Privacy Act around some of this, not directly to the point of how states deal with licences, but certainly around credit reporting, certainly around credit bands and certainly around what corrections need to take place. Probably absent within that code and legislation is some good solid guidance around how organisations need to behave when it comes to responding to citizens in this situation.

CHAIR: Senator Shoebridge?

Senator SHOEBRIDGE: Thanks for your attendance today and the work you do. There have been some reservations in some of the submissions about the size of the potential penalty. As you know, one of the provisions is that in some circumstances the penalty could be up to 30 per cent of a business's turnover.

To get a sense for the kind of damage caused by these privacy breaches, can you give us any insight into what you've heard from the people you've been dealing with, starting with the Medibank breach? What's been the human impact?

Prof. Lacey: The human impact for most within the Medibank breach is less about the credential exposure and credential risk, for example, those that might have a foreign passport or Medicare information exposed, than about the fact that sensitive, personal information has been accessed by a third party that wasn't authorised, and, in some sad and sinister cases, published online. The human cost is a very emotional, psychological and, in some cases, physiological impact. It is not uncommon for us, even beyond the Medibank breach, to have people come to us and say, 'I was physically sick when I found out this happened. I am no longer sleeping. I don't answer the phone.' It has quite a detrimental impact on people's core being.

The credential side of it, again, the affordance around protecting and responding is going to come down to the type of credential, where it was issued, who issued it, whether you're on a particular breach or not at the moment. Sadly, Senator, they're the things we can actually control. We may not be able to control what the criminal does, but we can control what the response needs to look like.

Senator SHOEBRIDGE: Have you had people who have had multiple breaches in this last 'breach season', if we could describe it as that?

Prof. Lacey: Yes, absolutely. People have received multiple notifications across multiple breaches. And just on that point—I think it's an important point you raise—there is the entertainment of looking at protecting people through arrangements across industry or government in saying, 'We'll protect your ID and we'll do X, Y and Z if you're caught up in these breaches.' At some point every Australian's going to be caught up in a breach. So if we're not thinking about that scenario now, we need to be. We're not just going to protect a cohort that was notified with one breach. Half the country has been notified of a breach in the last two months. That's the volume.

Senator SHOEBRIDGE: Yes. If you haven't had COVID or a privacy beach in the last few years you haven't been living in Australia!

Prof. Lacey: No!

Senator SHOEBRIDGE: Have you had a look at some of the provisions in this bill about information sharing by the Office of the Australian Information Commissioner?

Prof. Lacey: Yes.

Senator SHOEBRIDGE: So, for example, 33B is a general power to disclose information if the commissioner thinks it's in the public interest. Do you think that gets the balance right?

Prof. Lacey: Well, I think there's probably specific arguments as to why that provision's there. As a case in point, in IDCARE's work, if we find online there is a cohort of our community exposed where criminals are trading data, IDCARE will do one of a few things. If we can, we'll tell the person. We'll contact that individual and say, 'We have found your information online, and here are the protection measures we would recommend be put in place and we can assist you with X, Y and Z.' If it's one million people or 500,000 people or 100,000 people—well beyond the capacity of IDCARE, and we may not have their contact details—we will lean on the OAIC to look at ways in which we can innovate and work together to actually notify those people if the entity no longer exists. We've had that case a couple of times in recent years, where a business has folded but we've seen customer data swirl around in channels that can only mean bad things. In those cases it's important that the commissioner has the power to share information, least of which is to share it in a way that also reduces harm to protect people. I understand, at least from that context, why such a provision would be there.

Senator SHOEBRIDGE: But none of the public interest provisions in 33B seem to address that concern, which is there's no other way to communicate to the individuals.

Prof. Lacey: It's a specific case in point, Senator, yes. I'm sure there are other reasons why that provision would be in there, from a practical perspective for the commission to do its work, but the reporting to a commissioner about a breach does nothing to help the individual. It's about other reasons.

Senator SHOEBRIDGE: In terms of helping individuals, the great bulk of the submissions that we've received have said, 'Well, raising the penalty is all well and good. It may have some deterrent effect.' It's broadly supported. But the submissions all say, almost to a person, there's woefully inadequate resourcing for the information commissioner already and it's very unlikely we'll see more than one or two headland prosecutions, and really what government should be looking at is empowering individuals to take some action themselves. That would include through a statutory tort or statutory right of action. In your discussions, in your interface with the thousands and thousands of people you've been dealing with, would that be of benefit?

Prof. Lacey: Well, I'd agree with your summary of the submissions in terms of power. We would articulate support for such an arrangement. Broadly we are supportive of that increased penalty. Whether a tort is the right response to this scenario for people, I'm not sure. When people engage IDCARE they don't necessarily engage us in a way whereby they want to be litigious. They're in a very different mindset. They're in almost a more primal mindset, which is: 'What do I practically need to do here to protect myself? What does it mean for me? What measures exist to ensure that I know whether people are exploiting my information or not?' So, it's probably a different experience we'd have, and the direct question, 'Is there some other legal remedy I can pursue against the organisation that was breached?' We don't tend to see that a lot.

Senator SHOEBRIDGE: You're more in the ringfencing, protective initial-response part of the breach. Is that right?

Prof. Lacey: The analogy is that we are the emergency room in the hospital. People come in at any time, with anything, and they need to be triaged and we need to resolve as quickly as we can what the exposure is and build in some resilience going forward. How the broader system accommodates that going forward is probably beyond our remit. I will say that I think the OAIC is poorly resourced, given its remit.

Senator SHOEBRIDGE: To use the emergency room analogy, once you patch someone up, put on some emergency bandages and stanch the bleeding you pop them out the front door again. Is there anywhere you can refer them to so that they can get some kind of satisfaction, some kind of remedy, some kind of resolution?

Prof. Lacey: Yes, there is. We have a complex case unit within IDCARE such that, if we're seeing 'the response system'—and that might include government—act or behave in a way that's inconsistent with what we know should occur or happen then we will walk in the shoes of those people to assist them longer term. It's an incredible resource of intensive effort to do that. But we've had some good wins. We have a complex case last year that involved a gentleman who'd had repeated misuse and abuse of his New South Wales licence. His case itself really directly helped shape policy in New South Wales around licences. So, there is that aspect of what we do. There are other avenues of recourse for people, one of which is the regulator itself, in terms of complaints or dissatisfaction. But I think what you've reflected in terms of the submissions and the adequacy of the resourcing of the OAIC comparative to other places also needs some attention.

Senator SHOEBRIDGE: I commend you for the work that IDCARE does, but when you're taking on those complex cases, you're pressing government agencies, you're pushing to get some kind of resolution for people who have had maybe repeated breaches, you're basically doing the job of a regulator, aren't you? You're taking that part of the field that a more well-resourced, nimble regulator might otherwise fill.

Prof. Lacey: I'm not sure whether we're taking it. What we're probably doing is giving a regulator, if it was resourced in that way, the best chance to take it further to prosecute or go through a policy or legislative reform or whatever it might be. We don't waste the opportunity that we have engaging with the people who come to IDCARE through case management. We see it as a privileged position. So yes, it's very raw, it's emotional, it's practical, it's tactical—it's all of those things—in talking with the case manager. But we also sit back and say, 'Gee, I'm not sure Australia should be doing this' or 'I'm not sure organisation X should be doing this'.

Senator SHOEBRIDGE: You take the opportunity to try to get a systemic fix where you can.

Prof. Lacey: Of course. It's a responsibility.

Senator SHOEBRIDGE: My final question is about the concept of tiered penalties. We've had submissions from, for example, the Community Council for Australia, which represents a lot of not-for-profits, and they wonder whether they should have the same maximum penalty as a for-profit multinational. We've had concerns raised about the high threshold for serious or repeated offences and whether or not there should be an offence with a lower threshold. Do you have any views about tiered penalties?

Prof. Lacey: Yes, I think it's a useful consideration. The Privacy Act at the moment, as you'd know, excludes organisations with exceptions of those that have revenue of $3 million or under. So, typically a small or micro business wouldn't come into play unless they were a specific type of entity that trade in personal information or health information. Going to the earlier question I think the chair raised around broader reform, if the privacy act was expanded to include, for example, small businesses and microbusinesses, then I couldn't see anything but a tiered model being the right approach. The threshold that we would expect a small business or a microbusiness to have should be lower than what we would expect a multinational or a government agency to have.

CHAIR: Senator Shoebridge, you can ask one more question and then we'll go to the break.

Senator SHOEBRIDGE: There have been some concerns raised about how the structure of the proposed amended section 13G would operate. This is the one that says the penalty for a serious or repeated contravention is the greater of $50 million or three times the value of the benefit that the entity has received from the contravention, or, if you can't determine the quantum of the benefit, up to 30 per cent of the adjusted turnover of the body corporate. One of the concerns that's been raised is that that actually might provide a lower maximum penalty for an entity that was consciously and wilfully breaching privacy in order to obtain a benefit. For example, a corporation with a $1 billion turnover might onsell, or share for commercial benefit, some data and might obtain a $10 million benefit from that. If that's measurable, they're capped, if you like. They don't face the possibility of having a penalty that could be up to 30 per cent of their turnover, because you can identify the benefit.

Prof. Lacey: That's right.

Senator SHOEBRIDGE: Whereas if an entity has been reckless or negligent, and had someone rummage through and steal their data, they may actually face a significantly higher penalty because there's no identifiable benefit, and they may cop the 30 per cent turnover. In some ways it's a perverse arrangement—

Prof. Lacey: It is.

Senator SHOEBRIDGE: that might help the nastiest players get a lower fine.

Prof. Lacey: Yes. I think that's an important consideration when you're looking at the mechanics of how this would operate in practice and how it could be not abused but certainly used in a way to achieve the outcome, ultimately, that you're after. The outcome that you're after is to provide enough incentive for organisations to really think about how they're protecting people's data, whether they should collect it in the first place, how long they keep it for and the adequacy of their response. That's ultimately the outcome you're after, and I think you've highlighted the point there where in practice you may get a perverse outcome.

Senator SHOEBRIDGE: In fact, you may have defence counsel desperately trying to find some kind of benefit that the corporation got from the data breach in order to minimise the fine.

Prof. Lacey: Yes. Correct.

Senator SHOEBRIDGE: That would be perverse.

Prof. Lacey: I would agree. Yes.

CHAIR: Thank you very much, Professor Lacey. We appreciate your time. The committee will now suspend for morning tea.

Proceedings suspended from 10:58 to 11:11

BAILES, Ms Rachel, Head of Policy, Australian Information Industry Association [by video link]

BLACK, Ms Wendy, Head of Policy, Business Council of Australia, [by video link]

LOUIE, Mr Chris, Director, Digital, Cyber and Future Industries, Business Council of Australia [by video link]

POUNDER, Ms Kate, Chief Executive Officer, Tech Council of Australia [by video link]

CHAIR: Welcome. Thank you for taking the time to speak with the committee today. Information on parliamentary privilege and the protection of witnesses and evidence has been provided to you and is available from the secretariat. Would any of you like to make a brief opening statement before we go to questions?

Ms Black: Thank you for the opportunity to be able to give evidence to the committee on this bill. It is important to acknowledge that the BCA recognises that protecting the privacy of people's information is extremely important. Our members are very aware of this and accept the need for a stronger response, from both business and government, as we continue to face increased cybersecurity threats. For this reason, we agree with the intention of the bill, to provide Australians with confidence their data is being protected. Businesses do take this obligation very seriously, and we are concerned by the recent incidents, particularly where personal health data is stolen, and where other identity information is taken and by the risks that poses for people. We've also learned from these high-profile cases that there are broader issues that also need to be addressed beyond the amendments being proposed in this bill.

As we have highlighted in our submission, there needs to be improved coordination and cooperation between government, the range of agencies and business so that criminals can be caught quickly, the potential risks can be limited and customers have clarity about what they also need to do to protect themselves. In this regard, we understand why the bill proposes changes to the provisions affecting information-sharing. In that regard, we suggest that there should be a slight change to ensure that the reforms do not have the unintended consequence of more information being shared and put at risk. We understand why the government has decided to increase penalties, and further guidance on their application would be welcomed. Guidance about how these penalties will be applied needs to recognise where businesses have done their best to prevent these terrible crimes.

The bill also needs to recognise that businesses are going to be the victims of crime. As the Australian Cyber Security Centre has recognised, all organisations are facing an increasingly challenging environment. It should also be noted that the changes being proposed will apply to all parts of the Privacy Act, not just in responding to cyberattacks. So it needs to have the balance right in providing protections while enabling the development, adoption and use of new technologies powered by data. The importance of doing this has been recognised and encouraged by government. To this end, we support the overall modernisation of the Privacy Act and look forward to government undertaking significant consultation following the release of the review by the end of the year.

We also need to recognise that while businesses hold this data, in many cases it's not because they want to but because the government requires them to. This is why we've asked that a review be undertaken of the various data retention regimes put in place.

Finally, it's important we all recognise that protecting the privacy of Australians will require a team effort. All organisations need to be able to work in partnership with government. We also need to have the capabilities to lift security and privacy in Australia. Key to this will be filling critical cybersecurity skills shortages in Australia and simplifying the reporting regimes.

Thank you, and we are prepared to answer any further questions from the committee.

Ms Pounder: Thank you to the committee for inviting the Tech Council of Australia to appear at today's hearing. Recent high-profile cyberattacks have impacted millions of Australians. We sympathise deeply with the distress they've experienced, and we're committed to doing all we can to make Australia more cybersecure.

These attacks show Australia is becoming increasingly targeted by malicious actors. It's an escalating threat in our complex geopolitical environment. It makes it more important than ever for government and industry to work together to improve cybersecurity and privacy in Australia's national interest. We therefore support the government taking a comprehensive response to this instance, including modernising privacy laws so they are fit for the digital age.

We are not opposed to increased penalties or information gathering powers per se. However, we think this bill and the other measures the government is putting in place to help with Australia's cybersecurity response need to deliver the desired outcomes we're collectively seeking: firstly, to genuine protect privacy and to make Australia

more cyber-resilient; secondly, to incentivise effective disclosure, coordination and communication, particularly following a cyberattack; thirdly, to harmonise laws and make sure they still make sense and clearly state to industry what's expected of them if they comply; and, finally, to enable digital and cyber capabilities in our citizens and businesses so these heinous attacks don't stop us engaging with each other and the world. They are the key outcomes we believe this bill should be examined against.

We've made several recommendations in our submission to ensure the bill achieves these goals. These amendments include a safe harbour regime and a commitment to define serious and repeated breaches, and to explain the reasonable steps an organisation should take to avoid them. They're aimed at preventing breaches, encouraging a positive culture of disclosure, ensuring effective responses when they occur and providing organisations with greater clarity.

These amendments matter because the rules and penalties in the bill will apply to businesses and workers across the economy. It's easy to imagine that that means a big business. Reporting by the Information Commissioner's own office shows that health services organisations, hospitals, GP surgeries and aged-care homes are consistently the industries with the highest number of data breaches. They're most likely to cause a breach by human error as opposed to a malicious attack. When we review this bill, we need to imagine what these amendments will mean for our local hospitals and the amazing doctors, nurses and paramedics working in them; they are often the typical organisation and typical worker at the centre of one of these breaches. We have recommended a tiered penalties model and better guidance on reasonable steps.

I want to briefly note that the Information Commissioner's reporting shows that 62 per cent of data breaches are caused by malicious attacks. This means that in those really crucial early days, as an operational situation is unfolding, a cyber incident may be simultaneously overseen by police and security agencies as well as civilian agencies such as the OAIC. In these cases we think it's particularly vital that the disclosure and information sharing models are harmonised to ensure quick disclosure, enable an effective operation response and avoid compromising a response to a cyberattack.

Finally, I note we need to do multiple things to make Australia more safe, including reviewing our data retention laws and improving our skills shortages in tech and cyber workers. And we absolutely understand the desire and we share the desire of all Australians to see action on cybersecurity, but we believe it's our collective responsibility to ensure that any action we take genuinely makes us safer and genuinely makes us a more empowered community.

CHAIR: Thank you very much. Ms Bailes, do you have an opening statement?

Ms Bailes: Yes, I do. The AIIA is grateful for the opportunity to appear today. It is appropriate that this bill be subject to community consideration, so the AIIA thanks senators present for their keen attention to these matters. Australians have been gravely and rightly concerned by recent high-profile data breaches. Uplifting cybersecurity across the Australian economy is an urgent task, one in which the technology sector wants to partner with government. Telstra chair John Mullen on 25 October said of penalties:

I don't disagree with fines if people have been negligent, but you don't want an adversarial situation where people are reluctant to divulge everything that's going on with them.

You want people to come out and work together with government and industry to try and defeat this thing altogether.

While the explanatory memorandum refers to 'large multinational organisations', all kinds of organisations, including health service providers and relatively small businesses, have responsibility under the Privacy Act and may be subject to its penalties.

The AIIA does support the government's intention in this bill to strengthen our privacy regime. However, we do hold some concerns: first, regarding the haste with which this bill is being passed through parliament and the standalone approach to it in the context of a review of the Privacy Act, which is already afoot; second, regarding the unprecedented increase in penalties, which could have unintended consequences or, indeed, prove terminal for some businesses and the questionable substantiation of the quantum of increase. The AIIA accepts that courts must take all relevant matters into account in determining civil penalties under part 4 of the regulatory powers act. However, we believe that there should be recourse to be granted safe harbour and relief from penalties in the case of prompt help-seeking behaviours and information sharing, good-faith behaviours, the taking of articulated and delineated reasonable steps, or the application of appropriate cybersecurity framework. The bill should explicitly require that these factors be taken into account when determining whether to apply for or make a civil penalty order. This could constitute a safe harbour provision.

In responding to concerning data breaches, we encourage government to ensure due consideration and coordination of legislation with a constructive and collaborative focus on uplifting cybersecurity and cyberresilience across the economy.

CHAIR: Thank you very much. Senator Scarr, I hand the call to you to kick us off.

Senator SCARR: I'm not sure if our witnesses have been listening to the earlier testimony, but an issue that has arisen and we're asking questions in relation to is the appropriateness of this penalty regime in circumstances where a company or an organisation is the subject of malicious activity by a third party as opposed to, say, engaging in conduct consciously itself to obtain some sort of commercial benefit. The concern that I have is that the two positions, at least in terms of the drafting—and I'll ask a question about how the courts might apply it—seem to be equated or given some sort of equality in relation to the penalty regime. I'm interested in your comments in relation to that issue.

Ms Bailes: I note that the penalties mirror the ACL penalties that were recently increased by this government, but the AIIA believes it's not always a neat analogy. You've got positive action, anticompetitive action, but it doesn't marry across necessarily to being the subject of a large-scale data breach often by sophisticated actors. Indeed, there is the provision in the Australian Privacy Principles that is about reasonable steps. But we believe that, if the government is going to take the approach of mirroring those extremely significant penalties then, as a corollary, embedded in the legislation there needs to be that safe harbour so that courts and so that the commissioner can see in a delineated way what those reasonable steps could be. That can help to provide some context in applying that judicial discretion and, indeed, the discretion of the Information Commissioner.

Senator SCARR: Ms Black?

Ms Black: This certainly is an issue that we have raised in our submission, that there needs to be some sort of guidance provided as to how these penalties would be imposed. We've suggested possibly a tiering of penalties, so then you could also see what actions in business had taken and the court could have a look at what would be relevant. Also, the size of the company, considering this will impact businesses that are smaller through to the larger, and at the larger end, for the companies we represent, it could be quite significant.

Another area that also needs to be thought through is that these penalties are not just being imposed for cyberattacks. As I mentioned in the opening statement, these changes apply across the broad Privacy Act. We're expecting further significant changes to the Privacy Act post the review that's under way at the moment, and that will happen next year. When that occurs, there may have to be a further review as to how they'll be applied, but in this instance, if there could at least be some guidance provided—a possible tiering with the GDP arm—that would be of assistance, and something our members are certainly looking for with regard to this bill.

Senator SCARR: Ms Pounder, do you understand the point I'm making? It's one thing for a company to monetise private information to obtain a commercial benefit—then, I can see how the proposed penalties regime works effectively—but it's another thing entirely for a company to be the victim of a cyberattack. It doesn't obtain any benefit—in in fact, to the contrary, it leads to a whole range of costs, both financial and reputational.

Ms Pounder: Absolutely. I think the nub of your question is that, should you equate those two acts and deem them equally as liable for a breach under the act, should each receive the same level of penalty?

Senator SCARR: Correct.

Ms Pounder: Our view is quite likely no. When determining the penalties, the questions are: has there been a breach of the act; what is the nature of that breach—is it serious, is it repeated; and did the company take reasonable steps to prevent it? We can see that, where a company has intentionally tried to do the wrong thing, all of those answers may readily flow from each other, but in the case of a malicious hack we have to ask those questions very carefully. Firstly, a company can be the victim of a malicious cyberattack, and we know from the information that the commission is reporting that about two-thirds of the mandatory data breaches they receive are the result of a malicious hack. The company may not have actually breached the Privacy Act when that attack has occurred, firstly because cyber incidents don't necessarily result in a data breach and secondly because the data breach itself may not have been a breach of the Privacy Act. It's important not to lose sight of that distinction.

Secondly, when we think about the sophistication of some of the state-based actors or significant criminal syndicates, there can be some very sophisticated types of cyberattacks where a company may well have taken a number of reasonable steps, such as having the right, being legally required to hold the data in the first place or maintaining it securely. They may have very sophisticated systems, security and penetrating testing, or internal cybersecurity teams that are constantly monitoring for either errors or attacks. They may have trained all their staff. They may have detected an incident very quickly and instantly notified authorities and started cooperating with them—yet still they may have had a terrible attack. When we question whether there has been a breach of

the act—how serious it was, if it was repeated, and whether they took reasonable steps—all of those factors are very material. They should, therefore, also be material to the question of the right penalty.

Senator SCARR: Do you believe that those issues are of such importance that there should at the very least be some actual guidance provided in the legislation itself with respect to the tiering and the application of penalties, as opposed to just leaving it to the courts to sort it out?

Ms Pounder: I do. The reason for that is we should all have a shared incentive to not want these breaches to occur. If the act, firstly, defines what is a serious and repeated breach and, secondly, follows the model of DDPR—which has 11 principles in regulations that guide administrators as to how they should design and apply the penalty regimes, and what factors are relevant to those tests as to whether the company took reasonable steps—that helps everyone understand their obligations. There's a capability-building component to that, there's an awareness-raising component, and it also means that, legally, when a regulator has to review it, it's much more straightforward for the courts to determine it—we're not just determining it all through case law. Both from the perspective of building capability and improving cyber-resilience and from the perspective of legal certainty—and I note the Law Council has similarly said that this would be useful for these reasons—there is great value in putting that guidance in the bill and also then building on that through things like enforcement guidelines.

Senator SCARR: This is my final question. I just want to put this proposition to you because it was raised by previous witnesses. In relation to the concept of introducing safe harbour provisions, the concern has been raised that this could actually have the perverse effect and mean that companies are less proactive in terms of dealing with these risks because they have the benefit of that safe harbour, so the safe harbour becomes a comfortable hammock where companies are incentivised not to take the action they should take. I want to give each of you an opportunity to respond to that argument.

Ms Bailes: A properly drafted safe harbour regime wouldn't act as a hammock or a get-out-of-jail-free card. Rather it's the other side; it's the carrot, the incentive, for organisations to take a good hard look at how their staff, organisational levels and boards are functioning and to leverage fantastic tools, such as the Essential Eight and other cybersecurity frameworks. Rather than that safe harbour being an opportunity to sit back, it's an opportunity to lean forward and have a look at the legislation. Rather than just going, 'We better make sure we never fall victim to a data breach,' it's about being resilient and cybersecure by putting practical steps in place so that you can satisfy that safe harbour. This could have a fantastic incentivising effect across the board through health service organisations and community based organisations, as well as the large multinationals that we see in the explanatory memorandum.

Ms Black: You're right; there are a range of views on this. From our membership there are some diverse views on this. With the safe harbour what are we trying to achieve? Are we trying to create a culture within which a company is going to share information and react quickly if there is a breach so that the negative impact on their customers is minimised and the situation is rectified as quickly as possible? That is what we are trying to achieve. Therefore, if a safe harbour were created, you'd want to make sure that it would enable that to occur but also not have the perverse outcome you have raised.

I think that also flows back into your other point around the penalties and why we are arguing for some guidance on that. Concerns have been raised by some of our members that the penalties are so significant—and I'm not saying there shouldn't be some increase from where they were—that they may create a culture by which companies will be less inclined to react quickly and share information. That's a concern. That's why we're asking for guidance around this.

Those who have been taking steps and putting in practices and processes to minimise potential risks are not going to stop cyberattacks altogether. We know that. But, if they've taken the right steps, at least they can feel confident that they can respond quickly, tell other authorities, tell the government, tell the agencies and minimise the impact. That's what we are really trying to achieve out of all of this.

Ms Pounder: I think there's a strong case for at a minimum a safe harbour scheme when an organisation is reporting a cyber incident and they are reporting that to both security agencies and intelligence agencies, such as the Australian Cyber Security Centre, the ASD and police, and another civilian regulator. I note that Rachel Noble, the head of ASD, when asked about this by the Senate, recently said that, from an ASD perspective, she thought that would be 'a most excellent idea'. She said that's because when you're in those early throes of an operation and you are still trying to pull the people out of the sea and into the lifeboat you need full disclosure and full cooperation. You have security agencies going into a business checking its defences and trying to undertake forensic analysis to understand what has happened and the nature of the incident. Is it a terrorist attack? Is it a ransomware attack? Has there been a data breach? In that period of time, it is so essential that the business is fully compliant with those agencies and following their advice to the letter. That might include, by the way, doing

things that would be at odds, in some cases, with some of the requirements of the Information Commissioner, which might be to not be publishing information, to not be disclosing things, because it could be quite sensitive and material to the incident management and investigation—for example, if they're trying to substantiate who the perpetrator was and they need to retain some details in private in order to be able to validate any threats that have been made or data that has been published.

My view is that, as we all stand back and review what has happened, it would be healthy to review that national disclosure and coordination and communication model. In the event of a cyberattack, I support the BCA's proposal to have a single controller, and I think it should ideally be an operational one. They can then determine the best way to manage it. I think a safe harbour that enables that cooperation is important and would need, at a minimum, to be reflected through the Privacy Act and the Information Commissioner's role, just because we know that 63 per cent of the incidents being reported under mandatory breach schemes are a result of malicious attacks, so there is a real possibility that the same cyberincident is also then subject to the mandatory data breach laws. I think we want a harmonised approach across them.

Senator SHOEBRIDGE: Thanks, everybody, for your attendance and for your submissions. I want to go back to the way in which the proposed new penalty regime operates. It sets a maximum penalty that is the greater of $50 million or three times the benefit the corporation obtained, either directly or indirectly, from the breach, or, if the court can't determine the benefit, up to 30 per cent of the adjusted annual turnover. That's the regime. Arguably that provides for a corporation that may have a large turnover but deliberately, maliciously and wilfully breached privacy provisions in order to obtain a benefit actually facing a significantly lower penalty than a corporation with the same large turnover that was the subject of a malicious attack and was negligent in its defences. If the benefit that a corporation obtained was $5 million or $10 million, but their annual adjusted turnover is $1 billion or more, it may end up with this perverse outcome where the worst players get the lesser penalty. Have you looked at that? I might go to you first, Ms Pounder.

Ms Pounder: We have looked at it. Can I firstly say we have proposed a tiered approach to penalties which is more specific about the types of breaches or behaviour that would be associated with that penalty level. That's the model of the GDPR. It's partly for that reason—firstly, you can delineate through that tiering the behaviour that's most serious. I do think that would be a perverse outcome if it were the case, particularly if it were demonstrable that the behaviour that might trigger a lower fine was actually one where there had been a serious and repeated breach and it was clear the company hadn't taken reasonable steps. I think every Australian would expect that, in those circumstances, they would be the category of firm facing the highest penalty. So I think that is a reasonable question to ask.

Senator SHOEBRIDGE: In this case, if a multinational company with a billion-dollar turnover deliberately, consciously, in breach of privacy principles, sells data for $10 million to a third party, and that breach is found out, they will have a maximum penalty which is capped at $50 million. But they may have a competitor who were maliciously attacked and had the same amount of data stolen, and their competitor might face a penalty of up to $300 million. That doesn't seem to be good lawmaking.

Ms Pounder: No. I'll be brief so that the others may respond as well. I think the challenge is we've borrowed a penalty system from a law that was regulating quite different behaviour and activity, and so penalties that may have made sense in the context of one law may not make as much sense in the context of another that's regulating quite a heterogeneous set of behaviours in quite different companies. I do think it's worth asking: have we designed the right penalty scheme for this bill, this law?

Senator SHOEBRIDGE: If you've got entities engaged in collusive tendering or in anticompetitive behaviour, this kind of structure may make sense. But to just cut and paste it into the Privacy Act creates those kinds of perverse outcomes, doesn't it, Ms Bailes?

Ms Bailes: Yes, and I think what we're seeing here in the drafting is unfortunately a by-product of the haste with which these amendments were introduced, because it has such strong reference to other regimes for different kinds of conduct. I think we may also be seeing that in repealing the existing paragraph section 5B(3)(c) regarding the extraterritoriality. It's been suggested in submissions that it may not have been the intention of those drafting to mean that companies overseas, regarding their activities with foreign citizens, would possibly be caught up in Australian privacy law. There's also this issue where, because being able to calculate three times the benefit derived would act functionally as a cap, it would then not engage the third element, which is the turnover. I would find it hard to believe that it was the intention that that would then incentivise being able to show, 'Well, actually we really did derive benefit here,' in a court, for example. But, because this has been introduced quite hastily, it's being picked up now. That's our view.

Senator SHOEBRIDGE: With this current drafting, if a corporation had been the subject of an attack, and they had a large turnover, the corporation may be desperately trying to prove that they obtained some kind of benefit from it to avoid facing the maximum penalty of 30 per cent of turnover. That's how it would work in practice, isn't it?

Ms Bailes: Yes, functionally, and I find it hard to believe that that would have been the intention.

Senator SHOEBRIDGE: Ms Black, from your organisation's point of view, I assume you'd want a penalty regime that provides a higher, not a lesser, penalty for deliberate, malicious actions seeking to benefit a corporation than reckless or negligent actions that caused harm. I assume that's the kind of penalty regime you would like.

Ms Black: Yes, that would be the principle you would normally operate under and would be seeking. I would endorse the comments made by Ms Pounder and Ms Bailes here as well. That goes back to the key recommendation I think we've all put forward, which is seeking greater clarity around these penalties. As I've already mentioned, this is being put in the context of the entire Privacy Act, not just cybersecurity. But that's what it's being used for at the moment, and everyone is seeing it through that lens, but it does have broader ramifications. And, as you've rightly highlighted, it could end up with a perverse outcome. That is why, if we got some guidance around it and some tiering of penalties, it could be therefore clearer that, at least in those incidents where people have not been doing the right thing, they would be at the top end of the scale and others not. I think you raise a very valid point.

Senator SHOEBRIDGE: Ms Pounder, you raise in your submission on behalf of the Tech Council concerns about the resourcing of the OAIC. We had evidence earlier today from the Information Commissioner that the cost of doing the investigation and the work in relation to just one breach, the Optus breach, is likely to be in the order of $5½ million dollars, which they've obtained funding for, but their entire office's budget is in the order of $33 million. We could pass these laws and pretend that that's going to fix things, but, if there's a sole regulator with that level of resourcing, it's not really going to have the capacity to actively use these offences, is it?

Ms Pounder: My view on this is that we should take these recent attacks as a moment to sit back and make sure we have the best possible national model in place in the event of a cyberattack, because we should just expect that we will receive more of them, and they will become more severe and they will become more sophisticated. Based on that, I think we've seen with these recent attacks that we didn't have that model in place. I think the elements of that model would be early identification of the incident; early disclosure of it; full collaborative, cooperative models between the impacted organisations and relevant authorities; and noting that, in this case, the Information Commissioner will not be even the primary regulator or authority, particularly if you have security agencies, police and intelligence agencies involved. As we've seen in these attacks, there are many other regulators that might become involved, whether they are financial regulators, the ACMA, state agencies et cetera. I think putting that in place first, designing that really effective model for the coordination, for the communication back to affected people to help them get support, is vital. My view would be that the better model would be to design that end to end first, from what we've all learned, and then to think about different use cases that might test it, remembering that some of those will not involve the Information Commissioner, because a cyber incident may not involve a data breach, but some will. Then we would ask, based on that: how would we resource all these regulators so that all of them could play their right and appropriate role? I think that is a very necessary piece of work.

Senator SHOEBRIDGE: Your recommendation 7 is:

The Government should increase resourcing for the OAIC commensurate to the increased powers and the increased risk of data breaches across the economy.

Ms Pounder: Yes.

Senator SHOEBRIDGE: That's a necessary element to that national response—is that right?

Ms Pounder: I absolutely think that there will be a role for the Information Commissioner, noting, again, that not all breaches are cyber incidents as well. But I think, particularly for those that are cyber incidents, we can't consider the resourcing and the role of the OAIC in isolation from some of those other [inaudible].

Senator SHOEBRIDGE: Ms Bailes, does your organisation have a view about the adequacy of the funding to the Information Commissioner?

Ms Bailes: Absolutely. If the resourcing on the Optus breach has been, I think, in the order of $5 million, then it stands to reason that responding in these heightened ways to similar breaches may become unmanageable. But I think what's really important here, like Ms Pounder said, is that there's a cohesive approach by government. I know we've endorsed the concept of a council of tech regulators to address these broader issues of plurality of

regimes and reporting requirements, and parallel inquiries and consultations on foot at any one time, with related implications. It might include the Office of the Australian Information Commissioner, the eSafety Commissioner, ACMA, the ACCC and the ACSC. If that group can get together and work out how best to strategically approach these very serious cybersecurity incidents, then issues like the funding that each relevant body will require and the role that they each need to play in simplifying, for industry, the way we effectively respond to these incidents, I think, could be a really important recommendation here.

Senator SHOEBRIDGE: It's getting that balance right across the different regulators. The Signals Directorate has the better part of $10 billion, and the Information Commissioner gets $5 million. Perhaps considering the appropriate resourcing across the various regulators and enforcement agencies is urgent work. Would you say so, Ms Bailes?

Ms Bailes: Yes. It's definitely a consideration. Absolutely.

CHAIR: Thank you, Senator Shoebridge. I want to finish up and thank you all for your contributions, particularly around where things might need to be clarified in the legislation. I want to ask whether any of your organisations have a position on the proposed extraterritoriality provision in the bill, and where you might see the need for that to be clarified in any way.

Ms Bailes: I'm happy to speak to that.

CHAIR: Yes. Thank you.

Ms Bailes: I know that repealing the existing paragraph 5B(3)(c) is intended to ensure that businesses operating in Australia are still captured by the Privacy Act without needing that very strong thought of, 'Well, we thought the source of the information was in Australia.' I think that's the intention behind repealing that paragraph, but it may have an unnecessary effect of capturing all the privacy practices of businesses operating in Australia, whether they affect Australian citizens or activities involving foreign citizens, which I don't believe was the intention in drafting. It's also worth considering that extraterritoriality is a very seminal matter in the Facebook case that's still afoot. The Information Commissioner has brought those proceedings. Written submissions have not yet been made in that case. So while that's afoot, and while we've also got the review of the Privacy Act afoot, I believe that significant changes to the territoriality of the Privacy Act need to be considered in a cohesive manner through that review. The drafting needs to be looked at here: if the government decides to proceed with repealing that paragraph, it needs to look at whether there does need to be some wording added into that section regarding Australian citizens and the connection there, so some sort of Australian link.

CHAIR: Okay. Thank you. Tech Council or BCA?

Ms Pounder: We agree with Rachel's very eloquent answer and explanation. We would just note that we think it would make more sense, at a minimum, to clarify that the personal information collected or held should relate to an individual located in Australia, or something to that effect.

Ms Black: Chris can respond to that, but it is something that we have indeed raised that we have a concern about. Chris, do you want to make a further comment?

Mr Louie: Yes, thank you—and thank you, Chair. I definitely agree with the points that our wonderful colleagues have made on this. There's been an unintended consequence in the way this has been drafted, which, unfortunately, is going to mean that this will push the Australian Privacy Act out globally into the operations of entirely unrelated matters where it really wouldn't make sense to do that.

I do think it would be worthwhile, as both Ms Pounder and Ms Bailes have mentioned, looking at whether this could be amended or potentially—given the kinds of implications this would have, and the way the Privacy Act works—whether or not this should actually be considered as part of the broader Privacy Act review rather than being pushed through in this kind of haste. I would suggest that probably the recent incidents that have provoked this bill didn't really have that international dimension that would require this kind of response. It does feel that there isn't a burning policy problem that this needs to address right now. It's probably better to consider this in a very sober manner because of the implications it will have across the entire act.

CHAIR: Thank you so much. That is all the time that we have today. I want to thank you for attending and for giving your evidence.

BRAYSHAW, Ms Elizabeth, Acting First Assistant Secretary, Integrity Frameworks Division, Attorney-General's Department

GALLUCCIO, Ms Julia, Assistant Secretary, Information Law Branch, Attorney-General's Department

HENNESSY, Ms Isobel, Senior Legal Officer, Information Law Unit, Attorney-General's Department

NGUYEN, Mr Daniel, Acting Director, Information Law Unit, Attorney-General's Department

RAINSFORD, Ms Cathy, General Manager, Content and Consumer Division, Australian Communications and Media Authority

[11:52]

CHAIR: I now welcome representatives from the Attorney-General's Department and the Australian Communications and Media Authority. Thank you for taking the time to speak with the committee today. Information on parliamentary privilege and the protection of witnesses and evidence has been provided to you and is available from the secretariat.

I remind senators and witnesses that the Senate has resolved that an officer of a department of the Commonwealth or of a state shall not be asked to give opinions on matters of policy, and shall be given reasonable opportunity to refer questions asked of the officer to superior officers or to a minister. The resolution prohibits only questions asking for opinions on matters of policy, and does not preclude questions asking for explanations of policies or factual questions about when and how policies were adopted.

I'll go to the department first. Would you like to make a brief opening statement before we go to questions?

Ms Brayshaw: I might just make a couple of remarks if that's okay.

CHAIR: Of course. I know we've got lots of questions for you, so thank you very much for assisting the committee.

Ms Brayshaw: Thank you very much for the invitation to come today to assist the committee's process. The bill includes amendments to increase penalties under the Privacy Act, provide the Office of the Australian Information Commissioner with greater enforcement powers and provide the commissioner and the Australian Communications and Media Authority with greater information-sharing powers. The bill is being introduced now to address the more pressing issues arising from recent serious data breaches and cyberincidents which have the potential to cause serious financial and emotional harm to Australians. The bill is intended to promote the need for robust privacy, security and data protection. I'd also like to note that the bill is a first step in the government's agenda to ensure Australia's privacy framework is fit for purpose and responds to new challenges in the digital era.

As you have heard from other witnesses today, the department's review of the Privacy Act is underway, and it will be reporting to the Attorney-General by the end of this year. This review will recommend further reforms to ensure Australia's privacy framework protects the personal information of Australians, supports an innovative economy and responds to the new challenges in the digital age. Broader proposals, including measures to address the amount of personal information that entities are collecting and how they are storing it, are issues that have been raised and considered through this review process, and it's appropriate that these reforms be considered holistically in that process, given the range of complex and interconnected issues and other work across government.

We welcome questions from the committee.

CHAIR: Thank you. ACMA, do you have an opening statement?

Ms Rainsford: No, thank you.

CHAIR: Thank you so much. I've got a couple of questions. Obviously this legislation has come about in the face of recent data breaches which are of significant concern to the community, and you've outlined some of the measures that are in the bill to deal with those concerns. I want to go to the recommendations that the ACCC made that there be an increase in Privacy Act penalties to mirror the increased penalties for breaches of the Australian Consumer Law. When did the ACCC report make this recommendation, and what was the ACCC's reasoning behind its recommendations, if you can comment on that?

Ms Brayshaw: The recommendations related to the 2019 report on the Digital Platforms Inquiry, and as part of that inquiry it highlighted the close links between competition, consumer and privacy laws, and that there was a need to avoid a siloed approach to how we address those. The ACCC's report recommended that the privacy civil penalties should mirror the Australian Consumer Law, and I can give a little bit more detail on the basis for that

recommendation. The report noted that effective deterrence under the Privacy Act relies on regulatory oversight accompanied by meaningful sanctions for any conduct interfering with an individual's privacy. Given the size of some of the entities collecting, using and disclosing personal information in the digital economy, which does include digital platforms operating in Australia, the ACCC recommended that the maximum penalties for breaches of the Privacy Act should be increased to mirror the recently increased penalties for breaches of the Australian Consumer Law. And I do note that that was in 2019 and that, since then, the penalties in the Australian Consumer Law have increased.

CHAIR: I want to go to the penalties themselves. They're in the bill, there's a big number there, but I want to get an idea of context, particularly globally. How do the penalties in this bill compare with penalties for privacy breaches in other, comparable jurisdictions, particularly those that these larger company are practising in—for example, in the UK or the EU?

Ms Brayshaw: I might get Ms Galluccio to speak to this.

Ms Galluccio: The maximum penalty under the GDPR, the General Data Protection Regulation, in the EU has actually resulted in some very high penalties, where they can be calculated in terms of four per cent of the global turnover. For example, in 2021 Amazon was fined $746 million by the Luxembourg National Data Protection Commission for breaching the GDPR requirement to have a lawful basis for collecting and processing personal data. The penalties that we have in our bill would really only apply to the most egregious breaches by a company.

CHAIR: There has been some discussion this morning about the appropriateness of the penalties, and I wanted to give you a chance to respond. It still provides for a court to have discretion in relation to what is appropriate in particular circumstances. How have you been able to articulate that in the bill, or what is the thinking behind that?

Ms Brayshaw: The focus of this bill, which is quite targeted in terms of the reforms it's taking, is to seek to amend the existing section 13G of the Privacy Act. The way in which it seeks to do that is just to affect the quantum. It's not affecting the existing obligations under the act, nor is it affecting the way in which, in cases of serious or repeated breaches where the commissioner is of the view that civil penalties are warranted, she would go to the court to seek those, and it would be a matter for the court to determine, in the circumstances of that case, what would be appropriate.

CHAIR: We've had some witnesses today—and submissions—who proposed a tiered approach to penalties. Is that something the department considered or is considering as part of the Privacy Act review?

Ms Galluccio: That is something that we are considering more broadly as part of the Privacy Act review. We're looking at a range of issues across the Privacy Act review. There is one category of issues I would describe as just generally the enforcement of the Privacy Act. As the Information Commissioner outlined earlier this morning, she has a range of regulatory action that she can take. Its quite a spectrum, so at the very low end she can provide guidance and education; if there's a complaint she can attempt to conciliate; for more serious issues she may decide to make a determination; for a serious or repeated breach of privacy she can pursue a civil penalty.

The feedback that we've had through the review to date is that perhaps there's not enough of a spectrum in terms of being able to address the different types of seriousness of privacy breaches that can occur and, in particular, that there's not much in between a determination that the commissioner can make and when there's a very serious or repeated breach of privacy. One of the ideas that we are considering through the review is whether there should be a mid-tier penalty that could apply for any breach of the Privacy Act.

CHAIR: Is that not covered by this bill?

Ms Galluccio: No.

CHAIR: What is a serious or repeated data breach? I just wonder if you could take us there. Some of our witnesses or submitters have raised a few concerns about the clarity of that term. Is there some value in the OAIC providing further guidance on what is considered a serious or repeated breach under the Privacy Act review?

Ms Galluccio: The OAIC already does provide guidance on what a serious or repeated breach is. It includes a set of factors that they consider relevant when determining whether the breach is serious or repeated. Some of those factors include the number of individuals who are potentially affected, whether it involved deliberate or reckless conduct, whether senior or experienced personnel were responsible for the conduct and whether it involved sensitive information or other information of a sensitive nature. They're just some of the factors that the OAIC have listed in their guidance about what would amount to a serious breach under the Privacy Act.

CHAIR: Are you speaking to them about updating that guidance if this bill is passed, just to make it really clear for companies what their obligations are?

Ms Galluccio: That's right. Another one of the issues that we are considering as part of the Privacy Act review is whether the provision could be made clearer. One of those options might be through guidance. Another idea might be to take the guidance which the OAIC has done and specify those factors in the provision itself. They're all options that we're currently considering.

Ms Brayshaw: Noting that this is the first step in the government's agenda and taking initial targeted reforms, on your question as to considering further guidance that complements the bill if it's passed by parliament, I think that is something that would be of value. I certainly know that in discussions with the regulator about the different components of the bill they would see that it would be appropriate to update their privacy regulatory action to give further information as part of that, noting that we're also looking at this in the longer-term piece in the broader conversation out of the Privacy Act review. That's something else we'll continue to consider.

CHAIR: I've got a couple more topics to cover, then I will hand over the call. We've got a bit of time, Senator Shoebridge. In regard to the extraterritorial provision, some submissions to the inquiry have noted that the proposed provision is too broad or would capture businesses with no links at all to Australia. Can you explain the approach taken to that provision—the way that it's drafted? I know it's a very technical area of law, so I would like to understand the thinking behind the way it is drafted, and whether there is any further guidance that can be provided.

Ms Brayshaw: I think it was helpful to listen to the commissioner this morning in terms of her explanation around the purpose and intent, in terms of assisting the regulator in knowing when there is jurisdiction and how that works. In terms of the way the bill amends the provision, and the intent of it, currently there is a requirement to demonstrate that a foreign organisation is carrying on a business in Australia and, secondly, collects or holds personal information. The intent of this amendment is to remove that second requirement in relation to the condition to collect or hold personal information. The nexus that comes from carrying on a business provides a useful nexus for the purposes of this provision.

Secondly, it reflects the fact that we need to update our privacy laws to make sure they're fit for purpose. I note some of the earlier witnesses talked about this. Not all information is stored in Australia, and 'platforms' mean that the idea of having that limb is perhaps not as useful now. Certainly, the regulator's view is that we simplify the requirements of this provision so that it's clear as to what's possible.

So that's the approach that we've taken. The focus, if that second limb is removed, is that the nexus in that circumstance would be to demonstrate that the foreign organisation is carrying on a business in Australia. That mirrors the approach taken to foreign organisations in relation to competition and consumer law in Australia, and we know that, while it is framed slightly differently, the New Zealand Privacy Act has a similar way of dealing with that type of extraterritorial provision.

CHAIR: Thank you. One other thing I want to cover off is the question about small businesses. What privacy obligations are there on small businesses to protect personal information of Australians in cases where they may hold personal information? The breaches that we've seen play out publicly recently have obviously been in very large companies, and we're talking here about breaches and penalties of that scale. I don't want small businesses get spooked by some of the things we're talking about. Could you clarify that, because there have been some questions about that today?

Ms Galluccio: There are probably two points to make. The first is that most small businesses are currently exempt from the Privacy Act. Most businesses with an annual turnover of $3 million or less are exempt from the act.

Probably the other point to make in terms of Australian privacy principle 11, which is all about protecting personal information and keeping the information secure, is that the onus is on the entity to take reasonable steps to protect that information. That reasonableness element is important to consider in terms of the size of the entity. What might be reasonable for a large entity to do might not be for a smaller entity.

CHAIR: That's helpful. I guess there's reasonableness as well about the type of data that is being held? Yes? Okay. There were some nods at the table.

We've talked a lot today about the Privacy Act review. There is, as I understand it, more work to be done, but people might be concerned that it is going to be pushed out further and further. Do you have an idea about timing? Has the Attorney-General asked that there be a certain time by which the report is delivered to him so that there can be some progress on the other issues that have been raised today?

Ms Galluccio: We're very close to finalising our review. We're currently scheduled to provide the Attorney-General with our final report before the end of the year.

Ms Brayshaw: And then the next step would be in relation to government considering that and then there would be further implementation of what government seeks from that review. I think it would be fair to say that the Attorney-General has a real interest in this area and certainly has expectations in terms of this review being finalised so that we can move to that next step of reforming and updating our privacy laws.

CHAIR: I have some questions for ACMA, and, if Senator Shoebridge allows me some time, I may be able to sneak them in if there's some time at the end.

Senator SHOEBRIDGE: All power lies with you at the end of the day, Chair, as you know. I thank everybody for attending and for your work in pulling together this bill. It was an urgent reform, and you pulled it together. To go first of all to the proposed new penalty regime in 13G, this came from the ACCC recommendation where penalties were designed to penalise manipulating market behaviour, and in that context the potential benefit to corporates could be extremely large—hundreds of millions or billions of dollars in manipulating the market environment. Do you agree with that, Ms Brayshaw?

Ms Brayshaw: I think I do, yes.

Senator SHOEBRIDGE: You think you do?

Ms Brayshaw: Sorry, I'm just making sure I understand the context of where the question goes. In terms of the Australian Consumer Law, it's not an area of responsibility that I have. The area of interest that we've had is where the 2019 digital platforms report highlighted the links between competition and consumer privacy, and the types of harm that can come. To put it in context, I'm not an expert in Australian Consumer Law.

Senator SHOEBRIDGE: No, but if you're manipulating large markets, there's potentially very large upside in terms of the benefit from unlawfully manipulating markets, so I think we can agree on that.

Ms Brayshaw: Yes.

Senator SHOEBRIDGE: And so the regime designed to attach a penalty to the benefit that can be obtained has a kind of commonsense approach when you're in that context of the ACCC. Do you agree?

Ms Brayshaw: Yes.

Senator SHOEBRIDGE: In terms of privacy, though, the way this 13G operates is the maximum penalty under the proposed amendments for relevant privacy breach is capped at the higher of either $50 million or three times the benefit obtained from the breach or, if you can't determine a benefit, up to 30 per cent of the adjusted annual turnover. Is that how it works?

Ms Brayshaw: That's right.

Senator SHOEBRIDGE: If a corporation deliberately and consciously seeks to benefit from a privacy breach, maybe unlawfully onselling the information, they may obtain, say, a $10 million benefit from selling the information. If they had a $1 billion turnover, for example, the court looking at that would say, 'Well, what's the maximum penalty?' It's either $50 million or three times the benefit that they've obtained or, if you can't determine the benefit, the turnover. In that case you could determine the benefit, $10 million. Three times that is $30 million, which means that you are stuck at the $50 million cap. But if their competitor had the equivalent data stolen from them and they had been negligent in protecting it, in that case they wouldn't have obtained a benefit, so you would have $50 million or 30 per cent of their adjusted turnover, and their competitor might face a $300 million maximum fine. That doesn't make sense to me because one of those players consciously, deliberately and maliciously sought to breach the Privacy Act to obtain benefit and the other one was negligent and so found to be in breach. Have you thought about how those things work in practice?

Ms Brayshaw: I might make a couple of points first in terms of setting the consideration we've given to the provision and then I might ask Ms Galluccio to talk further. In terms of what the bill is doing, it recognises that the current penalties that we have are quite inadequate at 2,000 penalty units, and so the government's commitment was seeking to increase those penalties.

Then there's the consideration of the approaches that we've taken, in terms of how we have settled on maximums. It certainly still is a matter for the court to determine in the circumstances of cases—that's the maximum, and it will be a matter for the court to determine and consider all the types of issues that might be in a particular case, and you've given some examples of what some of the factors might be. The approach we have taken and the consideration we've given is that, given the digital platforms inquiry recommended that approach, we have used that as the basis for setting out the options for a court to consider to take that into the case. In terms

of that question about the different scenarios where there is recklessness versus deliberate benefit, I think I might ask Ms Galluccio to give a little bit more reflection in terms of how that operates.

Senator SHOEBRIDGE: Before we go to Ms Galluccio, these aren't options for the court. These are statutory caps on the penalty. What I'm putting to you is that the statutory caps operate in a perverse way where players, large corporates with large turnovers, may be desperately trying to prove they got a benefit out of the breach in order to minimise their maximum penalty. That's how it works, because if they get a benefit—a relatively modest benefit—then the 30 per cent turnover cap doesn't apply to them. That's how it works in practice, Ms Brayshaw, isn't it?

Ms Brayshaw: That's correct. What I would say is that at the moment a court can only make a maximum civil penalty of 2,000 penalty units. In looking at how and where we move, the government has decided to move to this proposal and this approach.

Senator SHOEBRIDGE: We've had a number of witnesses suggest that this model produces a perverse outcome where a conscious, deliberate and malicious breach faces a lower maximum penalty, for the same substantive kind of data breach, than a negligent or reckless breach. It's a perverse outcome, isn't it, where deliberate, conscious, malicious breaches—of a similar nature—face a lesser penalty than a reckless or negligent breach? That's not how the law normally works.

Ms Brayshaw: In terms of the circumstances you're presenting, I don't know if they would be like-for-like cases in terms of how a court would see the behaviour of recklessness versus something that was deliberate.

Senator SHOEBRIDGE: I'm talking about the cap.

Ms Brayshaw: I take your point that there is a cap. On the cap, the government has decided that in shifting from the current penalties, which are only 2,000 penalty units, we need to increase that. That has been informed by the approach taken with the digital platforms inquiry, and that's been the process in which we've set it.

Senator SHOEBRIDGE: That's why I put this to you. This model may work very well in a competition law environment, where there are potentially huge upsides and benefits from manipulating the market, but it doesn't naturally or even intellectually fit well in a privacy breach. The benefits are unlikely to be of the same order that you get from manipulating a market. Did you consider that when you were doing this drafting?

Ms Galluccio: Can I make one clarification: in terms of limb (c), there would still need to be a benefit. Under limb (b), if the court can determine the value of the benefit then that applies. Under (c), it's when the court can't determine the value of the benefit, but you'd still need to show that there was a benefit from the wrongdoing.

Senator SHOEBRIDGE: Again, we get to the same point. How do you read that (c) requires benefit?

Ms Galluccio: It says 'if the court cannot determine the value of that benefit', that benefit being the one referred to in paragraph (b).

Senator SHOEBRIDGE: Okay; potentially, that's how it works. To go back to the first point, do you accept that the regime—which is what I put to you—works more naturally in a competition environment, where the benefit is potentially very, very large from manipulating the market, than it does in a privacy regime, where we haven't had any evidence about the kind of huge upside market benefit that would come?

CHAIR: Sorry, Senator Shoebridge; I just want to remind you that officers can't give opinions. They may not choose to answer your question with an opinion.

Senator SHOEBRIDGE: My initial question was: did you consider the nature of the different types of markets, regimes, manipulating markets and privacy when you translated the penalty regime across?

Ms Galluccio: There are lots of different scenarios in which breaches of privacy obligations can occur. So, with paragraph (b) and paragraph (c), is there in the instance where the entity gets a benefit—say, for example, they onsell the personal information of individuals and obtain a benefit from that, and they do that in breach of the Privacy Act. Those limbs are there so that there can be some connection between the benefit gained by that entity and the wrongdoing. In those circumstances, I think having those limbs there is quite helpful.

Senator SHOEBRIDGE: But it may well be a very inchoate hard-to-determine benefit as opposed to a very direct benefit, like a direct commercial payment. The difference in the fines that a corporation may face could be in the magnitude of 10 or more in the maximum fine—so a hard-to-identify inchoate benefit. That corporation would face a much bigger fine than somebody who cut a deal and sold the data for a set sum. That's how it works in practice.

Ms Galluccio: It would ultimately be up to the court to work out what was or wasn't the benefit.

Senator SHOEBRIDGE: But, in point (c), they only have to find some kind of benefit. It could be a tiny benefit or it could be a hard-to-articulate benefit. If there's some kind of even modest benefit, that opens the door to (c), does it?

Ms Galluccio: I think it's a matter for the courts. If the court determines there is a benefit, then, first of all, it looks to limb (b) to look at the value of that benefit. If they can't work out what the value of that benefit was, they can look to limb (c).

Senator SHOEBRIDGE: Can you give an example of when limb (c) would apply? You must have workshopped some examples.

Ms Brayshaw: An example could be a situation where an entity has aggregated personal information and has gained a benefit in relation to that but it's unclear what precise benefit has come from that activity. It's at that point that the court could turn to looking at limb (c), to determine, of the greater of $50 million or (c), the type of penalty in the circumstances it wishes to impose.

Senator SHOEBRIDGE: My understanding of Ms Galluccio's evidence is: once they find a benefit but they can't quantify it, (c) is engaged. Is that how you read the act? If they find a benefit but can't quantify it, it's not an option; (c) is engaged, isn't it?

Ms Galluccio: If the court can't determine the value of the benefit—

Senator SHOEBRIDGE: But if they know there is one, then (c) is engaged.

Ms Galluccio: Yes. Just to clarify: there's still limb (a) to remember, the $50 million.

Ms Brayshaw: Because it's the greater of.

Senator SHOEBRIDGE: I understand. So a hard-to-identify inchoate benefit—I still can't work out the example for what kind of activity would satisfy the test of a benefit you can't determine the quantum of. Does anybody have any examples of when this big fine would apply? This is the headline part of the bill. I just want to know what it would apply to.

Ms Brayshaw: We could take it on notice and come back to the committee with an example.

Senator SHOEBRIDGE: Do we have an on-notice provision?

CHAIR: Yes, we do.

Senator SHOEBRIDGE: This is the headline part of the bill—there's this big fat fine here of up to 30 per cent of turnover.

CHAIR: They've said they'll take it on notice, Senator Shoebridge.

Senator SHOEBRIDGE: When you drafted the bill was whether or not the regulator has the capacity to do the work a part of what you took into account?

Ms Brayshaw: In terms of developing the bill, we did take into account and consider the role of the regulator and how these provisions would assist them.

Senator SHOEBRIDGE: Did you consider capacity? We've heard evidence from pretty much every stakeholder that they're not satisfied that the OAIC has the capacity. We heard from the Information Commissioner this morning that there are very real resource constraints and that, in fact, doing one investigation that may lead to a prosecution is likely to cost up to $5½ million and their entire budget is in the low 30s. Did you consider whether or not these new provisions could actually be prosecuted by the agency?

Ms Brayshaw: In terms of the consideration, yes. It's something that's in parallel to our engagement on the legislation. In terms of the Office of the Australian Information Commissioner being a portfolio agency, we have ongoing conversations with the office in terms of their resourcing and their ability to undertake their work.

In terms of the Optus data breach, you're aware that, as part of the budget, $5.5 million was provided over two years. That was in response to that engagement and discussion. A further $17 million over two years was confirmed in the October budget in relation to ensuring that the office is adequately resourced to address privacy complaints and take strategic enforcement action. That's a separate part that was confirmed in the October budget.

In terms of the capacity, we are always carefully looking at the resourcing requirements and the government is mindful of that. We're very conscious that the Privacy Act review could indeed look at the approach and the way in which the office operates and how we can support that, so there will be further consideration there. Yes, I would say that we have given consideration, and they are two recent measures that have been in the October budget.

CHAIR: Senator Scarr, do you have a question on something you want to follow up?

Senator SCARR: I want to pursue the line of questioning Senator Shoebridge and I have embarked upon in the course of this inquiry. Do witnesses recognise that the structure of this penalty clause is predicated on there having been a benefit and that that notion just simply does not apply in circumstances where a company has been a passive actor and has actually been hacked from the outside? I have been following the reason—and maybe you can take this on notice—but the concern I have is that this clause is like trying to fit a square peg in a round hole because in certain cases there just is no benefit. That should be reflected in the drafting. I'd like your response to that.

Ms Galluccio: That's right; there will be some circumstances where there just isn't a benefit, and that's when the maximum penalty of $50 million will apply.

Ms Brayshaw: You gave the example of a cyberattack, as opposed to a situation where a privacy breach is occurring because they're using information that they've collected without consent or something else. There are different scenarios. The approach to that penalty provision and the different limbs is seeking to take that into account, which is why there is that first limb.

Senator SCARR: I suggest you carefully reflect. Senator Shoebridge has been a barrister of some longstanding and I was general counsel and we're both struggling with the application of that benefit in this case. I think there has to be a better way to draft this clause to make it clearer to all stakeholders. I leave you with that suggestion. Thank you.

CHAIR: I thank you for appearing today and for the time it has taken to prepare those submissions that you gave us. Before we close the hearing today, we do have one tabled statement, and I seek a motion from a member of the committee to accept that statement.

Senator SHOEBRIDGE: I move the motion.

CHAIR: We accept that tabled statement. We are also seeking to determine a deadline for returning questions taken on notice during the day's proceedings—I don't think there were many, but there is one—of close of business tomorrow, because of the short time frame.

That concludes today's proceedings. The committee has agreed that answers to questions on notice for this hearing should be returned by close of business Friday 18 November 2022. I apologise for the very short deadline and thank you for your assistance on that. I thank all witnesses who have given evidence to the committee today, and those submitters that have provided evidence to the committee. I also thank Hansard and the secretariat.

Committee adjourned at 12:30