



COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

SENATE

FINANCE AND PUBLIC ADMINISTRATION LEGISLATION
COMMITTEE

**Data Availability and Transparency (Consequential Amendments) Bill 2020,
Data Availability and Transparency Bill 2020**

(Public)

TUESDAY, 20 APRIL 2021

CANBERRA

CONDITIONS OF DISTRIBUTION

This is an uncorrected proof of evidence taken before the committee.
It is made available under the condition that it is recognised as such.

BY AUTHORITY OF THE SENATE

[PROOF COPY]

INTERNET

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

To search the parliamentary database, go to:

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

SENATE

FINANCE AND PUBLIC ADMINISTRATION LEGISLATION COMMITTEE

Tuesday, 20 April 2021

Members in attendance: Senators Ayres [by video link], Chandler [by video link], Kitching [by audio link].

Terms of Reference for the Inquiry:

To inquire into and report on:

Data Availability and Transparency (Consequential Amendments) Bill 2020 and Data Availability and Transparency Bill 2020.

WITNESSES

ANTON, Ms Deborah, Interim National Data Commissioner, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet.....	1
ARNOLD, Dr Bruce Baer, Vice-Chair, Australian Privacy Foundation.....	15
BLOEMENDAL, Mr Ian, Chair, Privileges and Immunities Committee, Federal Litigation and Dispute Resolution Section, Law Council of Australia [by video link]	15
GADIR, Mr Jonathan, Member, New South Wales Council for Civil Liberties [by video link]	15
GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia [by video link].....	15
HAYTHORNTHWAITE, Dr Adele, Research Data Consulting Lead, Sydney Informatics Hub, The University of Sydney [by video link].....	22
KRAHULCOVA, Ms Lucie, Executive Director, Digital Rights Watch Inc. [by video link].....	25
MacDONALD, Mr Nathan, Principal Policy Lawyer, Law Council of Australia [by video link]	15
MENZIES-McVEY, Mr Paul, Assistant Secretary, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet	1
PAYNE, Mr Tim, Director, Higher Education Policy and Projects, Office of the Vice-Chancellor and Principal, The University of Sydney [by video link]	22
WARREN, Mr Justin, Board Member, Electronic Frontiers Australia Inc. [by video link]	25
WONG, Mr Chadwick, Senior Solicitor, Public Interest Advocacy Centre [by video link]	15

ANTON, Ms Deborah, Interim National Data Commissioner, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet

MENZIES-McVEY, Mr Paul, Assistant Secretary, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet

Committee met at 09:00

CHAIR (Senator Chandler): I declare open this public hearing of the Senate Finance and Public Administration Legislation Committee for its inquiry into the provisions of the Data Availability and Transparency Bill 2020 and the Data Availability and Transparency (Consequential Amendments) Bill 2020. This is a public hearing, and a *Hansard* transcript of the proceedings is being made. We are also streaming live via the web, which can be found at www.aph.gov.au.

Before the committee starts taking evidence, I remind all witnesses that, in giving evidence to the committee, they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated by the Senate as a contempt. It is also a contempt to give false or misleading evidence to a committee. In addition, if the committee has reason to believe that evidence about to be given may reflect adversely on a person the committee may also direct that the evidence be heard in private session.

The committee prefers all evidence to be given in public, but, under the Senate's resolutions, witnesses have the right to request to be heard in private session. It is important that witnesses give the committee notice if they intend to ask to give evidence in camera. 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 given in camera. Such a request may of course also be made at any other time. On behalf of the committee, I would like to thank all witnesses appearing today for their cooperation with this inquiry.

I now welcome representatives from the Office of the National Data Commissioner. Information on parliamentary privilege and the protection of witnesses and giving evidence to Senate committees has been provided to you. I remind senators 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 a 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 and how policies were adopted. Officers of the department are also reminded that any claim that it would be contrary to the public interest to answer a question must be made by a minister and should be accompanied by a statement setting out the basis for the claim. I now invite you to make a short opening statement, and at the conclusion of your remarks I will invite members of the committee to ask questions.

Ms Anton: Firstly, I would like to thank the members of the committee for inviting me to appear today and allowing me to deliver an opening statement on the Data Availability and Transparency Bill 2020. We developed this bill because the world is changing. Technology allows us to do more with data, but the way our world operates from a legislative point of view is it is all in silos that have been built up over time. To do more with data requires that we break out of our existing silos and engage sensibly with risk.

The bill before the parliament has been developed in response to the Productivity Commission's 2017 inquiry into data availability and use. That inquiry noted:

The potential value of data is tremendous; as is the scope for Australia to forgo much of this value under the misconception that denial of access minimises risks.

... ..

These risks—and the desire for privacy and confidentiality—should not be downplayed or trivialised. They are real and important. But, many of them are able to be managed with the right policies and processes—and better managed than they are now.

The bill before you seeks to do just that.

The bill will create a data-sharing scheme overseen and regulated by a new independent national data commissioner to allow sharing for the right reasons with the right people, with appropriate controls to manage risk. I have tabled for the committee a graphical representation of the key controls that participants need to work

through in order to share data under the scheme, and I trust that that will support our discussions today and your ongoing considerations of the bill.

The bill seeks to progress a necessary set of reforms to modernise APS data-sharing practices, to set higher and consistent standards and to add additional transparency, to ensure the public know what is being done with their data. Ultimately this means that the bill will enable the Public Service to function better and be more responsive to the needs of Australians.

The purpose test embedded in the bill states that data can only be shared for: delivery of government services; informing policy and programs; and research and development. These are important controls of the scope of the data sharing enabled by the bill. It specifically precludes sharing for purposes that relate to national security or that may have a negative impact on individuals such as when pursuing an enforcement action. The safeguards described in the bill provides layers of defence that create a consistent and strengthened approach for the entire APS to use when managing data. The data-sharing principles across five domains identify risks and apply controls to ensure risks are appropriately managed. They are based on international best practice and are already incorporated into similar state laws.

Accreditation is also a key safeguard under the bill. Accreditation requirements mean users of the scheme must prove they have the relevant skills and capability to access government data. For those seeking to access personal data, they have additional requirements: they must be covered by the Commonwealth Privacy Act 1988 or equivalent state or territory privacy legislation. This gives confidence to the public that they have redress should things go wrong, and gives data custodians confidence that entities can be held responsible for the personal information they access under the bill. Importantly, this means foreign entities not covered by Australian privacy laws cannot seek to access personal information under the bill.

The National Data Commissioner has an important role to oversee these safeguards and take action to reduce harm if data sharing is not compliant with the requirements in the bill. To ensure the sharing under this bill is trusted by the public, we have built in transparency elements. The key terms of data-sharing agreements will be made publicly available, laying out what data will be shared, how this will benefit the public and how risks will be managed or controlled.

The bill has been developed using a privacy-by-design approach, which means privacy has been considered at every stage of the legislative development process. We have commissioned three independent privacy impact assessments on the bill, and we published the third and final PIA, which aligns with the bill as introduced to parliament, on Friday 16 April. For the chair's reference, we have provided a copy of that through the committee secretariat. The third PIA concluded that, in the context of the benefits that can be achieved through increased data sharing, our layers of defence are strong and robust, and represent a reasonable, necessary and proportionate response to privacy. The PIA also highlights the important work yet to come for the commissioner in progressing from legislation to implementation.

I want to leave you with my views on why these reforms are so important. During the three years of co-design and consultation on the bill, no-one I have spoken to, whether it be a public servant, a researcher, a privacy advocate or a member of the public, has disputed the value of data. Data is the difference between silo delivery of government services and the user experience that citizens expect and have experienced through services such as myTax. Data takes the guesswork out of government policy design by helping our policymakers to craft informed and insight-driven policy and programs that benefit all Australians. Data drives the research sector by helping academics and researchers identify valuable insights and improve Australians' experience and quality of life. All of those things matter. Yet many of the submissions to the committee are concerned about the sharing of personal information and ask the question, 'Have we got the balance right?' We believe we have, but we equally welcome this scrutiny process.

We have designed a principles based bill to ensure data sharing is secure, effective and transparent. The safeguards and controls that apply to data sharing in the bill are rigorous and able to be consistently applied across the entire Public Service, raising the bar on current APS practices. I am happy to respond to any questions that members of the committee may have.

CHAIR: Thank you very much for your opening statement, Ms Anton. I might kick off with a few questions. At a parliamentary inquiry earlier this year, the director-general of ASIO said:

Foreign intelligence services and their proxies are all too willing to take advantage of the openness that is integral to our universities and research institutions to steal intellectual property and cutting-edge technologies.

I was wondering what consultation you've had with ASIO and other security agencies regarding the bill that we are discussing here today.

Ms Anton: The bill was co-designed with the Public Service, including the national security agencies as well as many of the stakeholders, during our various rounds of consultation. In terms of your broader question about security, what might be helpful for you and the committee is to understand that, while the bill contemplates the sharing of data with foreign entities, the bill has a series of controls. I might take you the controls. The short answer to your question is that we have co-designed the bill in consultation with the national security community. In particular, there are exemptions for national security purposes that have been carefully crafted with those, as have some of the other controls in the bill.

More particularly, I do note that opening point that data cannot be shared for a purpose that relates to a prejudice of national security as per 15(2). In accrediting entities other than Commonwealth government entities, essentially, our criteria for accreditation is that the entity's participation in the data-sharing scheme would pose no concerns for reasons of national security as per section 77. The commissioner can suspend or cancel accreditation for reasons of security as per clause 81. As I noted in my opening statement, it's not expected that foreign entities, which are not covered by Australian privacy law, will be able to access personal data as they can't satisfy the privacy coverage test under clause 28.

Data-sharing agreements which may involve working with research or government policy purposes and engaging with the research community which you allude to do have a requirement for an accredited user who accesses the data. Again, there's a people principle as part of 16(4). Under that, the commissioner is able to share information with ASIO. If ASIO has concerns about the sharing of information with particular individuals, the commissioner can take action against the accredited user's accreditation to limit the sharing of data. The commissioner is specifically authorised to provide information to ASIO under clause 108. The commissioner may impose conditions of accreditation as appropriate for reasons of security, including on the basis of adverse or qualified security assessments under clause 78(1). That condition could include limiting access to shared data to individuals within an entity or could prevent shared data being accessed by particular individuals under clause 78(2). Importantly, decisions to refuse to accredit a foreign entity for security reasons, to suspend or cancel the accreditation for security reasons or to impose conditions are not reviewing by the AAT, which is set out in clause 118.

Ultimately, it's really important when considering the bill that the final decision to share data under this act ultimately rests with the data custodian, the Commonwealth public servant, and it makes clear that there is no duty to share. This bill is creating a framework to share, but there is ultimately no onus on the Commonwealth to share, and that's not a reviewable decision; they can simply say no. They do have to provide reasons why not, but ultimately, if they can't manage the risks, if it's not for an appropriate purpose, they can simply say no. From my point of view, those are quite a few layers of control—the creation of an accreditation scheme that works with the research sector in terms of accessing data that links back into the work being done by ASIO. Those are new controls designed specifically for this scheme.

CHAIR: One of the concerns that has been raised around this whole idea of foreign interference in the university sector, though, is that the purpose for which data might be provided isn't necessarily going to be up-front in terms of what the university or the entity might be asking the data commissioner for the data for. That sentence was terribly constructed; my apologies. It's not always going to be very obvious why the data is being asked for, so how can we be sure that, once the data has gone to one of these entities, there is some sort of ongoing monitoring in place to ensure that it's not being used for a purpose other than that for which it was initially requested?

Ms Anton: I go to the flow chart that we've provided you with. There is a series of controls we have worked through. There needs to be a very up-front conversation about what data is being shared, why it is being shared—and, again, that check-in with ASIO. But your point is after the fact. The commissioner themselves is established as an independent statutory officer. The left-hand side of that diagram shows they have responsibilities for monitoring, regulation and enforcement of the data sharing. They are able to undertake own-motion investigations. As you'd expect with any regulator, they're actually able to go back and talk to the people who are sharing data, seek evidence from them and make sure that they are doing the right thing. There is also a complaints mechanism built into the legislation for those participating in the scheme. Where they think the data sharing is not happening appropriately, they're able to make complaints that the commissioner can respond to.

As you would expect, there is quite a series of enforcement related actions which could ultimately lead to suspension or cancellation of accreditation injunctions on the sharing, giving binding directions about what is happening and ultimately seeking civil or criminal penalties where appropriate. At the end of the day, there is a stick to go with the permissive: yes, we want to share, but there are controls in place at the other end. Paul, did you want to add to that?

Mr Menzies-Mcvey: The only comment I would add is that data-sharing agreements must specify the purpose for which the data can be used and provide that it can't be used for any other purpose. The data-sharing agreements are under clause 20 of the bill. All data entities that are parties must comply with it. It will be a breach of the DAT Act if it is used for another purpose, and the commissioner, as Ms Anton has said, would have regulatory powers to enforce that agreement.

CHAIR: That ties in nicely to my next question. What are those monitoring and compliance processes that you have in place to ensure that entities are only using the data for the purposes under which they have sourced it under their data-sharing agreement?

Ms Anton: Obviously, we don't have them in place at this point, because the office doesn't exist. What the bill contemplates in terms of those regulatory powers, as I've mentioned, is really about creating—to start with, the bill sets out what you're trying to do. There are then a series of subordinate documents and guidance materials that need to establish the rules more clearly to give confidence to entities that they are using things appropriately, be they regulations, rules, data codes or legislative instruments. The back end of the bill is really about more of those enforcement elements such as the capacity to conduct an own-motion investigation. It is also about injunctions placing conditions on accreditation. That ongoing monitoring is part of ensuring that the public can have confidence that the scheme is being used appropriately.

If you imagine the scheme starting up, in the first instance I imagine the commissioner will place quite a lot of scrutiny on the first series of data-sharing agreements that are made, because this is about taking and translating the law into practice and making sure that the guidance that they have provided is correct and appropriate. Then they're able to go in and, if they would like to, essentially require evidence from the custodians that that information is being used correctly. So those scrutiny processes are there. The practice of how they will be used, the normal statement from a regulator, will be about a scaled and appropriate enforcement approach. That is about doing deep dives early to make sure that it is being used appropriately.

CHAIR: Other than having the ability to consult with security agencies when you're determining if an entity should become accredited, what ongoing oversight will security agencies have to ensure that access to government data isn't being used even inadvertently to the advantage of foreign powers?

Ms Anton: The bill allows us to share information with ASIO from time to time. It gives us the capacity to share information with ASIO. What's really important to remember is that the data-sharing agreements are about what is being shared and where that is going to be publicly available, so that information becomes part of the public domain and the information that they can readily access in addition to the information that they may secure from us. I would anticipate that, as part of their usual processes, they will keep an eye on that. I can't speak for them in terms of what they will do; I can simply say that the information will be publicly available.

CHAIR: We talk about security agencies having an input at that initial point when we are accrediting a third party to access government data, but is there, through the commissioner's ongoing compliance monitoring of accredited entities, some sort of legislative trigger at which the commissioner says there needs to be input from national security agencies to determine whether or not this data is being used appropriately, or is that more ad hoc?

Ms Anton: I don't believe there's a specific trigger in the bill that would do that. From my perspective, that's just part of the usual practice where the commissioner, where it deems necessary, would consult with those agencies.

Mr Menzies-Mcvey: As mentioned before, at any time after accreditation a security agency could provide an adverse security assessment to the Data Commissioner, and the Data Commissioner has powers then to take appropriate action, which may include either suspending or cancelling the accreditation, which would prevent any further data sharing, or imposing conditions on the accreditation, which might say that the people of concern can no longer have access to that. The commissioner will then have regulatory powers to ensure that the conditions on the accreditation were being complied with.

Ms Anton: Any actions taken on the basis of the security advice are non-reviewable by the AAT, so they can simply be taken.

CHAIR: Are security agencies comfortable with the bill as it's currently drafted? You mentioned at start that you consulted with them in developing the bill, but what was their final say on the bill?

Ms Anton: Ultimately, as with any piece of legislation, the bill went through a cabinet process to make sure that the requirements of the bill and the policy authorities were appropriate and approved. Obviously, all agencies provided advice to government and cabinet in those considerations.

Mr Menzies-Mcvey: The intention is that, if the office of the commissioner is established, we will enter into MOUs with both ASIO and the Office of the Australian Information Commissioner to document the day-to-day working relationship.

CHAIR: Thank you for that. Finally, given the prevalence of cybersecurity risks, does the transfer of government data to third-party agencies increase the risk that that data can be accessed by hackers? If so, what requirements will the commission be putting in place through this legislation to ensure that government data can't be inappropriately accessed?

Ms Anton: The core risk management framework that's outlined in the bill is related to the data-sharing principles. That considers five dimensions that must be applied to any data-sharing project. The project principle is principally about whether this is the right data for that purpose. The people principle is: are these the right people to access the data? The relevant principle probably, in terms of what you're talking about, is the setting principle, and that requires that the data is shared in an appropriately controlled environment. That setting principle includes but is not limited to the following elements: that the means by which the data is shared or appropriate, having regard to the type and sensitivity of the data to the control the risks of unauthorised use or release and reasonable security standards are applied when sharing the data. Essentially, that principle allows for more detailed guidance to be provided in the subordinate material to agencies to make sure that, if there are particular requirements around where data can be stored and transferred, that should be taken into account.

Again, the principle of the bill is essentially that you should share data in the way that is most reasonable and that you're able to manage risks. In terms of those settings, if it's not conceivable that you can manage risks by providing it to a third party then there are other avenues available to access that data. A very commonly used approach by some of our agencies such as the AIHW and the ABS is to provide access to data in a secured facility that they run and that people have logged access to.

So, while the bill doesn't preclude providing data to third parties, it does put an onus on data custodians and those people who are receiving the data to have reasonable security controls in place. If they don't then the onus is back on both of those parties to say this is not the appropriate way to actually request data access. That happens in a negotiation and a conversation, and both parties need to be satisfied that they have appropriate controls in place to safely manage the data before that sharing takes place.

The other point I would make is that my sense is that there is a desire from the research sector, in particular, and from other parties to access government data to deliver good outcomes. I think there is a very strong awareness amongst those parties of the importance of maintaining appropriate security and controls and of maintaining the public's trust as we embark on a more robust sharing process.

Senator AYRES: I have a couple of general questions, and then I want to ask a series of questions about the relationship between data-sharing work and some of the government's compliance programs and other programs that either have been underway or are underway at the moment. Before I do, I was listening to your responses to Senator Chandler's questions and I think you've answered the questions in terms of who the data is shared with, but it's true that the data you're creating, as you're going through data sharing and data matching, is of much more value than the individual siloed data, isn't it? It's of more value to the public sector and to the agencies that you're working with, but it's also of more commercial value and of more value to foreign powers that might engage in the kinds of activities that Senator Chandler's described. That creates a greater onus for the protection of the data, doesn't it?

Ms Anton: I think you're going back to the PC's comment in my opening statement. There's an opportunity here, but there's also an important set of risks that need to be managed—absolutely. The Productivity Commission made the point that, at the moment, there isn't a consistent approach to sharing data. From my perspective, if we propose to do more to deliver better outcomes for the Australian public, then the bill and the frameworks it creates are about raising the standards of consistency across the public service by pulling on some of the best practice that occurs both domestically and internationally in terms of the data-sharing principles. Let's be smart about how we do this.

Principles based legislation allows us to refine and tighten those controls over time and make the most of it. I note your point about it being of interest to commercial players and other governments. I would make the point that, firstly, there are very clear purposes for which data can be shared, which is about government service delivery, research and development, and the support of policy design. We've constrained the purposes for which data can be shared—that was in our very first lot of public consultations. Ultimately, a control point for me is the transparency elements of the bill: that what is being shared needs to be published on a website, that there's a need to be very clear about what is happening and why, and that there's a need to explain what the public interest is that's being met as part of that data-sharing principle.

I don't dispute your point. I think there are both increased benefits and increased risks. The point I made in my opening was that this is really about whether we have struck the right balance in terms of designing that control framework.

Senator AYRES: That's alright in terms of agreements to share data. That works right up until the moment there's a breach, doesn't it? Senator Chandler pointed to the risks of sharing with third parties, but, of course, the big data breaches have been of government information being inadvertently provided or provided as a result of some cybersecurity breach. This is more valuable data, because it involves data matching and is the result of data analytics work across agencies. You may not have a data-sharing agreement with the person or the foreign power who's got the data or released the data but it's created nevertheless, isn't it?

Ms Anton: Going to your point about where the data has most value—you're talking about particularly the integrated datasets—

Senator AYRES: Yes.

Ms Anton: I would point to an additional control in the bill around the authorised data service provider. Noting that more integrated data has a richer value, the bill seeks to formalise in legislation some existing policy practices in the Commonwealth—that under the current frameworks it's authorised integrating authorities—so there's only a very small set of very experienced players who are able to actually manage complex integrated data assets, which have to meet very, very high standards in order to do so. Those are the likes of the ABS and the Australian Institute of Health and Welfare. The bill itself seeks to recognise that, if you are seeking to undertake complex data integration to build a complex data asset that has that increased value, the only people authorised to do so are the authorised data service providers. So there is a higher bar built into the legislation for the creation and management of those types of assets.

Senator AYRES: What are the penalties for breaches for data-sharing agreements under the act?

Ms Anton: The penalties under the act are constructed in two ways. Obviously, in order to use the act, you have to meet the requirements of the act. If you're not meeting the requirements of the act, then the penalties actually rebound to the original legislation under which the data was collected. One of the challenges of trying to design something that fits across a whole lot of pieces of legislation is: how can we accurately determine what are the relevant provisions and penalties that should be applied? If you are not using the act as intended, then, basically, you're in breach of the original sharing of the bill under which the act was collected. The bill itself then provides for additional penalties or gap coverage where people are simply not complying with, for example, provision of information to the commissioner or where it wasn't otherwise covered in original legislation. Paul, did you have the relevant clause on that one?

Mr Menzies-McVey: Yes, certainly. For breach of the mandatory terms of a data-sharing agreement, which include the requirement to only use it for the agreed purpose, it's a civil penalty of 300 penalty units. That's clause 20. But, as Ms Anton was saying, there are general penalties applying for if the sharing or use was purporting to rely upon the authorisation in the bill and the bill doesn't cover that, in fact. There are both civil penalties, which are the 300 penalty units, and criminal penalties, which is imprisonment for two years, for intentional reckless breaches.

Senator AYRES: I noticed in the legislation that the data is referred to as Australian government data and/or public sector data or public data. Who do you think owns the data?

Ms Anton: My general sense is we, the government, hold the data in trust for the public. They do provide that information, and it's a responsibility, as with many functions of the government, to hold that in good faith for the public.

Senator AYRES: That's the thrust of a range of the submissions—that this notion of privacy and consent is really getting away from people. Some of this data is provided, in some senses, voluntarily; people consent to it being provided, but this act contemplates that it may then be used for other purposes, as determined by the data custodian, that would not have been contemplated by the person when they gave what passes for permission on the government website. It's an expanded notion of consent. And some people provide this mandatorily; they don't have a choice. If they want to receive a government service or a government benefit, they provide the data or they don't get it. What do you say to those criticisms?

Ms Anton: I would make the opening point that it's not just about personal data—that the Commonwealth collects data on a range of fronts—but I note that your concern goes particularly to those concerns about personal data. I just wanted to make sure that we position the scheme as: it can relate to business data or environment data; it is broad in its contemplation. It's the question of how the bill interacts particularly with the Privacy Act. The bill relates to an express authorisation to disclose, collect and use personal information, where the requirements of the

DAT bill are met. Basically, it's an authorised exemption, an expressed authorisation to use the bill under the Privacy Act. The Privacy Act provides for, essentially, secondary use frameworks to be met, and this bill then creates a very complex set of controls about what is reasonable and practical in those instances. I do note the overriding concerns, ultimately, about the need to maintain privacy, and that has been very material to our work throughout the whole process.

The bill is designed to complement, not to duplicate, the Privacy Act. That was actually one of the key design points that we were asked to contemplate at the beginning. I think one of the important elements is that the Privacy Act and the Australian Privacy Principles do continue to apply to the sharing of data under the bill, if it is about personal data. Again, clause 16(8) essentially makes the point that data sharing should be minimised as much as possible. So—again, I think these are important and valid controls—you should only be sharing the data that's necessary to do the job.

For anybody, under the bill, to access personal information, they have to have privacy coverage. We have done our work through the privacy impact assessment. I do note that the PIA, which we've now provided for your information, does recognise that ensuring that the APPs, the Privacy Principles, still apply—or comparable principles, in terms of recognition of state and territory work. They are a really important baseline for protecting personal information. On that basis, they recognise that we haven't duplicated those protections that are still available under the Privacy Act.

As to those controls and recourse: having remit for the public is still really quite important where things go wrong, which I guess is kind of what you were getting to. So, again, clause 28 makes very clear, where data sharing is related to personal information, that they are able to then make complaints under the Privacy Act. We're not seeking to duplicate those complaint and redress mechanisms under the Privacy Act. But, in terms of even contemplating the equivalent elements with state and territory law, we did work with the Information Commissioner on this and make very clear—again, trying to do a principles based expansion for the future—that those protections of personal information need to be comparable to the Privacy Principles, there needs to be monitoring for compliance with the law and there needs to be the means for individuals to seek recourse if the individual's personal data is dealt with in a way contrary to the law. So, while we haven't imported the Privacy Act into the bill, those really important links under 28 and the capacity to refer things out to the Privacy Commissioner do maintain the importance of privacy in the work that we're doing and still rest that control, where it's more appropriately dealt with by the Privacy Commissioner, with her.

Senator AYRES: It does put a lot of power in the hands of the Data Commissioner, many of whose decisions will be non-reviewable.

Ms Anton: I would just note that the decisions to share the data are ultimately left with data custodians. So they're left with senior public servants. Our view was that, in terms of sharing, they are in the best position to make an appropriate risk assessment, both on whether it's in the public interest, in their particular domain and context, to share, appropriately, and also on whether the appropriate controls have been met. So those decisions rest with data custodians in the first place. It is then for the commissioner. They could review whether they've met the terms and conditions in the act, to do the right thing, ultimately. But, again, what they have done will be on the public record as part of those transparency measures in the bill.

Senator AYRES: Yes, and when I read those submissions, on the one hand, you've got the privacy advocates and the legal advocates, and on the other hand there's an argument that there's an overwhelming public purpose in sharing the kind of data that's contemplated. The problem from their perspective is that the bill is drafted by true believers in the overwhelming public purpose and that it doesn't take into account the privacy concerns in any way approaching that.

Ms Anton: I understand the point, but I would also respond that we have conducted three independent privacy assessments to support the development of the DAT Bill. In each of those privacy impact assessments they provided advice about where we should tighten and improve things. The third and final one, which matches the bill that we presented to you, was conducted by Information Integrity Solutions, which is headed by Malcolm Crompton AM, who is a former privacy commissioner. Angelene Falk, who is the information and privacy commissioner, sits on the National Data Advisory Council. We have worked closely with them on their submissions, and obviously she has made a particular submission to the committee, which I would draw to your attention, which puts her views on the record in terms of the privacy controls that are in the bill. I do note there are some suggestions for improvement in there as well.

Senator AYRES: Is data collected by the COVIDSafe app capable of being shared under this framework?

Ms Anton: No. Two layers of data will be excluded in the bill, just to be clear. The bill itself contemplates data that is not permitted to be shared, and then there will be accompanying regulations about other specific data that will be excluded. The COVIDSafe app data—it's certainly the intention, whether that was in the draft regulations that were released when we were doing the consultation on the bill.

Mr Menzies-McVey: It will be one of the types of data that will be excluded from sharing by regulation.

Ms Anton: Similarly, there are other exemptions around electoral roll data and My Health records as well. We did a consultation process, and when the draft legislation was released for public consultation before it was presented to parliament, there was a set of those regulations publicly available, and there was a list of excluded pieces of data included in that. The final version of that obviously will be settled.

Senator AYRES: I want to come to some of those areas now and just understand what the scope of the prescriptions are, if I can put it that way. The NDIA is currently going through a process, which I think has been the subject of a bit of public discussion, for using data for compliance purposes. What is the relationship between the data sharing that's contemplated by this bill and the compliance regime that the NDIA is proposing to establish?

Ms Anton: On this, Senator, I draw your attention to clause 15, which specifically goes to data-sharing purposes. So it explains what the permitted purposes are, which are those I explained in my opening statement—delivery of government services, informing government policy and programs, and research and development—and I would describe this as thinking about what the patterns of use are. When we do government work it's actually useful to observe patterns. It precludes enforcement related purposes, and clause 15(3) then goes into a recitation of that being about:

- (a) detecting, investigating, prosecuting or punishing:
 - (i) an offence; or
 - (ii) a contravention of a law punishable by a pecuniary penalty;
- (b) detecting, investigating or addressing acts or practices detrimental to public revenue;
- (c) detecting, investigating or remedying serious misconduct;
- (d) conducting surveillance or monitoring, or intelligence gathering ...

That language is there to describe a set of precluded purposes. So I don't see how enforcement action under NDIS would be supported by the bill as drafted. Based on a single-word description—you've characterised it as compliance action—it's intended to preclude that.

Senator AYRES: It's intended to preclude that. What about the kind of information that NDIS participants provide? Is that now capable of being shared across agencies, subject to the processes of the act in a framework?

Ms Anton: I think one of the challenges with principles based legislation—and the PIA went to this—is that it provides signposts, not a specific road map. I think what's always important in these circumstances is to understand what the scenario is and then, going through the flowchart I provided, what the purpose is. You can only do one of those three purposes and you still then have to explain why it's in the public interest to do that. You have then got to go through who we are sharing with, why we are sharing, whether we are sharing the minimum amount of data that they need to do the job that they are contemplating, and, at the end of the day, what the output is. A lot of this is going to be about research. What's the research? What's the output that research might help inform? I guess the point is that it might inform better public policy. If you can look for patterns of use or what's happening, those things might tell you how effectively the program is working. Again, with anything you do, it still needs to be made public that this is what you're doing, and there needs to be an agreement with the data custodian on what the outputs of that research are. It's very hard. This is principles based legislation. It creates those rules in a broad framing, without specific examples. Ultimately, it has to be assessed on a case-by-case basis as to whether this is a sensible thing to do. And, again, the onus ultimately is on data custodians. Data custodians don't have to share, at the end of the day. If they don't think this is a sensible thing to do and they cannot manage the risks then they can make a decision not to share. That can't be overturned by a commissioner suggesting they should, and I think the research sector is a little bit unhappy with us on that design point.

Senator AYRES: That's decisions that public servants made. I'm interested in the data that's been provided by participants in a scheme like the NDIS. Is it possible for the NDIA to use this framework to collect data that is then used to make assessments about the level of support that's provided to individuals?

Ms Anton: I think that goes to individual identified information. The bill contemplates that, where individual information is provided, it's also relevant to make reference to probably the exit clause, which does include a step

where individuals are importantly required to validate that the information there is correct for that to go on and be used for other purposes. So, yes.

Mr Menzies-McVey: And, Senator, where personal information is being shared, the project principle provides—and this is in 16(2)—that the sharing of the personal information of individuals is done with the consent of the individuals, unless it's unreasonable or impractical to obtain their consent. So, if another entity were sharing personal information with NDIA for the purpose of delivery of government services, which I think is what you are contemplating, both the data custodian and NDIA would have to form a view about whether it's appropriate to obtain consent from the individuals concerned. In some cases, the individuals may wish to do that because it would save them providing the same information to NDIA that they have already provided to another government agency, and it might assist service delivery. So it's entirely possible that a consent model could work in that and be quite beneficial to all concerned.

Senator AYRES: But that's what I'm interested in—the relationship between improving government service delivery. In another context, the robodebt scheme was explicitly targeted at government revenue, through a compliance mechanism. If data sharing is used to determine the appropriate level of support for an individual, there's a very close relationship between that and subsequent compliance activity.

Mr Menzies-McVey: At the moment, as Ms Anton said, if NDIA sought to obtain information for a compliance purpose, which I think is the premise of your question, it wouldn't be possible under this bill. They would have to seek that information using one of their existing powers. As you know, most organisations have some capacity to share data already, albeit in limited form, so they would have to negotiate the use of those powers for compliance purposes.

Senator AYRES: Are you saying that this provides a smoother pathway for some purposes? So they are developing a capability, and I want to come to that capability in a moment. But you're saying that this provides for a smoother pathway for some purposes but not all purposes?

Mr Menzies-McVey: That's correct.

Ms Anton: Correct.

Senator AYRES: In the context of another inquiry, the Digital Transformation Agency gave some evidence about the Data Integration Partnership for Australia—\$17 million was allocated to them to do some of that work. There was some evidence of an intensification of resources and activity in data sharing and data integration, with five new units and many hundreds of data analysts employed, including a social health and welfare analytical unit that sits across the Department of Social Services and the Department of Health, and, no doubt, the NDIA and others, and a similar unit in the Department of the Prime Minister and Cabinet to sort of aggregate some of that work at the top level of government. Do you have oversight over those data analytics units or do you have some engagement with them?

Ms Anton: We certainly have some engagement with them. You mentioned the Data Integration Partnership for Australia. We sit within the office of the Prime Minister and cabinet, and that initiative was administered by a branch within a close area of ours within PM&C. So we're certainly attending the same meetings, with regular reporting through, I think, the broader data governance arrangements. There's a deputy secretaries data group, and there was a specific DIPA steering committee on the Data Integration Partnership. We're certainly aware of the work that's happening. Obviously, the development of the bill has been done. I mentioned that point about co-design. We had a number of workshops with the Public Service itself about how we can design the bill in a way that will actually support its functioning, and we have ongoing discussions on many of the technical elements that we're trying to provide in terms of best practice.

In the middle of last year, we released some general guidance for Public Service agencies called The Foundational Four. Clearly, alongside increased data sharing, we need to make efforts to improve the skills and capability of the Public Service, and I think that was essentially what the inquiry into the APS reforms that you were referring to was about. We've certainly provided guidance about what doing data well looks like. The Foundational Four is practical guidance to all agencies about how to lift their skills and capabilities. There is complementary work being done by David Gruen as the head of the APS data profession in terms of lifting the skills and capabilities of individuals. If we're going to make more of data, clearly, we've got more to do with individuals. We have more to do at agency levels with this set of reforms and imagine a consistent set of rules that we can describe for the Public Service about how to share data safely, be it with the act or outside the act. Some time ago, we released the data-sharing principles as general guidance for the Public Service to use. We also released a general data-sharing agreement on how might we embed, in our data-sharing practices, the risk management framework so that we're all doing this in a consistent way. We released a draft of that in COVID. We

will adapt and adjust that to fit the bill, obviously, before we have a final version of that. All of those activities go to as a public service how can we make sure that we are sharing and using data more effectively? Importantly, from those analytics units, what came out of that were good examples about how can we use data more effectively to achieve good public policy outcomes? You may have heard some of that evidence in relation to sort of pharmacovigilance stuff of combining health data to work out where there are adverse impacts, that then can flow into guidance material for doctors to make sure that we are actually having safer health outcomes. The ABS has done good data sharing to support provision of appropriate funding to independent schools, looking at what are the socio-economic needs of different schools—

Senator AYRES: I might just cut in if that's okay because I'm conscious of time. I have two questions about that, I suppose. In the event that the bill is passed unamended, the data commissioner won't have oversight over all of that data integration work. You might collaborate and engage about work but you will only have oversight over the work that is done under the framework that's been contemplated by the bill. Is that right?

Ms Anton: The act contemplates, at clause 42, functions for the data commissioner. The first elements of those relate to, basically, advice, guidance and regulatory functions as set out in the bill. It also does have an advocacy function in clause 42(1)(d) of promoting and understanding the acceptance of the benefits of, and best practice in, sharing and releasing public sector data, and it's safe data handling practices. In essence, because the role of the bill is to say, 'We have got to do this safely and develop ongoing practice', from my point of view, we continue to provide that advocacy and advice in a public sense to the broader public service as well.

Senator AYRES: But it's not the same as oversight. There is a very large program underway and being contemplated by the government. The future Data Commissioner will have oversight of a narrow band of that. You may have an advocacy role and a sort of collaboration engagement role in terms of other parts of the government's work. That work cascades upwards in terms of policy advice through to the Department of the Prime Minister and Cabinet. What are the protections that ensure that that quite powerful data and information is only used for the narrow purpose of policy advice and once it hits ministers' offices and the Prime Minister's Office it isn't used for political purposes?

Ms Anton: The bill complements other avenues that are already authorised for data sharing. Going back to the flow chart I provided you, if data can be shared under existing authorities then agencies are still free to do so. It doesn't displace existing data sharing arrangements that exist in the current legislation nor the activities of departments. The role of the commissioner is to provide an alternative pathway to share with this legislation and, noting your earlier comments about balancing risk and privacy, to make sure that we are managing those risks appropriately. The role is constructed as the regulator of the data sharing system. It's not constructed to look at every piece of advice going to government.

Senator AYRES: The name, the office of the Data Commissioner, sounds awfully like somebody who is in charge of data across the Commonwealth. That's not the case. Have all of the regulations been drafted and tabled? Will the Senate have the advantage of seeing those prior to the legislation proceeding before the Senate?

Mr Menzies-McVey: The regulations obviously can't be made until the act is passed, but we do have a draft of the regulations and we're continuing to work on that draft, refining language in relation to certain parts of data that will be excluded. But we do have a draft of those regulations.

Ms Anton: Yes, and the draft was released alongside the consultation version of the bill. But there have been further refinements to that since then.

Senator AYRES: I'm conscious of time—back to the political officers question. They are exempt from the provisions of the Privacy Act now. What are the additional probity risk issues that you see there with the information provided? With the work that is being contemplated by the bill—data-sharing work and data-matching work, data analytics work—what are the additional risks that you'd see there and what measures have been undertaken to deal with those risks?

Ms Anton: Going back to my earlier comments about the Privacy Act, it does apply and continues to apply to public servants as data custodians. There is a specific Australian government data code that was issued by the Information Commissioner, and all public servants are responsible for meeting their obligations under that code in the exercise of their duties. So that is not negated by the legislation; those obligations still stand.

Mr Menzies-McVey: And, Senator, it would be in the case of personal information. The sort of information that you're talking about, I think, would have been for the purpose of informing government policy and programs, which would very often not require the sharing of personal information, and, if it's not required, then it won't be shared. As I've mentioned previously, the purpose for which the information can be used must be set out in a publicly available data-sharing agreement, and the data-sharing agreement will provide that it cannot be used for

any other purpose. So there is no real capacity for there to be a slippery slope, where it was obtained for one purpose and then used for another, because it will be clear to the public that the data can't be used for that purpose, and that will be backed up by the penalties in the legislation.

Senator AYRES: Chair, I'm done for the moment. I think Senator Kitching might have some questions.

CHAIR: Senator Kitching, I will pass the call to you before we wrap up with these witnesses.

Senator KITCHING: Ms Anton, I think you said there's a lot of data-sharing with the ABS. Is that correct? Did I hear that correctly?

Ms Anton: The ABS has a data lab that is used to support data-sharing. The Australian Institute of Health and Welfare is another of those lead agencies that also do a lot of work on data-sharing, particularly in the area of health research.

Senator KITCHING: Is most of that information de-identified?

Ms Anton: Largely, yes, it will be de-identified information. It depends on the circumstances in which it is being shared. But again, really, what both of those agencies practice is the data-sharing principles as outlined in the bill, and they are doing data minimisation, which goes to that point.

Senator KITCHING: Who else is a lead agency?

Ms Anton: The ABS and the AIHW are the two that I would point to. If you go back to the authorised integrating authorities that I mentioned earlier, they are the agencies that have been, under policy as it currently stands, anointed as having higher skills. I think they also incorporate, at a Commonwealth level, the Australian Institute of Family Studies—and the Department of Social Services, I think. They're the ones that come to mind, off the top of my head.

Senator KITCHING: Are you able to take that on notice and send back to the committee a list of the agencies that are regarded as having higher skills, or however you might identify them?

Ms Anton: Yes, I will send you a list of the Commonwealth agencies who are integrating authorities as it stands. I don't think I've missed anyone, but if we have, we'll certainly let the committee know.

Senator KITCHING: Thank you. You call them—

Ms Anton: Authorised integrating authorities. I will just ask my team if they can send me a list via email while we're still appearing, to try and save us all some time.

Senator KITCHING: That would be very helpful; I would appreciate that. They have better skills than some of the other agencies—is that right?

Ms Anton: They have a higher level of skills, yes.

Senator KITCHING: Are they going to mentor other departments who might be also sharing data?

Ms Anton: Yes. In fact, probably more particularly—I'm just scanning through my bill. The data-sharing principle 16(2)(d) states specifically: 'the data custodian considers using an ADSP—an authorised data service provider—to perform data services in relation to the sharing'. We're envisaging that the integrating authorities transition to authorised data service providers. So the bill actually specifically asks agencies to think about whether they have the skills and capability—

Senator KITCHING: But it's 'they should consider'; it's not mandatory.

Ms Anton: It's not mandatory, but it does require that they consider whether they have the skills and capability to do that. Ultimately, they need to be satisfied that they do. If not, it directs them—

Senator KITCHING: Do you think it should be at a higher level than 'should consider'?

Ms Anton: There are specific requirements in relation to performing data integration under the authorised data service provisions. Paul, have you got the clause?

Mr Menzies-McVey: Clause 29 of the bill allows the minister to determine by rules, which are disallowable instruments, what data services must be performed by an ADSP, which are these entities that are accredited to a higher level. Currently it is likely that the minister will make a rule that will require complex data integration work to be done by an ADSP.

Senator KITCHING: In relation to that, when you say 'the minister', do you mean the minister for each agency that might be sharing data or do you mean—because you're based in PM&C—the Prime Minister?

Mr Menzies-McVey: No, it's the minister responsible.

Ms Anton: The minister responsible for the legislation.

Senator KITCHING: Ms Anton, I like the idea that this information is held in trust on behalf of the public, I think you said. In terms of the public interest, are there positives that you can see in sharing information that benefit the public? Where do you see the benefits?

Ms Anton: If we go to each of the purposes, in terms of government service delivery, the bill contemplates how we support Tell Us Once functionality. If the public have told us something and it's held in silos and we can't share it, wouldn't it be simpler and easier for them if we could actually pick it up and reuse it where they're comfortable with that? Again that goes back to the earlier questions around consent and potential validation. I do think it's about streamlining government services.

It is also about improved public policy outcomes. I described for Senator Ayres the earlier example of data sharing being used to support better allocation of funding to independent schools on a more fair basis. The previous formula, I think, just took an average of the postcode in which the student lived. The ABS was able to work with tax data—this was never seen by the policy agencies—to actually figure out what the income of parents was. In other words, it more accurately assesses their capacity to pay. Using the controls of that expert organisation like the ABS, the product that came out of that was essentially a formula that said, 'This is what the school reasonably needs.' I think those public policy outcomes are really important.

Each of these different areas contemplates more being possible. I mentioned research and development earlier. Work done by one of those analytics units in the Department of Health looked at the different combination of medicines that were taken by people who had a heart issue, and they identified that there was some really bad combinations that led to particular issues for individuals. Again, changing those prescription guidelines led to potentially saving lives, ultimately. So it's certainly possible with all of this that there are more benefits, essentially—to support the Public Service to do their job more effectively and to work with researchers to make sure that we are solving the real problems that Australians are facing today.

Senator KITCHING: With the health data, for example, most of that would be de-identified data?

Ms Anton: Yes. The language we've used in 16(8) in the bill is that data should be minimised, which allows for service delivery, where you do actually need identified data, but equally, if it's about research partners, it is largely about de-identified data.

Senator KITCHING: Where it's not de-identified, can people opt in or opt out? Let's say you're a recipient of a government program like the NDIS or other services. Do you have an option to have your data not included?

Ms Anton: The legislation, in 16(2)(c), contemplates that any sharing of personal information—going back to that identified stuff—of individuals is done with the consent of individuals, unless it is unreasonable or impracticable to seek their consent. That question was raised in, I think, the scrutiny committee, and the response from the minister. Obviously we need to provide some initial guidance on what those circumstances might be. I expect we'd work with the Information Commissioner on that.

Senator KITCHING: You don't have those guidelines drafted now?

Ms Anton: No. We start with the bill and make sure that we've settled that and then work on the—

Senator KITCHING: The reason I ask is that I think it might be quite efficient to have the guidelines as soon as the bill is passed, if that is the case. If it takes a year to get guidelines out, you might have some departments and agencies giving out information or identifying recipients, for example, of government programs. You might have some of that information going out if you don't have the guidelines in place when the bill is passed.

Ms Anton: I understand your caution. Going through the flow chart, in order to use the bill what needs to happen as a very first step is that agencies need to be accredited as users under the bill. So we have to work through the process of accrediting organisations first, and we're working through that guidance material as well. In parallel, side by side with that, we will then work on the guidance material about: 'When you are sharing, these are the rules.' I'm not concerned that agencies could jump the gun and use the bill before they are accredited and they understand their obligations. We will work to make sure that that guidance material lands at the same time so that the scenario you're contemplating does not happen.

Senator KITCHING: That's good. How long do you think it'll take to accredit the agencies with higher skills, let's say?

Ms Anton: We are looking at the transition arrangements we may have in place. The authorised integrating authorities, which I referenced earlier, have already gone through an assessment process.

Senator KITCHING: But with no guidelines. But you're saying—

Ms Anton: Sorry; they have actually had to follow some guidelines.

Senator KITCHING: Can you table those?

Ms Anton: Yes. We're happy to do that. The information that they've had is publicly available. To come back to your earlier question, my team have sent me through an email. The current Commonwealth agencies who are integrating authorities are the Australian Bureau of Statistics, the Australian Institute of Health and Welfare, the Australian Institute of Family Studies and the Department of Social Services.

Senator KITCHING: I have another couple of questions and I'm happy for—I do want to ask about DSS. I think you said before, Ms Anton, that one of the benefits that could come from the DAT bill is the streamlining of government services. Is DSS already doing that? For the sake of time, I'll couple that with another question around—no, actually, can you answer that first. Is DSS already using data to streamline government services?

Ms Anton: The authorised integrating authorities relate back to research purposes. Their current activities are not related to service delivery. In terms of the integrating authority framework that I outlined, that was principally designed around the construction of those complex integrated data assets. That framework didn't link into service delivery in the same way that the bill does.

Senator KITCHING: I'll give you an example. Unfortunately, I sometimes have to put in FOI requests to various departments and agencies, simply because they don't answer the questions I put on notice in the first place. One of the reasons they can give, which under the Freedom of Information Act is a reason, is that it's an unreasonable diversion of resources. What I wouldn't want to see happen is—let's say that you need personal information from recipients of NDIS moneys, and the department decides that it will be an unreasonable diversion of resources to actually ask every single person who is a recipient whether or not they want their data included, even though it's personal to them. How do we overcome that instance, because I can assure you that whatever optimism I had a few years ago has been quelled by the fact that that's how people respond to questions on notice and to FOI. Some of the FOI requests—even though they're approved by the freedom of information commissioner, the department is still not wanting to release information. I think this is actually a much more serious issue, where people might want to have the opportunity not to have their data included, because it is personal data, but the department itself decides that is too much of an effort to ensure that that happens. How do we overcome that?

Ms Anton: That goes to guidance material that we will develop in relation to 16(1) and (2) in terms of that personal information and consent.

Senator KITCHING: Will you outline that a department can't use that, can't say, 'This is going to take too long,' or 'It's going to be too work intensive?' I think people should be given the option about whether their information, their personal information, is shared. The exception for me would be national security reasons; those agencies should have what they need. But in terms of people who may not necessarily be engaged, they receive money from the Department of Social Services but they may wish not to have their information shared, I would hope that the guidance material, which is yet to be produced, doesn't actually give the department an out for asking people.

Mr Menzies-McVey: In his response to the Scrutiny of Bills committee, Minister Robert did undertake to table an addendum to the explanatory memorandum that contains further guidance about the phrase that I think you're concerned about, the 'unreasonable or impracticable', for obtaining consent. That's already on the record, that the minister will provide further guidance about that for the House debate.

Ms Anton: Going back to your earlier point, the other point in this is that it's really important to look at the balance of this, look at where you don't need to share the personally identified information—

Senator KITCHING: Yes, but you've also said, Ms Anton—

Ms Anton: It is not personal information as defined under the Privacy Act; it is just patterns—you're looking for patterns in the research to inform work. In trying to balance those data-sharing principles you can dial up controls in one area and dial down controls in another area. If it is impractical to seek consent from every participant of the NDIS then the counterpoint is that you should strip out personal information so that there is not identifiable stuff in there as well.

Senator KITCHING: The standard will be you have to opt in rather than the other way? In fact, you're not releasing any personal information unless someone consents, rather than the other way around?

Ms Anton: So—

Senator KITCHING: Yes or no?

Ms Anton: It depends. If it relates to service delivery then that is about individuals, and we've made the point in the bill about the exit mechanism and validation. When it comes to individual information then the requirement

in the bill is about minimising that, so the circumstances we would need the identified information would need to be controlled for.

Senator KITCHING: Would you be able to table with this committee the guidance material when you have it? Is that going to be a year away? How long do you think it will be?

Ms Anton: As principles based legislation, our plan was to settle the principles and then work through the guidance material after that. The bill does contemplate for the commissioner to do that in a number of forms. That can be in the form of a data code that can be subject to disallowance or in the form of guidelines that entities must have regard to but are not disallowable instruments. Both of those are contemplated by the bill. At the moment we do need to settle the final form of the legislation. I note that a very early version of the data-sharing principles and guidance was released in 2019 I think, but it didn't contemplate some of these more recent concepts and language in the bill.

Senator KITCHING: I am fully in agreement about research of patterns of movement or whatever, but I'll have a look at the *Hansard* for your response, Ms Anton, in relation to data sharing where people's personal details are identified. I think that they should have control. I think you should have to opt in to that system.

CHAIR: Senator Kitching—

Senator KITCHING: I've finished, Chair.

CHAIR: I was just about to say that I recognise it is very difficult when we are all videoconferencing or teleconferencing. We are quite over time. Are your questions wrapping up there?

Senator KITCHING: I've finished. I will have a look at the *Hansard*. Ms Anton, could you table for the committee any material that you think is going to go to guidelines or guidance material?

CHAIR: Thank you very much, Senator Kitching. I note that a few things were taken on notice in that section. I flag now that the secretariat has advised me that the deadline for answers to questions taken on notice is 22 April, which is two days away. We have a quite tight reporting time frame on this. Before I dismiss these witnesses, I seek agreement of the committee to table the two documents that were emailed to us via the secretariat from the commissioner at the start of the hearing. That is all in order. I thank the officers of the Office of the National Data Commissioner. Thank you very much for your testimony today.

ARNOLD, Dr Bruce Baer, Vice-Chair, Australian Privacy Foundation

BLOEMENDAL, Mr Ian, Chair, Privileges and Immunities Committee, Federal Litigation and Dispute Resolution Section, Law Council of Australia [by video link]

GADIR, Mr Jonathan, Member, New South Wales Council for Civil Liberties [by video link]

GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia [by video link]

MacDONALD, Mr Nathan, Principal Policy Lawyer, Law Council of Australia [by video link]

WONG, Mr Chadwick, Senior Solicitor, Public Interest Advocacy Centre [by video link]

[10:24]

CHAIR: Welcome. I understand that information on parliamentary privilege, the protection of witnesses and giving evidence to Senate committees has been provided to you. I now invite you to make a short opening statement. At the conclusion of your remarks, I will invite members of the committee to ask questions. Does the Public Interest Advocacy Centre have an opening statement?

Mr Wong: Yes. Thank you, Chair and members of the committee, for the invitation to join you. Members of the committee may know that the Public Interest Advocacy Centre is a community legal centre based in Sydney. We provide legal help and undertake systemic policy advocacy on issues that impact, in particular, people who are experiencing disadvantage or are marginalised in society. For decades our work has included work with people experiencing homelessness, people with disability, Aboriginal and Torres Strait Islander people, asylum seekers, and children in care and protection, among others. Our experience in working with these communities has greatly informed our submission to this committee.

PIAC does not oppose in principle appropriate, secure and informed consent based sharing of public sector data for the purposes of improving socio-economic outcomes. But we do not believe this bill provides sufficient safeguards for a data-sharing scheme which represents a fundamental reform to the way in which public sector data is shared and used. We share the concerns that have already been highlighted by the scrutiny committee and by the Parliamentary Joint Committee on Human Rights.

We have made a number of targeted recommendations in our submission to address these structural issues. The recommendations cover three umbrella issues. The first is empowering individuals in the use of their data. That includes strengthening consent requirements, notifying individuals about their data that is being shared, allowing consent to be withdrawn, and creating merits review and complaints processes. The second is ensuring that the data-sharing scheme excludes particularly sensitive matters that should not be captured by this broad scheme. That includes immigration detention medical records and the AFP's access to the scheme. The third is strengthening oversight of data sharing. That includes introducing regular audits by the commissioner, introducing a civil penalty regime for certain data breaches, and publishing a register of efforts to seek consent for the sharing of personal information. I would be happy to discuss these matters further.

CHAIR: Thank you very much, Mr Wong. Do we have an opening statement from the New South Wales Council for Civil Liberties?

Mr Gadir: Yes. Thank you, Chair. Thank you, members of the committee, for the opportunity to appear before you today. I really want to draw the committee's attention to the discrepancy between the ostensible goals of this bill and what it actually allows to occur. This bill is a really big carve-out from the protections of the Privacy Act applying to a very high risk activity of data sharing. This is happening at the same time that another arm of the government is telling us they want to strengthen the Privacy Act. So the term 'public sector data' is really giving the impression that data contemplated by the bill is aggregated statistics of some kind. As you've already heard early today, it does in fact include personal information. And the definition in the bill is far broader than the goals would require, encompassing 'all data collected, created or held by the Commonwealth or on its behalf'. This obviously includes detailed personal information. This kind of information is often intimate and sensitive. It includes information about living arrangements, about relationships, about finances that is disclosed to Centrelink to receive a pension or disclosed to Immigration as part of a visa application. And people are revealing the most intensely intimate parts of their lives right now to Border Force, as they beg for permission to leave the country.

So the broad definition of public sector data is not really the right one for this bill. If this bill is really just to improve service delivery and to inform policymaking and to allow for research, then let's have a definition of public sector data that reflects that. Let's exclude personal information from the definition of public sector data

and say that it must be anonymous. Let's also say that the permitted purposes should not include making administrative decisions that will affect individuals. And, if we aren't excluding personal information, we need notifications to individuals whose data is being shared, we need a public interest test and we need a no harm standard. Basic fairness and civil liberties are really under threat when personal information we are compelled to disclose to a government agency is then spread silently behind the scenes to other agencies or private companies and is able to be used in surprising and unexpected ways.

The Council for Civil Liberties supports the excellent suggestions made by the Joint Parliamentary Committee on Human Rights and in the submission from Melanie Marks and Anna Johnston, which is signed by many privacy professionals.

CHAIR: Thank you very much, Mr Gadir. Does the Australian Privacy Foundation have an opening statement?

Dr Arnold: Yes. Thank you. The Hon. Stuart Robert has promoted the legislation as providing 'strong privacy and security foundations for sharing within government'. It's both deeply regrettable and very unsurprising that the bills do not provide those foundations. The bills reflect the ongoing erosion of Australian privacy law in favour of bureaucratic convenience. The bills are not accompanied by a strengthening of the Office of the Australian Information Commissioner, our regrettably inward looking and grossly under-resourced privacy and FOI watchdog. The bills obfuscate recurrent civil society requests for privacy protection. They do that by Balkanising responsibility, with the new Data Commissioner sitting alongside the information commission and other privacy agencies. Ultimately, requests for privacy protection are not exceptional or inappropriate; they simply reflect the entitlements of people in Europe, Canada and New Zealand, among other locations.

Submissions to this committee and to a wide range of other bodies have highlighted substantive concerns regarding matters such as misplaced trust in de-identification and plans to share data on a population scale with state and territory governments and non-government entities. The committee's time is valuable, so I'm not going to restate those concerns. Instead, I want to call for greater transparency about the sharing. Governments often claim that if you have nothing to hide you have nothing to fear. On that basis, there should be full transparency about government data-sharing programs so that specialists, journalists, courts, ordinary citizens and even Senate committees can hold government to account. If, as Stuart Robert says, governments must share, tell us quickly and comprehensively what is being shared, how it is being shared, why it is being shared and to whom it is being shared. If government cannot walk that talk about trust and about accountability, the bills, I think, should be rejected outright, consistent with the Senate's function as a protection against an overreaching executive. Thank you.

CHAIR: Thank you very much, Dr Arnold. Do we have an opening statement from the Law Council of Australia?

Mr Ganopolsky: Yes. Thank you. The Law Council recognises the importance of facilitating government data-sharing arrangements and the need for the continued improvement of robust policies to govern these arrangements. We are therefore generally supportive of the policy intent behind the bill. However, our submission has identified a number of concerns and areas where we see potential risks associated with the scheme in practice. These primary concerns can be separated into two distinct areas: the adequacy of the privacy protections underpinning the actual scheme; and the proposed abrogation of legal professional privilege, which is of particular importance to our membership. As the committee would be aware, there is a delicate balance to be struck between the collecting and sharing of data and the right to privacy and appropriate safeguards. In this respect, the Law Council reiterates the need for considered, robust and properly resourced oversight mechanisms and safeguards for data sharing in order to uphold the rule of law, to protect privacy and human rights and to ensure the data is shared in a trusted and responsible way.

The adequacy of privacy safeguards under the proposed scheme has been queried by both the Senate Standing Committee for the Scrutiny of Bills and the Parliamentary Joint Committee on Human Rights, as well as through many of the submissions to this committee, including by others represented on the panel today. The Law Council shares many of these concerns and our submission puts forward several recommendations that have been developed to address privacy concerns within the bills should the legislation proceed. Without repeating the recommendations in full, the Law Council has focused on the scope and practical application of the scheme, including four major areas: the resourcing and expertise within the Office of the National Data Commissioner; the need for de-identification to be the default and *prima facie* position prior to any sharing; the need for prior express consent in relation to the sharing of biometric data; and the appropriate accreditation of entities under the proposed schemes.

The privacy concerns are well covered in our submission, as well as by other contributors to this inquiry. But, as the peak body for the legal profession, we wish to focus on our concerns relating to the proposed abrogation of legal professional privilege. I now ask my colleague Ian Bloemendal to speak to these matters.

Mr Bloemendal: Our submissions in relation to client legal privilege, or legal professional privilege as it is also known, can be found at paragraphs 33 to 40 of our written submission. The Law Council is of the view that there is insufficient justification provided in the explanatory memorandum for the proposed abrogation of client legal privilege in clause 105 of the bill. Obviously the EM concedes that legal professional privilege is an important right that ought to be abrogated only where there is strong justification. I think that echoes the High Court's view in *Baker v Campbell*, where Justice Dawson said the proper functioning of our legal system depends upon freedom of communication between lawyers and their clients, which wouldn't exist if one could be compelled to disclose what passed between them for the purpose of giving or receiving legal advice—if that's what this bill proposes to do. We've got a fundamental and basic doctrine of common law that protects confidential communication between lawyers and their clients, which this bill seeks to exorcise. It's not a matter that should be lightly considered or abrogated.

The Law Council opposes this blanket abrogation of legal professional privilege, particularly because it doesn't prevent derivative use. Derivative use, which the bill proposes, would fundamentally undermine any purported protections that the bill might otherwise create. In reality, derivative use would mean that there's no meaningful protection that exists. When I read the explanatory memorandum, at paragraph 527, the justification that is given is that data-scheme entities might obtain legal advice before they enter into data-sharing arrangements, and that might be material to investigations under the clause. Well, many organisations get legal advice on arrangements which they are about to enter into which authorities might find interesting to read and love to read, but that does not give justification for that legal advice should be open to be compelled by a regulator. ASIC and the ACCC, for example, would love to have an ability to read your and my advice that we receive from our lawyers on matters that are the subject of their investigations, but that just doesn't happen. There are multiple High Court authorities which identify why there is a real public interest in the administration of justice, which is there to encourage full and frank disclosure by clients to their lawyers and the reason why a person should be entitled to seek or obtain legal advice in relation to the conduct of their affairs and how that goes.

I'd like to draw your attention, if I could, when you have the opportunity, to paragraphs 34 and 36 of the submission. If legal professional privilege was abrogated, it would effectively preclude an organisation from getting advice about their responsibilities within the DAT regime. They couldn't really get safe advice about the veracity of the conduct of the regulator or advice about the commissioner's conduct, without the risk that that advice would be exposed and compelled, and I doubt that there is a real perceived need for that to occur. In the absence of a compelling explanation of the perceived need to compel privileged information, which is confidential, we submit that proposed section 105 of the bill be omitted. If the provision is to remain for some reason then the Law Council has put forward an alternative approach in our submissions for the consideration of the committee. Thank you for your time. We welcome the opportunity to answer any questions that the committee might have.

CHAIR: Thank you very much to the Law Council for those opening statements. I will hand the call to Senator Ayres.

Senator AYRES: Thanks very much. I'll try and rattle through these efficiently. I might try and direct them to one of you, but I'm very happy to hear contributions from any of you on these questions.

Firstly, you may have been online and heard the discussion with the Data Commissioner. And Dr Arnold is quite right: one of the architects of this legislation, Mr Robert, was also an architect of the robodebt scheme. Aside from an interesting proposal from the Law Council, I think, for de-identification by default, which seems like a quite straightforward proposition, there are a range of—let me ask another question first. I wasn't entirely satisfied that compliance activities were a prohibited purpose for data sharing. What was prohibited was quite narrow in scope—that is, for law enforcement activity for prosecutions. It's not the same as supporting an activity that's trying to determine what level of support an individual is entitled to. Do you accept that compliance activities are outside of the scope of the scheme? Mr Wong first, perhaps?

Mr Wong: Yes. I agree with that concern. I think, in relation to enforcement related purposes, that that particular exclusion is defined by reference to offences, contraventions of law, investigation of matters or practices detrimental to public revenue, serious misconduct et cetera. What we've seen proposed, for example, in the NDIS is around clawing back funds that have been used by participants in ways which the agency considers to be inappropriate. This is still the early stages. We haven't seen what the exposure draft of the law will be, but—at

least from media reporting—that is an example of something which may not be in contravention of the law and may not be captured by the exclusions in the act.

Senator AYRES: There's a real asymmetry to this. There is a building of data-matching and data-sharing capabilities in the public service. I think in evidence that we received in another committee, some [inaudible] in one program. What inequities does that create?

Mr Wong: Sorry, Senator, I missed the question.

Senator AYRES: I'm saying that there's a significant ramping up of data-sharing capability, in terms of the amount of staff and the technology that has been engaged in. How does that change the unseen ways that data sharing is used to formulate policy and approaches to government service delivery?

Mr Wong: I think there are two point there. One is that this is such a fundamental reform to the way in which so-called public sector data is shared that we don't know what the boundaries or the limits will be to the sharing of personal information. We heard from Ms Anton previously that it is largely about de-identified data, but we don't know what personal information will be included, even for research and development. As we're seeing with the proposed changes to the NDIS Act, new changes to law or introductions to existing pieces of legislation may well cover areas for data sharing that are not currently being conceived. That's one issue. It's just the uncertainty about how broad this is.

The second part is this oversight issue, which has been mentioned a number of times now. Ms Anton also emphasised the role of the data custodian, and for clarification that really means the Commonwealth government agency who holds the information. They have outsized power and a level of discretion in determining who gets access to what data, what data can be shared, what data falls within the purposes, whether the data can fall within the purpose of improving government policy or research and development, which can be very broadly interpreted, as well as whether it's unreasonable or impracticable to seek consent and, then, the circumstances in which that data is shared and to which agencies they might share that information. So, theoretically or hypothetically, if information is being sought by the National Disability Insurance Agency from, say, the tax office, Centrelink or whichever other compliance agency they want information from, the agency that will decide whether to share that information will be another Commonwealth government agency. There really isn't any form of oversight in that sharing and there are no merits review processes.

There are two issues there, in summary. One is the unknowable limit or boundaries of the information being shared, and the other is the lack of oversight in the discretion that the data custodian has.

Senator AYRES: Are there any other responses from the panel? Is there anything else you want to convey to us about those issues?

Mr Gadir: I also want to highlight the question posed by the Committee on Human Rights, which is: why is the Australian Federal Police, which is a law enforcement body, not listed as an excluded entity? Also, as Mr Wong mentioned, when you have regulators that are going to be underresourced, we can't rely on them to be the only protection mechanism. We have to make sure that the words in the bill reflect what the government is saying is the goal, and I'm not satisfied that the words in the bill do that.

Senator AYRES: Dr Arnold, it was you, I think, in your opening statement who talked about transparency, in terms of people outside being able to look in and citizens being able to observe what kind of data-sharing arrangements are in scope.

Dr Arnold: Yes.

Senator AYRES: How, in your view, would that be effected and how would that improve the scheme?

Dr Arnold: For starters, a range of stakeholders would be able to see what's actually happening, and the legislation really provides very little transparency. We're very much relying on individual agencies doing the right thing. Individual agencies may well have very different views about what's appropriate and what's not. The notion of consent here, with respect, is just a nonsense. We have nice language that government agencies will be custodians. Having worked in the Public Service, talking to public servants, talking to consultants who work for the Public Service and talking to students who are public servants—they regard this data as their data: 'It's government data. We can do with it what we like.' We will in practice have very weak oversight of what's happening.

Something that is very importantly and that often isn't picked up is that, when we look at the history of privacy legislation in Australia, or privacy regimes in Australia—and possibly my irritation, having provided submissions to committees over the last 20 years or so, is reflected in my tone today—what we see is that we start off with lovely motherhood statements from people like Stuart Robert: 'It will be good. It's in the national interest. You

don't need to worry. Trust us.' But over time we see a creep; we see an erosion. We may start off, potentially, with this legislation, which doesn't look too bad, but over time it will be weakened. It's opened up to a range of bodies that we would consider to be inappropriate and it's opened up to uses which we would consider to be inappropriate—uses which are administratively convenient but possibly punitive.

Senator AYRES: Thank you, and thank you to the Law Council for your submission. I did have some questions about legal professional privilege, but, Mr Bloemendal, I think you've covered that issue for us neatly. I have a couple of specific questions. In your submission you deal with biometric data. What are the particular concerns about that question?

Ms Ganopolsky: I'll address the biometric data point. There are two questions that arise on the use of biometric data. One is the very breadth of what is biometric data, leaving aside the legal definition. These are immutable characteristics that go to each individual. Importantly for us, as lawyers, they are characteristics that cannot be changed, unlike a password or some other mathematically produced identifier. The second issue arises in that the Privacy Act has defined 'biometric data' in a very limited way. There were good policy reasons for that back in the day when the legislation was drafted.

The answer really sits in the definition of what is sensitive information. That includes the two types of biometric data, and those types are very narrow. We broaden that explanation in the submission we provided, from paragraph 73 onwards. Essentially, what the definitions within the Privacy Act do is limit the type of biometric data to data used to identify individuals, not any other form of biometric data, and to biometric templates, which are a very specific, mathematical representation of biometric data. That's it. That's included in sensitive information, and sensitive information commands a high level of protection. You have already seen some discussions about that and how APP 6 distinguishes between health information and sensitive information when it comes to protection, requiring higher consent standards and higher transparency. If you were to leave the definition of biometric data as it is in the Privacy Act, you would lock it in to those two types of biometric data and leave everything else to be simply another creature of identifying information, where it's identifiable. That's the technical problem with how the two regimes collide. Does that address the question?

Senator AYRES: Yes, it does; thank you. This question is for any of you: where does the bill intersect with Australia's international human rights obligations, and in what sense do you say that it's deficient?

Mr Gadir: I'm not an expert on international human rights. Earlier the witnesses from the government were explaining how the Privacy Act would continue to apply, but that is not correct. The fundamental disclosure from the government agency to some private company that would be enabled by this bill is actually a carve-out from Australian privacy principle 6. That's a basic part of the international human rights framework. What does that APP6 say? It says you only use or disclose personal information where it's reasonably expected by the individual and it's related to the primary purpose of collection. I would say, and perhaps the professor can confirm this, that would be a breach of the international human rights concept of privacy.

Senator AYRES: Are there any other observations about that, more broadly? I want to come to privacy in a moment.

Dr Arnold: We're largely talking about an aspirational regime here. It's not judicially enforceable. A range of civil society—I think including the Law Council, over many years—have suggested that Australia needs to introduce a statutory cause of action, regarding an egregious innovation of privacy. Basically, you need individuals whose privacy has been disregarded and legal power to do something about it—and when we look at the history of entities such as the Office of the Australian Information Commissioner, it's misplaced trust, alas—rather than trusting that the privacy commissioner will somehow come to the rescue.

Senator AYRES: There's a review of the privacy framework being undertaken, at the moment. I see that from each of the organisations there are a range of suggestions or recommendations about how the bill might be improved, in terms of privacy. Just as a preliminary issue, is there a problem with this bill proceeding in advance of that review being concluded and considered?

Dr Arnold: With respect, I think the bill should not be passed until we've looked at and, ultimately, fixed the existing weak regime. The bill is being driven by institutional imperatives, with political convenience, without any regard for human rights.

Senator AYRES: Are there any alternative views to that? I'd be surprised if the Australian Privacy Foundation said anything else. Are there any other views to that about the merits of proceeding prior to that review process concluding?

Ms Ganopolsky : I'd like to make a suggestion, from a legal perspective. There is a risk that you are putting the cart before the horse. What is contemplated under this bill is a very large data-sharing arrangement that will be

systemic in nature. What is contemplated under the review of the Privacy Act is, potentially, an overhaul of the regime, including higher sanctions and higher levels of intrusions and different rights and causes of action that would form part and parcel of our privacy regime. So, from the point of view of building a series of infrastructure, you are, potentially, putting the cart before the horse in that it will have to respond to a brand new regime. That's a kind of legislative risk that's there.

If I can round off, again, from a purely legal perspective, the fundamental difficulty that cuts across the discussion here from a privacy perspective is that, at least retrospectively, the data that's already been collected has largely been collected through the forces of interaction with government. Sometimes it's by force, sometimes it's by implied interaction. It's very difficult to cure that without a substantive systematic approach to that very question. That's why the question of de-identification has received so much attention. Out of all of the suggestions at the legal level, that is probably the one that comes closest to addressing that very fundamental question of what you do with the existing data that's been collected under the existing regime with existing expectations.

The current language of APP6 really talks to that as an existing dataset. So unlocking that, even with the best intention, is conceptually and operationally a very hard thing to do without committing to a form of de-identification. Bringing it back to the legal question, without putting de-identification as a *prima facie* legal obligation, you're not making much progress in that very structural conflict that one needs to address very expressly.

Senator AYRES: There's a sort of blizzard of proposals on privacy. Does de-identification of itself substantially resolve the concerns that are motivating the other recommendations? Does it partly do it, does it wholly do it or is it not a substantial enough amendment to the legislation itself to support the passage of the legislation through the Senate?

Ms Ganopolsky: From a legal point of view, it substantially doesn't, because from a privacy perspective—obviously provided identification is effective—it removes the dataset from an ability to identify individuals, so it takes away the privacy risks entirely. Actually, it takes away the privacy regime entirely, because, if the data is genuinely de-identified, it is not information about individuals, and the rights and freedoms of individuals are not impacted by the data. The reason it contains such power is that not only does it deal with information that's actually collected as part of the interactions individuals have with government but it deals with information that the government generates, and that is a very protective position both for the information for the government entities that are interacting and exchanging data and, clearly, for the individuals. So it's a very powerful control, hence the recommendation to legislate for it, rather than leave it at that operational level.

Senator AYRES: The policy objectives that are set out—the three: supporting government service delivery, policy development and whatever the other one was—don't require identification to the individual level, do they?

Ms Ganopolsky: No.

Senator AYRES: They might require certainly geography and a range of other characteristics but not individual identification.

Ms Ganopolsky: In fact, that's the opposite of what they require. They require trends, they require functions and they require a level of analysis that shows community behaviour, not individual behaviour, so it's a complementary approach to the very objectives as set.

Senator AYRES: One final question: is there a view from the panel about whether the bill is actually capable of amendment to deal with these proposed amendments, particularly around the privacy issue, or is it a back to the drawing board kind of operation?

Ms Ganopolsky: Is that a question to the Law Council?

Senator AYRES: Let's start with you, yes.

Ms Ganopolsky: The Law Council thinks that the bill is salvageable if the recommendations are addressed and both the substantive and the draft points are met, and that includes the privacy point and clearly the privilege issue that has already been raised and aired.

Mr Wong: From PIAC's perspective, there also needs to be a fundamental reconsideration of the intention of this legislation. It's cutting both ways in the sense that government services' first purpose is intended to require personal information, because that is where the government is seeking to share personal information between different agencies potentially to ensure that someone doesn't need to provide their information three times to three different agencies—that seems to be one of the intentions. You've also coupled that with research and development, which, as Ms Anton said, is largely about de-identified data. They are two entirely different

purposes, and I would submit that you can't really capture them both in the same piece of legislation, especially if one of the proposals is to de-identified data.

Senator, I might come back to, briefly, your earlier point about privacy rights and international human rights law. The other point to flag there is that we haven't seen what particularly sensitive data will be excluded from this regime. There was an exposure draft of the proposed regulations which excluded things like health: My Health Record. One of the concerns we raised as PIAC was that it didn't include immigration detention health records. The health data of asylum seekers and refugees is covered by the Migration Act, not by these other processes. Without knowing what sort data is excluded from the bill we don't know what other privacy rights under international law are also raised. For instance, under the Convention on the Rights of Persons with Disabilities there are particular provisions around protection of their health and medical records—for obvious reasons they're particularly sensitive. Without seeing the full suite of regulations and guidelines it's very difficult to comment on that. I know that Ms Anton was saying that there's a process in place where you look at the legislation first before moving onto the regulations et cetera. But I think what we need is the full package of proposed reforms before we're able to comment on some of these privacy issues.

Mr Arnold: Yes, I would agree with that.

Senator AYRES: Thank you all for your submissions in the discussion today. Thanks, Chair, I am done.

CHAIR: Thank you, Senator Ayres. I don't believe there are any other questions from committee members. We will send these witnesses off with thanks for your testimony here today, for making the time and apologies for running a little bit late. We're rapidly catching up time.

HAYTHORNTHWAITE, Dr Adele, Research Data Consulting Lead, Sydney Informatics Hub, The University of Sydney [by video link]

PAYNE, Mr Tim, Director, Higher Education Policy and Projects, Office of the Vice-Chancellor and Principal, The University of Sydney [by video link]

[11:06]

CHAIR: Welcome. Information on parliamentary privilege and the protection of witnesses and giving evidence to Senate committees has been provided to you. I now invite you to make a short opening statement. At the conclusion of your remarks I will invite members of the committee to ask questions.

Mr Payne: Thank you, Chair, for the invitation to participate in today's hearing. The University of Sydney's interest in these bills stems from our desire to help achieve a better framework governing how Australian researchers access data held by Commonwealth agencies. This is important so that research with the potential to deliver benefits for the community can be conducted in a timely fashion with robust safeguards to protect against privacy and national security breaches. Currently our researchers often report enormous variability across Commonwealth agencies around the rules governing access to datasets for research purposes. We have examples of Commonwealth funded research grants expiring because datasets could not be accessed within three years. Other researchers have preferred to source data from overseas, rather than try to obtain it from Commonwealth agencies.

We commend the Office of the National Data Commissioner for the exemplary public consultations that they have run over the last three years while developing this legislation. As a result the bills are thoughtfully designed and carefully drafted. We strongly support the aims of the legislation but believe there remains some areas where the parliament could improve it further.

We've noted the concerns raised today by other stakeholders about the adequacy of privacy protections and agree these issues are critically important. A key concern to the university is the absence of a definition for the term 'public benefit' in the main bill, even though data custodians across the Commonwealth will be required to apply this test each time they consider a request for data. If research in the public benefit cannot be easily and consistently identified by data custodians we fear that there will still be unnecessary time delays and potential for poor and inconsistent decision-making. We therefore believe that a review mechanism needs to be included for decisions to reject data requests for research intended for public benefit. We also recommend that departmental data custodians be required to report regularly on all data requests received and their outcomes.

It is difficult for us at present to gauge the full impact that the legislation will have on universities and other not-for-profit research institutions. We strongly recommend against the charging of fees for accessing data for research undertaken by public-funded research institutions. We're concerned about the compliance costs that public research organisations will incur due to the accreditation requirements the legislation will create. We therefore recommend that an advisory panel including research sector representatives be built into the legislation for the first three years to help co-design the governance and the legislation's rollout.

We believe this legislation presents a rare opportunity for the parliament to establish a single coherent system for the sharing of Commonwealth datasets for research purposes that will benefit all Australians. We are confident that our remaining concerns can be addressed if the government commits to ongoing consultation and co-design, with inputs from experts representing the research sector. I'm happy to take questions.

CHAIR: Thank you very much, Mr Payne. I might start off. I note that you're from the University of Sydney, so I might ask questions relevant to the University of Sydney but then more broadly, if you can answer. How is your university positioned in relation to preventing cybersecurity breaches where hackers may seek to access or steal sensitive data?

Dr Haythornthwaite: I can take that. I do not work in information technology but I work closely with our representatives there and with cybersecurity. We have a concerted program that is addressing cybersecurity risk, as all other research institutions in Australia are doing. We are in a constant state of improving those. We are taking part in the review of critical infrastructure that's currently underway at the moment, with the legislation there, to put in even more robust risk governance frameworks to address cybersecurity risks. We have a dedicated information security officer and a team of cybersecurity analysts who stay abreast of the current developments in the cyberworld. As you're aware, it's a current state of escalation and there are always new threats to be identified. To date we have managed to have very good cybersecurity governance of our systems; that includes our administrative systems as well as our research systems.

Mr Payne: I can add that we have reported in detail on our efforts in these areas in another submission recently, in relation to foreign interference. The university is also required to report through its compact agreement with the federal government, as are all universities about their approaches to foreign interference, as part of that cybersecurity.

CHAIR: I'm not sure whether or not you were tuning in earlier in the day but I raised a few concerns about exactly what you just spoke about, regarding foreign interference at universities, with the National Data Commissioner—hence these questions to you now. Do you think your researchers being provided with access to this sort of data, which previously wasn't being released by the government, might provide an incentive for cybercriminals or foreign actors to target universities for cyberincursions? If that is a risk you've identified, what is your university doing to combat that?

Mr Payne: Firstly we would say that the data that would be accessed through this act is largely data that is already accessible. The difference is that it's not accessible through a common framework. Different rules and processes and policies apply in different agencies. What we like about this bill—and, I must say, the university has been involved with the process for the last five years; I think we have made six or seven submissions on this since the Productivity Commission did its review of data availability and use in 2017—is the consistency that it brings. We like the fact that there are high standards set for third-party data agents and also for accredited research institutions such as the university. Under this legislation each public research institution would have to become accredited, and then it becomes our responsibility to make sure that all of our researchers and research students are aware of the standards and the expectations; these are set out in a standard form data-sharing agreement which can be adapted for each agency. It would just bring so much more consistency.

The National Data Commissioner has also looked very carefully at best practice in other jurisdictions to see how they are doing it. We also have the experience in New South Wales of working very closely with the New South Wales government, which has made data sharing for public benefit a huge focus. We have researchers doing lots of research with datasets. In relation to transport, last week one of our start-up companies in quantum control signed an agreement with the New South Wales department of transport to do analysis of data in real time using quantum technology, potentially, to improve the allocation of resources across the New South Wales transport network.

CHAIR: Mr Payne, you just said that, through this framework, the onus will be on universities to ensure they clearly set the standards and expectations of their researchers or their students that might be accessing data under this scheme. Does the University of Sydney have even a vague idea of what that compliance framework is going to look like internally, and how that framework will be continually monitored to make sure that data, once it goes from government to a university, is being used for the purpose for which it was originally accessed—that it's not getting into the hands of people who shouldn't be accessing it?

Mr Payne: That goes to one of the recommendations we've made about the need for ongoing engagement between the data commissioner and the research community. Potentially this could link into the work of the University Foreign Interference Taskforce. At the University of Sydney we have robust mechanisms for ensuring compliance with legislation and that we will go through our normal processes to comply. We are concerned about the costs of compliance—there is no funding provided for research institutions here—but we'll just have to cope with that. There are already costs involved in complying with the processes. Our training will be upgraded. All research requires ethics approval if it involves human or animal datasets; Dr Haythornthwaite can talk in more detail about that. Perhaps what's missing at the moment is a national framework for ensuring there are consistently robust approaches taken across the whole of the sector.

Dr Haythornthwaite: I agree. We deal with a lot of sensitive data as part of our normal research activity. We have systems and classifications of data rated to those systems available to all researchers, and we have a lot of outreach in education and policy to ensure that researchers are aware of the resources they have and their obligations to protect the data they are working with. There is also the national research code, which they all comply with, which is also a condition of their employment at the university. As Mr Payne said, all research that involves human subjects has to have the approval of the human research ethics committee from our university or from data providers who release the data to us. We also have contractual obligations on datasets that are shared with us by government and other third parties, and there are very strong stipulations on what you can and cannot do with the data within those research contracts.

CHAIR: Finally, can you provide some examples of how greater access to data would be beneficial for researchers and perhaps the nation more broadly, considering how that research might impact our lives?

Dr Haythornthwaite: There are many examples we could give in the health and social sectors. Some of the great value that we get from these research data sets is when you combine them and you link them to actually be

able to address much broader and deeper questions than you would through just single data sets. For example, we have epidemiologists working at the university who are able to combine data sets from births, deaths and marriages registries with maternal health and fetal health outcomes and also early education outcomes to be able to come up with policy initiatives that help children with developmental issues in early childhood. Mr Payne has also given examples of how we can combine transport data with quantum computing to be able to give a better method of running transport systems and getting increased efficiencies. There are any number of different research questions that could be answered if the data was available. What we must do is balance the public benefit of acquiring that data and conducting that research with the privacy considerations that we all agree are very important and getting that balance right and getting a workable framework that means that we don't get bottlenecks every time we try to link data sets because it's just too hard getting data from data custodians.

CHAIR: Thank you very much for your responses to my questions. I will now handball to Senator Ayres.

Senator AYRES: There is just one question from me really, which I can't promise won't lead to others, but we'll see how we go. One of the challenges in this bill is that it deals with data being used for different purposes. In terms of data being provided to research institutions, you may have heard the discussion we had in the previous panel about a proposal that the presumption be for data to be de-identified. Are there circumstances in which research institutions like the University of Sydney would require data to identify individuals or is it all essentially de-identified data that you're using when you're engaging with government departments about data use?

Dr Haythornthwaite: We believe that data should be minimised wherever possible and that you only use the degree of sensitivity of data that you actually need to answer the research question. So, wherever possible, we recommend that the data should be anonymised or aggregated in some way to remove any risk of identity. However, when you're linking different data sets, then you need to link using common identifiers. The best way of doing this is to use a third party such as the current integrating authorities or the proposed accredited data service providers, to provide a secure service to link those data sets together, using a common identifier, and then to remove those identifiers before they give them to the researchers. That way, the research institutions do not have to work with identified data. We're very keen to encourage that wherever possible.

Senator AYRES: So, in the way that you envisage this working, when the data arrives with you, it's anonymised, but of course to do data integration or data-matching work it requires some identifiers.

Dr Haythornthwaite: This is one of the problems at the moment. Because there are very few integrating authorities, there are very large bottlenecks, because the integrating work is specialised. At the moment, you need to get permission and ethics approval from each data supplier linking into that process. So, if I were to link three datasets together, I would have to get three lots of permission from three different data custodians and three lots of ethics committee approvals, probably, to be able to do that. That all takes a long time, and then the integrating authority would link those together. One of the major benefits we see in the legislation as proposed is to provide a smoother running of this particular part of the framework so that these long delays are avoided.

Senator AYRES: Public sector resources would be doing the data integration work and engaging with the research institution that's requesting it, but the data would then be provided to you in a way that allows you to complete the research program. At the moment, there's data-matching work that's going on within universities with separate permissions from separate owners of datasets.

Dr Haythornthwaite: Most of the data matching is currently happening through integrating authorities.

Senator AYRES: Thank you for your submission. I'm done, Chair.

CHAIR: Thank you very much for your economy of time, Senator Ayres, and thank you to the University of Sydney for your submission and for appearing today. We will send you off with our thanks.

KRAHULCOVA, Ms Lucie, Executive Director, Digital Rights Watch Inc. [by video link]

WARREN, Mr Justin, Board Member, Electronic Frontiers Australia Inc. [by video link]

[11:26]

CHAIR: I welcome representatives from Digital Rights Watch and Electronic Frontiers Australia. Information on parliamentary privilege and the protection of witnesses in giving evidence to Senate committees has been provided to you. I now invite you to make a short opening statement and, at the conclusion of your remarks, I'll invite members of the committee to ask questions.

Mr Warren: Thank you, Chair and committee members, for the opportunity to speak today. Good intent is just a start. There is some good intent behind this legislation, and there are some potential benefits, such as only having to provide information to the government once instead of saying the same thing dozens of times to different people. Good intentions, while necessary, are not sufficient, and there are myriad reasons to be concerned about this legislation and the approach taken to creating it.

The government demands to be trusted without first demonstrating that it is trustworthy. In fact, it has done quite the opposite. The list of failures is long. In 2016 the government published a trove of Medicare data, the MBS/PBS dataset, only to pull it offline after experts pointed out they could re-identify people in that dataset. There has been some discussion about de-identification today, so that's particularly important, I think. The government response was to try to outlaw pointing out the problem, not to stop it from happening in the first place. In 2017, Centrelink provided private personal information about a payments recipient to a journalist in order to 'correct the record' in what was widely viewed as retaliation designed to silence a critic. In 2020, only a year ago, Service NSW leaked 738 gigabytes of data including personal information of 186,000 people. That was a data breach.

Then there was the entire robodebt saga, which has already been canvassed here today, in which the government unlawfully took money from hundreds of thousands of people after a laughably ham-fisted data-matching exercise and, for years on end, continued to insist that everything it was doing was fine. It was not fine. It took a private class action to force the government to stop.

The government demands that we consent to this, yet we can't say no. It's illegal to not complete the census or to fail to file tax returns. If we want access to society's services, which is, after all, the actual point of having a government in the first place, we have to provide personal information before we can do so. We have Medicare cards, drivers licences and all manner of forms to fill out, and we may have done so gladly, based on a bargain that we made in the past. My drivers licence photo was taken over a decade ago, when I still had hair. I allowed for my photo to be taken so I could drive on the public roads—a fair bargain—but then that photo was uploaded to a central database for other purposes, like facial recognition, that I didn't sign up for and never said was okay. We had a deal and now, after the government has already collected all of this private personal information about us, you tell us that you are altering the deal, some like bureaucratic Darth Vader. That might pass for consent in ministerial offices in Parliament House, but it doesn't out here in the real world.

We're asking for governments to do more to protect our privacy, and we have for decades. We keep asking for more protections from the likes of Google and Facebook, but the government seems focused instead on turning itself into Facebook. When the government gets it wrong we have essentially no recourse. Like a bad boyfriend, time and time again you just keep promising that this time it will be different; this time you will change. We want to know what happens if you fail again, just like all the other times before. We're the ones who get hurt, not you. All you offer is a chance to hurt us again and you won't let us leave. That concludes my statement.

CHAIR: Thank you very much. Digital Rights Watch, please?

Ms Krahulcova: Thank you for inviting us to speak on these bills and their impact on digital rights. We appreciate this opportunity. For those unfamiliar, Digital Rights Watch advocates for free and open internet, democratic accountability, and individual rights and freedoms in the digital era. As such we have consulted and contributed to dozens of parliamentary hearings on everything from telecommunications privacy reform to most recently the media bargaining code. We see great overlap in all this work that we do, and that's why I bring it up, and that is the act of reshaping the relationship between government and individuals. I think there is a shift in responsibility and a shift in accountability across all these fields, and we're extremely concerned about that direction.

In the interests of the committee's time—and I want to give time for questions—I won't repeat the submission, but I will reiterate for those tuning in that there is a Privacy Act review currently underway and it aims to bring Australia in line with international data protection and privacy standards in part so that trade and ecommerce can

continue, privacy decisions can be handed out and we can continue being a relevant international partner. It does not make I think policy sense or financial sense to be passing this legislation while money is being spent reviewing the Privacy Act, especially if this legislation as primary legislation will be exempt from the resulting rules and standards in that review.

In fact, the proposal as it is is even rewriting existing privacy principles. In our submission we brought up the fact that privacy principle 6 is essentially being rewritten, and that is the primary [inaudible] definition. There are exceptions to that in that the existing privacy principles, but this is a top-down override of privacy principle 6 and it is a blunt approach that dilutes legal protections and remedies currently available to Australians, and there are not many to begin with.

The bill also does not require specific testing against competing public interest claims, and I think that's important to privacy [inaudible]. There is a need for 'a description of how the public interest is served by the sharing'. There's no need to actually balance competing public interests. I think that's important because you can also make a [inaudible] case for something but it's much different when you do a calculation. I would say that that's insufficient.

Further, I'm concerned about the impracticable clause to obtain consent. I think that has been brought up before today. It's almost absurd because it will never be practicable to obtain consent at that level. I was working in Brussels for several years for another NGO called Access Now. I remember when the GDPR was implemented. What happened was not practical. Everyone was [inaudible] by a variety of emails [inaudible] consent to different data-sharing purposes. [inaudible] by email for government services. That was not practical, but it was an interesting and important exercise that highlighted to people exactly where their data was and what purposes their data was shared for. Using that language already doesn't set this up, I think, as a timely legislative update.

That brings me to a point on research I want to highlight. We went into it in our submission a lot, so I won't go into the details. I'm super happy to speak about what GDPR has done, in that regard, in Europe. We don't want to copy and paste here but there are some important protections for data sharing that GDPR introduces. We want evidence based public policy. That's incredibly important and benefits society at large, especially given the sensitive nature of data held by government agencies, specifically the ones mentioned that handle incredibly private personal information. But it's paramount that the bill tightens up its provision to ensure that the data is secure and individual privacy remains protected and all the data remains anonymised.

We have seen cases where security researchers have been able to de-anonymise data that has been leaked in Australia and there has been very little done by the government. There's really no mechanism for this sort of research to be turned into action and for changes to be made on the basis of it. Now, largely, those sorts of studies are ignored and that's an incredible problem. As Justin pointed out before me, and I would agree with everything he said, there are a lot of examples where leaks have happened and privacy of individuals was not sufficiently protected. In most of these instances, individuals have no redress or compensation by the government, and I think that is a broken system.

Lastly, I would like to raise this issue of the bill allowing for data sharing for enforcement purposes. That's something that's been brought up as 'It won't happen; it can't happen.' In our submission, we find that there have been some word changes in 15(4). I'm happy to discuss that, but we must be absolutely sure that (a) no such gaps in legislation exist and (b) we don't preclude any protections that come from the Privacy Act review through this legislation.

As things become digital, it's imperative that we examine the role and relationship between government as an entity that provides governance, security and services and individuals as [inaudible] that entity and what that relationship should be. Looking at this from a strictly value based type of calculation, which is what data sharing often [inaudible] and it's something that consumer data rights, for instance, also does, it does not paint a complete picture. I would argue that it's imperative that we take a principle based approach to data governance or we risk reducing individual lives to numbers and a bottom line. I think that creates a real issue for democratic governments. I'm happy to answer any questions. I hope that was helpful.

CHAIR: Thank you very much. That was very insightful. I have a couple of questions before I pass to the deputy chair. This is probably one for Ms Krahulcova. It doesn't, necessarily, go to exactly what you just talked about but I'm interested in your thoughts. Once we've granted access to data to these third parties, do you have any concerns about how that data might be accessed beyond that third party, whether it's through a cybersecurity incursion or through hacking or something like that?

Ms Krahulcova: By third party do you mean by entities or—

CHAIR: Once government data has been provided to a third party, under the legislation that we're talking about here today do you have any concerns around oversight of how that third party deals with that data, in terms of potential cybersecurity attacks, hacking and that sort of thing?

Ms Krahulcova: Yes, absolutely. What we elaborated on in our submission, on this point, was also that there's no required ethics test even for sharing with certain research institutions and private entities. I know that we have representatives here from the University of Sydney and I know some of the bigger institutions have that sort of mechanism for any studies they do. That's not always the case, and I think the legislation should be very clear about what its expectations are because, yes, you're really losing sight of that data. I would argue that, as its primary custodian, you have a responsibility to people to understand just how that data might be used and how that makes them vulnerable.

I would also flag that a lot of the time when datasets get cross-referenced and big databases are created, that creates a honey pot. If that's a foreign concept, it just means it creates a really lucrative opportunity where a lot of data on individuals is interlinked. We've seen in previous iterations where in South Korea, for instance, the central government database that they created was taken offline a few weeks later because it was subject to so many cyberattacks. People were just wanting to hack it and get that information because it linked people's social security numbers, or whatever their equivalent is, with names and birthdays. It just makes identity theft incredibly easy, as well as understanding the population at large.

CHAIR: Thank you very much. I have a question regarding the census. Both submissions reference census data as an example of information that Australians may not be comfortable having shared with third parties. Do you think there's any risk that people will be less likely to complete the census this year if they're concerned about the privacy of that data?

Mr Warren: Yes, we already know that to be true based on the last census. There was a lot of controversy at the time, you may recall, regarding the linkage of names and addresses in order to create a longitudinal dataset from multiple censuses, rather than the census being an individual snapshot of data from that particular time. There were a lot of people who were very concerned and who publicly stated they would not complete the census at that time because of that perceived risk. The perceived risk from this kind of data-sharing of essentially the entire dataset is vastly greater than that. So, yes, we would absolutely see a chilling effect, particularly for people who have a memory of what governments have done with census data in the past. Some of those will be fresh memories, because they have escaped those regimes to come here to Australia, where they believe that kind of thing doesn't happen.

Ms Krahulcova: I would just add that in January last year there was a consultation conducted by the Australian Bureau of Statistics that actually explored integrating private datasets as a way to fix the census. What they were proposing was actually taking the aggregate census data, and taking data mainly from something like the electrical grid, to patchwork and fix them to the households where the answers were incomplete or flawed. There was a huge privacy impact assessment that happened on the back of that. Ultimately, they agreed it's not a good idea because it will erode the trust that people have and the social contract that a census operates under. It's very lucrative, and, from a purely financial or efficiency standpoint, it makes total sense. In effect, you wouldn't have to have a census; you could just pull everybody's electricity usage data and paint a very clear picture. But there's a reason that's not what we do, and there's a reason that the census is held the way it is, because you need participation and you're legally obligated to participate. I 100 per cent agree with Justin that, yes, that would erode people's trust in that mechanism.

CHAIR: Thank you very much for that response. Senator Ayres, I will hand over to you.

Senator AYRES: Thanks very much. Ms Krahulcova, in your opening statement you referred to the compliance enforcement question, and changes that you say happened in the draft that haven't resolved your concerns about that. There's a lot of public interest in both the robodebt context and the emerging issues around data-matching being used for compliance with the NDIA. What do you have to say about that? Could you expand on your opening comments about that issue?

Ms Krahulcova: As to why data shouldn't be used in those ways?

Senator AYRES: In what sense do you think this smooths the path for that kind of data-matching activity for compliance purposes?

Ms Krahulcova: I think Justin might want to add to this as well. I think the overly broad intent of this bill and the description of how public interest is served by the sharing—you can make a hundred different cases across a lot of agencies that public interest would be served by sharing the data. That's why I think that test is insufficient. Just because something is well-intentioned or would serve public good in a very narrow view doesn't mean that it

should be done. There are also limits, and many data scientists will be able to tell you of the sort of data that you're able to aggregate. A lot of NGOs have done research like this. Privacy International was one of them. They actually showed that data aggregated through social media services, which ends up with targeted advertising, political advertising et cetera, is actually an incredibly flawed and incomplete picture of who you are. We over-trust and over-rely on data, because there are a lot of consultancies who have a very big financial stake in making that narrative stick. So we over-trust and over-rely on this when it's creating really imperfect pictures of people's lives. At a human level, I think it's cruel to rely on the numbers and merge datasets to paint people's lives in those instances. Justin?

Mr Warren: Yes. To expand further on the point, the legislation as drafted is about intent. There are some loopholes in part D that have been added in there as well about sole purpose. There are certain things where there is a dual purpose. There are some quite convenient loopholes in there that I could very easily craft an argument to drive through, so they should definitely be removed, which was in our submission. But there's good intent here, in that we want to do something which sounds beneficial. That may be true when the actual intention matches the stated intention. That is not always true. Sometimes humans lie. Any safe system needs to be designed to take that into account, because the purpose of a system is what it does, not what you intended it to do. So, if the legislation is written with, 'If you intended to do this for not an enforcement purpose, then sharing is fine.' When we then find out later on that it was actually used for an enforcement purpose, what happens? What are the consequences for that outcome?

It's particularly challenging with data privacy, because data privacy, like life, once it's gone, it's lost forever. Intent is the difference between murder and manslaughter: the victim is still dead. In this case, our privacy has still been invaded; it's still been lost. We can't ever get that back, and what we see here are things like some civil penalties of 300 penalty rates, which at the current rate works out at about \$66,000. Personal information is extremely valuable. If I managed to get hold of a data leak of every Australian's medical record, 66 grand sounds like a pretty fair fee. You can pay more than that to various data brokers to get access to datasets. So maybe I just go, 'Okay, I'll pay the fine.' Those are some of the issues that we need to wrestle with with this—that it's not good enough to have good intent; we need to have systems that deal with bad intent and bad outcomes.

Senator AYRES: To what extent does a presumption in favour of the production of anonymised data as a result of the data sharing activity resolve your concerns?

Mr Warren: No, for two reasons. One, the source data is actually coming from the most sensitive data, which is about individual people, rather than starting with something which is inherently safer, like data about government operations. Why aren't we studying something that's easy and much safer, just inherently safer? Because it's about aggregate operations of government, and we're analysing what government is doing. Why don't we start there and prove capability and then build trust with people to say, 'Yes, we can actually do this in a safe manner,' before we start dealing with the really sensitive and delicate data that's about individuals? That's incredibly valuable data, which is why researchers want access to it. I understand that. But starting with the most dangerous option seems misguided to me. We also know—and we have proof because it's happened—that people like to think that they can de-identify this data, and then they don't. Or they say that it has been done, and then they're told, 'No, you're doing it wrong,' and they attack those critics and do it anyway, and then we prove them wrong. Or they say, 'Oh, this is really complicated to do.' Often the idea of complexity is different, so what I consider to be complex mathematics is very different to what a PhD in mathematics would consider to be difficult. The cybercriminals who are getting access to this data or who want the data because it's incredibly valuable to them are very smart. They can buy people with PhDs. There are lots of people who are very good at this, and none of them have to tell you what they're doing. They all just grab the data, re-identify it and get on with what they're trying to do—and you might never even know. We've seen the response from government so far when we try to point this out. It is to pretend that it doesn't happen, and that doesn't inspire confidence.

Senator AYRES: How does this re-identification process work? What does that mean?

Mr Warren: There are a variety of techniques. Essentially, you take data in one dataset and correlate it with other information that is publicly available or, in some cases, private datasets that you've already collected. For example, I can work out where you are in time and space and I only need four data points to do that. There was an article by Will Ockenden some years ago, before the metadata retention was passed, showing that, if you have access to the metadata from someone's telephone and got access to that and published it online and then invited people to tell him things about his life, they worked out where he lived, where he worked and where he'd like to go for lunch. I think they worked out where his parents lived. You can find out a lot about people with surprisingly little information. And because it's surprises people, because it doesn't seem obvious, that's why it's so very, very dangerous. Smart people can do amazing things with this data. In fact, that's often what the big data

exceptionalists like to say: 'We can do this amazing stuff. If you just give us access to this data, we'll be able to do a whole bunch of amazing things.' The bad guys can do amazing things too, because they have access to the same maths.

Ms Krahulcova: If I may, I'll just elaborate briefly on that. I think it's often a big concept for people to grapple with. For instance, an insurance company having aggregate datasets about where certain diseases are more prevalent or which neighbourhoods have a higher risk of this or that are just very real consequences, even in anonymised datasets. People always tell me that they're not too worried about it, the data, like, 'What's that going to do?' But if your insurance premiums go up or your insurance goes up on your house, because there are certain risk factors that they've been able to derive from information that you disclosed to the government, because you thought they couldn't operate as a private entity and they wouldn't share that data, suddenly the private entity has that data, and they're able to, in a very real way, impact your life. Mobile phone operators really want to do this and offer different sorts of plans in different neighbourhoods based on the socioeconomic status. I was a member of the World Economic Forum consumer data group a year ago. Health companies are keen to get very nuance data on people, because they want to literally market and sell people custom-tailored vitamins based on their lifestyle, based on their commute, based on every data point about them. It compounds critical issues, such as people being misdiagnosed or not diagnosed for certain illnesses. Where is the responsibility? You have that data as the government. You shared it with private entities and it's making people's lives worse. It's making their lives more expensive—or cheaper. But what is the responsibility?

I'm sorry I keep coming back to this example, but I think GDPR was very specific about the conditions under which academic institutions can get data specifically for these reasons. They're also very strict about data minimisation, technical measures to protect that data at the institution—privacy by design and default. There are a lot of concepts that I think need to be introduced before it's ready. That's why we stressed that the privacy factor should come first, and this legislation shouldn't supersede it. I'm really worried that we're going to have a very painful fight about the Privacy Act review and, in the end, this is going to do something else entirely, because it was passed a year before it. Please be wary of the sort of world we're creating for people and the injustices that we risk perpetuating.

Senator AYRES: That's your primary view, is it—that the Privacy Act review ought to happen first? Mr Warren, I wouldn't have necessarily read this in the explanatory memorandum, but the second-last page of your submission quotes the explanatory memorandum, saying:

Data sharing decisions by data custodians will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data.

This is one of the most high-handed things I've read for a while. That was in the context of the capacity for review of decisions. There has been some discussion about transparency—what data-sharing decisions are being made and how Australians see into that. In your view, is the legislation redeemable by amendment and, if so, what are the top three priorities for you, in terms of amendment?

Mr Warren: That's tricky, because the approach being taken is that it came out of the Productivity Commission and took a very financial view of data having value—that it's government data and we should unlock greater value from it. Firstly, I would question that. There's lots of government policy that never gets enacted, even though we have plenty of data about what we should be doing. Yet we ignore it, sometimes for many decades. We haven't closed the gap for 30 years, for example. Maybe we should get on with doing that first before we go researching new problems and proving that we will actually do something with all this lovely research. Having said that, I think there is room for greater data access and transparency. The trouble is that it's: what data? If data about individuals were removed and this became data about operations of government, then I think that the legislation would have value. We, as individuals, could gain greater faith that government could keep data safe, because it would be data about itself rather than data about us. That would align the incentives of government to make sure there wasn't a data breach and that the Russian or Chinese government wouldn't get a hold of all this lovely data. Prove you can do that first, then you can come for my medical scans.

I would also like to see consequences. If a breach happens, there should be a private action, which has already been passed by the Australian Law Reform Commission. That has been waiting to happen since 2014. At the moment, the only recourse that we have is to wait for a regulator to occasionally act. We have had plenty of royal commissions about circumstances where regulators have failed to act. So we are left with no recourse if the government decides not to police itself. That must change. There must be consequences for bad behaviour. Waiting for good intentions and hoping that we can shame people into behaving in the correct way does not work. There must be consequences, and the consequences have to actually happen. If we wait for government to do

them, then we are at the mercy of a government that polices itself or decides not to. And, unfortunately, we're seeing that happen far too often.

The final one would be just to have fundamental privacy protections that exist as a matter of Constitution. We, in Australia, are unlike any other comparable democratic regime. We do not have a bill of rights that encodes things like personal privacy. That must happen. It's astounding that we're here in 2021 and we still don't have that as a fundamental part of the make-up of our democratic society. That would provide us with a backstop of protection, no matter what government decides it wants to do from day to day. Maybe this government can be trusted with this access and transparency legislation, but the next one may not. We need to have that kind of continuous protection regardless of the vagaries of one government changing to another. We've seen in other regimes overseas very recently what happens when there is a sudden and rapid shift to an extreme. Laws can simply be ignored.

If those were to happen, yes, I think this legislation would be redeemable. It's a big ask, though. Failing that, I think you need to wait until privacy more generally is reviewed and we start to grapple with this as a whole-of-government exercise, rather than trying to carve out a special exemption to get rid of all these pesky privacy laws that we don't really want to have to deal with.

Senator AYRES: Thanks, both of you, for that discussion. Chair, I've concluded.

CHAIR: Thank you very much, Senator Ayres. If there are no further questions from other senators, that will be all from these witnesses today. Thank you so much for your testimony. I would like to thank all witnesses who've given evidence to the committee today. Thanks to Hansard and Broadcasting for their support as well. The deadline for questions on notice is 22 April. I now declare this meeting of the committee adjourned.

Committee adjourned at 12:01