CORRECTED

REPORT OF PROCEEDINGS BEFORE

STANDING COMMITTEE ON LAW AND JUSTICE

INQUIRY INTO REMEDIES FOR THE SERIOUS INVASION OF PRIVACY IN NEW SOUTH WALES

_____

At Sydney on 30 October 2015

_____

The Committee met at 10.15 a.m.

_____

PRESENT

The Hon. N. Maclaren-Jones (Chair)

The Hon. D. J. Clarke
Mr D. Shoebridge
The Hon. B. Taylor
The Hon. L. J. Voltz

CHAIR: I welcome everyone to the first hearing of the Standing Committee on Law and Justice inquiry into remedies for the serious invasion of privacy in New South Wales. Before I commence I acknowledge the Gadigal people, who are the traditional custodians of this land. I pay respect to the elders past and present of the Eora nation and extend that respect to other Aboriginals present. The inquiry is examining the adequacy of existing remedies for the serious invasion of privacy in this State. The Committee's terms of reference require it to consider the adequacy of existing remedies for serious invasions of privacy, including the equitable action of breach of confidence and whether a statutory cause of action should be introduced to respond to such invasions. In addition to these issues, a number of submissions to our inquiry have alluded to the capacity of the criminal law to respond appropriately to serious invasions of privacy.

Today is the first of two hearings we plan to hold for this inquiry. We will hear today from the New South Wales privacy and information commissioners, the New South Wales Council of Civil Liberties, the Australian Law Reform Commission, representatives from the legal fraternity, academics, and the Australian Privacy Foundation. Before we commence I will make some brief comments about the procedures for today's hearing. Today's hearing is open to the public and is being broadcast live via the Parliament website. A transcript of today's hearing will be placed on the Committee's website when it becomes available.

In accordance with broadcasting guidelines, while members of the media may film or record Committee members and witnesses, people in the public gallery should not be the primary focus of any filming or photography. I remind media representatives that they must take responsibility for what they publish about the Committee's proceedings. It is important to remember that parliamentary privilege does not apply to what witnesses may say outside of their evidence at this hearing. I urge witnesses to be careful about any comments they may make to the media or to others after they complete their evidence as such comments would not be protected by parliamentary privilege if another person decided to take action for defamation. The guidelines for the broadcasting of proceedings are available from the secretariat.

There may be some questions that a witness could only answer if they had more time or with certain documents at hand. In these circumstances witnesses are advised that they can take questions on notice and provide the answer within 21 days. I remind everyone that Committee hearings are not intended to provide a forum for people to make adverse reflections about others under the protection of parliamentary privilege. I therefore request that witnesses focus on the issues raised by the inquiry's terms of reference and avoid naming individuals unnecessarily. Our witnesses are also advised that any messages should be delivered to the Committee through the Committee staff.

ELIZABETH COOMBS, NSW Privacy Commissioner, Information and Privacy Commission, sworn and examined:

CHAIR: Before we commence with questions would you like to make an opening statement?

Dr COOMBS: I would, thank you. I hope to keep it brief. Madam Chair and members, thank you for inviting me here today to address the Committee. I am conscious that I am your first witness to appear in the public hearings. I would like to express my appreciation for this opportunity but also my very strong support for the introduction of a statutory cause of action for serious invasions of privacy. I know that you will be hearing many issues over the course of the hearings. I would like to have the opportunity to address some of the matters that might come up in some of the later hearings. I will give a brief overview of my submission to commence and then, as I said, some of those issues which I anticipate will come up. As the privacy commissioner it is my statutory role to act as an advocate for the protection of the privacy of the citizens of New South Wales. My concern is that their personal information, in addition to their broader privacy rights, is protected. I draw your attention, as a context to this inquiry, to the fact that privacy is a basic human right. Article 17 of the United Nations International Convention on Civil and Political Rights, of which Australia is a signatory, says:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

This is the important part as well:

> Everyone has the right to the protection of the law against such interference or attacks.

New South Wales privacy legislation does provide some protection. There is absolutely no doubt about that. My report to Parliament tabled earlier this year says that those pieces of legislation have stood the test of time well in general, but they really concern information privacy. I argue that neither the Privacy and Personal Information Protection Act nor the Health Records and Information Protection Act deals sufficiently with the broader concept of privacy as described by article 17 of the declaration. Most definitely they do not deal well with the broader concept of privacy—that notion of being left alone, of the right to freedom from interference or from surveillance and the right to solitude. Privacy is increasingly becoming an asset. That is not just the view of an advocate for privacy such as me; it is proven through empirical, quantitative and respected research. Privacy is something that an individual believes gives them the right to control their lives and information about them. We as a society do not condone acts by individuals or businesses that use physical violence or threats to rob people of their property. Information about you, as set down in the Act, is an important asset. I argue that privacy in this sense deserves similar protections against theft and harm whether actual or threatened.

It is all the more important in an age where we not only have technological advances but we have ever increasing technological advances. The Privacy and Personal Information Protection Act was introduced in 1998, seven years after the internet but many years before we had iPhones, smartphones, iPads, Facebook and other tools that people use in their everyday lives. We could not question that technological advancement has led to a rise both in benefits and convenience to citizens but it has also led to a rise in serious threats to their privacy—sometimes through their own actions, sometimes through the actions of other parties or business or government. It is our responsibility to try to keep up to this evolution. Data breaches intentional or otherwise are unfortunately not an uncommon occurrence. As I was walking to the train station this morning I saw a billboard saying that there had been very significant identity thefts just recently where people's tax file numbers have been stolen. The important thing is it is not just about financial information; these things have a domino effect. That information which has been stolen by one will be onsold to others and so the uses are pervasive and ongoing.

I also want to spend a little bit of time on the rise of revenge porn, given the seriousness and the very offensive nature of such acts but also the fact that they have received quite broad media attention. With other breaches such as the Ashley Madison breach, the salacious nature has brought those ones to the fore. But there are other cyber attacks which affect many people, such as the one on Adobe customers that affected 38 million people worldwide of which 1.7 million were Australians. There are some more micro-level examples. One is a telco. Recently in the last couple of months there was an allegation that that telco had inappropriately accessed the personal information of a customer who also happened to be a journalist.

I think many people who raise concerns about the introduction of a legal remedy for serious invasions of privacy point to common law as an avenue which currently exists. Common law most certainly has a very

fine and respected tradition. Common law, though, dates back to the twelfth century. Anything that is 900 years old is going to move very, very slowly. I think that is what we are seeing in the submissions which have written about why common law in itself is not sufficient. In a globalised economy where we have instant and worldwide communication, and where anyone with a smartphone can become an Internet superstar in a matter of hours, the ability of the common law to protect privacy rights, and regulate appropriately and comprehensively the appropriate use of people's information or incursions into their privacy, is hampered by a lack of flexibility and timeliness. Lord Leveson, when he came to Sydney—

CHAIR: Dr Coombs, I am sorry to interrupt but I would point out that we only have limited time for questioning here today.

Dr COOMBS: I would just like to make the point that Lord Leveson made the point that these things are not insurmountable in law. So I would just like to say to you that we have now got the reports for a statutory cause of action by the Australian Law Reform Commission, the Victorian Law Reform Commission and the NSW Law Reform Commission, and a variety of other reports which make it clear that there is a need for action on the serious invasion of privacy.

In the submissions that the inquiry has received to date there are many of that same view, such as those from the Law Society of NSW, the NSW Council for Civil Liberties, the Office of the Australian Information Commissioner, the Australian Privacy Foundation and legal experts from a variety of institutions—for example, I see that you will be talking to Professor Normann Witzleb from Monash University. There have only been three submissions in total that have been specifically opposed to the creation of a statutory cause of action. I have touched on some of the points that they concern themselves with such as the common law. They will also I think address the issue of what will happen if New South Wales takes a leadership role. Would that cause a fragmentation and a patchwork quilt?

CHAIR: Dr Coombs, sorry to interrupt, but if you have a written copy of your opening statement then you are able to table that.

Dr COOMBS: Thank you, I will do so. I also wanted to say that if the Committee is not of a mind to make a recommendation for a statutory cause of action then there are certain actions that could be taken to improve the coverage of the Privacy and Personal Information Protection Act 1998 [PPIP Act] and the Health Records and Information Privacy Act 2002 [HRIP Act], which might be something the Committee would be interesting in doing. I would like to make the very strong point, as I know Committee members have heard me say before, that New South Wales has a strong history of support for privacy which cuts across the political continuum.

In 1975 New South Wales was the second international jurisdiction to introduce protection of privacy rights. I notice that the Victorian law reform commission in their report said that there was nothing wrong with Victoria taking the lead—in the way that New South Wales did back in 1975 when it acted as a catalyst for the introduction of legislation throughout Australia—in relation to a statutory cause of action. If the Committee is interested in what would be recommended as a key element, I would certainly be very happy to provide a further submission on that. I thank the Committee for its patience.

CHAIR: Thank you, we will now move to questions.

The Hon. LYNDA VOLTZ: Dr Coombs, in your submission you say that a statutory approach needs to be taken in regards to this.

Dr COOMBS: Yes.

The Hon. LYNDA VOLTZ: Obviously the law is inadequate in regards to these matters. In particular I note that your submission uses the term "revenge porn". The Law Society of NSW in its submission outlines the intentional infliction of emotional distress. It is one of those areas where we start to get into the complexity of law, because the idea is that this "revenge porn" is about in some way taking revenge on someone. I think of incidents such as where Lara Bingle had a photo of herself put out by Brendan Fevola, a footballer. At the time they were in a relationship so that was not "revenge porn" as such, but it was a bloke doing something to a woman—he did not have her consent but he thought it was okay. It is more about the message, is it not?, as you said, that this is not acceptable behaviour.

Dr COOMBS: It most definitely is not acceptable behaviour. It is extremely offensive. It gives us a sense of the different way that violence can be perpetrated in our community than it once was. Once you could shut your door on people who wished to attack you. But now with cyber identity and a cyber profile there is the means to put things out beyond just your immediate circle to the whole world. It is incredibly damaging to the individual. It strikes at the heart of who they are and what they are. I think it is very important. It is about not just observable damage but also psychological distress. A cause of action needs to be able to actually address those forms of damage. I would just like to make one further point about revenge porn, if I may. Yes, it is very serious and it is very offensive. But it is not the only form of serious incursion of the privacy of an individual. It is one which does receive more media attention than others, but it is only one form. My real desire is to see that we have a cause of action which is comprehensive and addresses other forms of serious incursions of privacy.

The Hon. LYNDA VOLTZ: Could you give us a couple of examples?

Dr COOMBS: Many of the requests which I get—which I simply cannot deal with, both because of the terms of the legislation and also because of resourcing—go to the issue of surveillance. People have very grave concerns about that. People also have concerns about the case where someone takes information which may have been given to them through trusted sources and makes it more widely available. They are concerned about people coming into their house and taking photographs and then putting those out. So there are a variety of forms which this can take but it goes to a person's ability to control their life and that of their family. A lot of these incursions are not limited to an individual but rather concern their family, children and others who may be dependents.

The Hon. LYNDA VOLTZ: So you are talking about, for example, a closed-circuit television camera on the neighbour's house that is aimed at your bedroom or your kids playing in the backyard? I take it that you are talking about that type of intrusion.

Dr COOMBS: Yes, neither of the pieces of New South Wales legislation addresses acts undertaken by private individuals or small businesses. I will not go into the details of the health legislation which does provide some coverage—but it is patchy. There are other serious incursions of privacy, and we hear about that. People ring us up or speak to me when I am at various functions advocating privacy and how to appropriately manage it. People come up to me and raise these issues. They are concerned that they are not able to find a readily available, easy and inexpensive way of getting redress. It is of concern to them. Of course it then becomes a matter of concern for me as the NSW Privacy Commissioner.

Mr DAVID SHOEBRIDGE: I have a question that follows on from that. If we put a statutory cause of action in and then we give jurisdiction to determine that to, say, the District Court, the Supreme Court or the Federal Court, we could well be setting up just a rich persons' remedy—

Dr COOMBS: That is right.

Mr DAVID SHOEBRIDGE: That would be a deeply problematic outcome, would it not?

Dr COOMBS: I would like to draw to your attention the proposal that was put forward to the Australian Law Reform Commission by my Federal colleague Timothy Pilgrim, the Australian Privacy Commissioner. He proposed a complaints model to run alongside that statutory cause of action and the access to the courts.

Mr DAVID SHOEBRIDGE: Would part of the solution to ensure that it does not become like defamation law—which is just a rich person's game—potentially be to empower your office to be able to make some binding determinations?

Dr COOMBS: At the moment I do not have those powers but in my submission I raise it is a sensible way to go, because it is a concern—it should not just be for the people who have the means to gain access to the courts.

Mr DAVID SHOEBRIDGE: Of course some of the people who are most vulnerable and who have the most urgent need for remedy are women who are already involved in domestic violence proceedings. The women's legal service has suggested giving additional remedies such as takedown orders and other powers under the Crimes (Domestic and Personal Violence) Act 2007. These women have proceedings before the courts

already, and the police are there able to prosecute the case; and the ability to have some additional orders and remedies in those proceedings seems like a very effective way of giving real justice.

Dr COOMBS: I did read that submission. I think there are great difficulties now in getting material taken down from the Internet. I might just acknowledge that under the Google "right to be forgotten law" that was introduced in the European sphere there are very practical issues about, once it has been put out there, how effective you are in being able to bring it down. The phrase "digital eternity" does mean that once it is out there the horse has bolted.

The Hon. DAVID CLARKE: Dr Coombs, you support the development of a statutory cause of action. Is there a jurisdiction in the world that you would point to as providing a good model for this?

Dr COOMBS: I will come back to you on that, but I would like to make a couple of points if you would not mind? It was Professor Witzleb who pointed out that Australia is standing virtually unique amongst those countries that have common law tradition not to have a legal remedy of a statutory cause of action for serious invasions of privacy. He does say that where there are existing human rights bills you need to look at the context. That is a summary of some of the major points that he was making. I would like to come back to you on that.

The Hon. DAVID CLARKE: You said that Australia's privacy laws should meet international standards. Is there a gold standard of what those international standards should be? Where do we find these international standards?

Dr COOMBS: A variety of mechanisms have produced standards—APEC, OECD and the Apple ones as well. In terms of the particular statutory cause of action, in attachment D to the submission that I have provided to the Committee there is a comparison of various models that have been put forward by different law reform commissions. When we look at those we need to be looking at: What is the need of the ordinary person and that person's ability to access those? The advantage that I see this inquiry has is that the Committee has those reports that are very strongly researched. That will give this Committee the ability to pick up elements which will best meet the situation needed here in New South Wales. I would be very happy though to take that on notice and come back to you on that question.

The Hon. DAVID CLARKE: Are you going to take on notice what the international standard is?

Dr COOMBS: Yes.

The Hon. BRONNIE TAYLOR: Following on from Mr Shoebridge's question, my daughter had someone hack into her Facebook page and then they shared it. That was horrible for her. She felt very powerless in that situation—we all did. If the Committee were to make a recommendation on the constant theme to this inquiry that you have spoken about, do you think we also need to make sure that it is accessible to everybody—as Mr Shoebridge has said—and not to just those who can afford it? Perhaps we need to draw a line in the sand so that people know there is a process they can go through. Do you feel that the horse has bolted? For example, you spoke about Lara Bingle and I see it happening with my children. Do you think we also need to draw a line in the sand so that people know this is not okay and they stop doing it?

Dr COOMBS: That is a very valid point. We need to be communicating what is expected and what is appropriate behaviour. The ability to take action does start to get that re-education and refocusing that there are consequences to behaviour of that sort. At the moment I think people who may, for whatever reason, whether it is unintentional or with malice intent, possibly are not seeing the consequences of their behaviour, but most definitely the victim is experiencing the consequence, and that can live with them for many years.

Mr DAVID SHOEBRIDGE: There is not a lot of generation Y around this table. Is there a cultural difference in terms of privacy expectations between the younger generation and the group of individuals sitting around this table?

Dr COOMBS: No, there is not. In fact, research coming out of the Pew Research Center in the United States is showing that the young might be sharing more information but they want to know who is using it and how they are using it. They have very strong views on that. I might have mentioned in another inquiry that the ability to use certain technologies to protect your privacy has been taken up most vigorously, in greatest numbers, by those under the age of 24.

Mr DAVID SHOEBRIDGE: They know the pressure points and they want their rights respected.

Dr COOMBS: That is right. They also know the technology to know how to do it—unlike myself who loves the convenience of technology but I am not very well versed in some of those applications that can delete your text messages instantly, and all sorts of other varieties of ways of seeing who is seeing your information.

The Hon. LYNDA VOLTZ: There are very good examples of laws being used to change social behaviour—for instance, random breath testing and the criminalisation of drink-driving is a good example of how you can change the social norms over a short time.

Dr COOMBS: Some of the issues that Lord Leveson was speaking about in his speech were good to read because he actually talks about that, as did Michael Kirby. Back in 1996 Michael Kirby said cultural norms and behaviours have not evolved, and one of the reasons for that is because there has not been a consequence or a sense of it being really inappropriate.

Mr DAVID SHOEBRIDGE: Do you think the idea of using the NSW Civil and Administrative Tribunal [NCAT] as the primary venue for a contested dispute to be resolved is a cost-effective way of dealing with this?

Dr COOMBS: I do. That is a very respected and reputable institute.

Mr DAVID SHOEBRIDGE: That was a recommendation of this Committee in another inquiry so we obviously all support the NCAT.

Dr COOMBS: Right. It does come back to having an enforceable means to actually get behaviour changed.

Mr DAVID SHOEBRIDGE: And promptly?

Dr COOMBS: That is right.

Mr DAVID SHOEBRIDGE: And without bankrupting someone if they fail in their cause of action or if they have to defend the cause of action?

Dr COOMBS: And I think that people do find it easier if there is something that is more informal, particularly if it is a matter for an ordinary person, not someone who is used to dealing with legal matters.

The Hon. LYNDA VOLTZ: Some things can be resolved that way, but for others we need to make it clear that it is a crime. There is a difference between hacking into a Facebook page to put up a joke for someone who is out of control, as opposed to sending naked photos of an obviously distressed person around to your mates.

Dr COOMBS: I think it is important to realise and to reflect that there are a range of remedies underneath this whole statutory cause of action, which can include the NCAT, determinative powers for the Privacy Commissioner, and access to courts of law. I do have the power to conciliate but I have no means to enforce if someone breaches what has been determined or agreed in that room.

Mr DAVID SHOEBRIDGE: The Privacy and Personal Information Protection Act [PPIP] has very patchy coverage.

Dr COOMBS: It does.

Mr DAVID SHOEBRIDGE: For example, it does not cover all private citizens; it does not even cover all statutory-owned corporations. Can you briefly outline the narrow nature of the State privacy laws?

Dr COOMBS: It is primarily public sector agencies—government agencies, councils and universities. That is the PPIP Act. Under the Health Records and Information Privacy Act [HRIPA] it is private health service providers and organisations with more than $3 million in turnover per year that deal in or hold health information. Non-government organisations, which are increasingly providing services for government, are not

necessarily covered unless it is by contract. State-owned corporations are not covered by New South Wales legislation.

Mr DAVID SHOEBRIDGE: So disability service providers being contracted to do work previously done by the State Government are not roped in by our State privacy laws unless the contract expressly provides?

Dr COOMBS: It is a grey area.

Mr DAVID SHOEBRIDGE: Should it be grey? Or should it be black and white?

Dr COOMBS: Underneath my report to Parliament I do recommend making Acts abundantly clear. At the moment unless they are dealing with health information—organisations dealing with disability information would be because that is a health service, so they would be captured. I will take advice from my colleague, but the Department of Family and Community Services is most certainly looking at privacy protections to actually set that in place and having the appropriate exemptions.

Mr DAVID SHOEBRIDGE: Social housing providers, for example, are not health related?

The Hon. LYNDA VOLTZ: I think we are getting a bit off the track.

Dr COOMBS: If I could just come back to your original question about exemptions? The NSW Law Reform Commission report does go through where the exemptions are considered either to be too broad or where the Privacy Commissioner should issue statutory guidelines to enable them to interrupt. In the case of law enforcement, it was education and administrative functions.

CHAIR: Thank you for your appearing before the Committee today. Your response to the questions taken on notice is due back in 21 days. Committee members may also have additional questions, which will be forwarded to you. You are more than welcome to table your opening statement or to provide it as a second submission at a later date if you would like to.

Dr COOMBS: As a courtesy, could I just let you know that it is my intention—unless there is a view to the contrary here—that I will be issuing a media release putting my position forward.

CHAIR: That is fine.

(The witness withdrew)

ELIZABETH TYDD, NSW Information Commissioner and Chief Executive Officer, Information and Privacy Commission New South Wales, sworn and examined:

CHAIR: Welcome. Would you like to make an opening statement?

Ms TYDD: I would. Thank you very much. I am very conscious that the submissions that I have made and my appearance today are not central to the issues before the Committee, particularly in relation to the thresholds that the Committee has established around serious invasion of privacy, and that my input into the Committee's consideration would be of a general nature in relation to the operation of the Government Information (Public Access) Act 2009 and also from the perspective of the regulatory regime. I acknowledge that I appear before the Committee today in two capacities: as Information Commissioner, and therefore championing open government, but also in the role of upholding my duty to the Information and Privacy Commission [IPC] to act in its best interest in my capacity as the chief executive officer.

I will touch on some of the key issues raised in my submission, in particular some of the possible implications that no doubt the Committee will be turning its mind to, the application on government-held information within the open access regime, and some broader jurisdictional questions. The submissions have focused on the more detailed areas about information regarding the Act. If the Committee has specific questions, the IPC is able to respond, and I will respond on notice.

I am mindful of the terms of reference, in particular the threshold of seriousness, and that my comments will be reflective of the operation of the Government Information (Public Access) Act 2009. Turning to the Government Information (Public Access) Act 2009 and my capacity as Information Commissioner, I will highlight some concerns specifically as they relate to government-held information. There are a number of potential implications for a statutory cause of action, particularly in a broad sense, on the release of government-held information and, therefore, the implication for public sector agencies and citizens.

The Government Information (Public Access) Act 2009, as I am sure Committee members are aware, establishes an explicit presumption in favour of disclosure of information. It is based upon the principles of proactive release of information and, very importantly, a public interest test balancing factors in favour of and considerations against the release of information. It also establishes a number of safeguards to protect privacy. The use of the public interest balancing test is one of those safeguards. It assists decision-makers in not only identifying but weighing up the considerations for and against the release of information.

The Government Information (Public Access) Act 2009 also requires a consultative mechanism in which third parties must be consulted prior to the release of information. Whilst that may not be the dominant consideration, it is a factor that must be taken into consideration in balancing those rights in relation to government-held information. It also provides the ability for a person to make a complaint to the Information Commissioner. There may be a couple of circumstances in which information that is released that has been government-held information—that is, released under the Government Information (Public Access) Act 2009—impacts upon a person's privacy. Again, I am conscious of that threshold of seriousness. It can be where an individual requests access to their own information or information that involves someone else and, likewise, in relation to government agencies and their requirement to consult.

If a statutory cause of action was made out, the information as to why it was sought and the purpose may also need to be considered. The New South Wales Civil and Administrative Tribunal or the courts would need to consider those issues. In exercising those functions it is anticipated that there could be an impact on the types of information released and the future behaviour in relation to release from agencies. Again, I specify that that is in relation to government-held information. It does not cover the sorts of matters that were raised in the media this morning and some of the questions I heard earlier in the hearing.

I draw the Committee's attention to the report of the Australian Law Reform Commission [ALRC]. I know the Committee has had regard to that. In particular, I draw the Committee's attention to part 12 of the draft bill that was attached to that report. It stated:

> The objects of this Part are:
>
> (a) to recognise that it is important to protect the privacy of individuals, but that the interest of individuals in their own privacy must be balanced against other important interests (including the interest of the public in being informed about matters of public concern) …

Public concern is quite a different concept from the individual releases that I heard the Committee discussing earlier. This type of decision-making framework has since been adopted in legislation—and it is adopted in the Government Information (Public Access) Act 2009—to enable a proper balancing exercise to occur, particularly at a lower threshold than the threshold that the Committee is currently considering.

I turn to potential regulatory issues. The submissions traverse these issues. I heard the Committee considering issues in relation to ensuring that there is a cohesive system to address these issues and that there is complementarity, to the degree possible, between existing legislative regimes, be they privacy protection specific legislation or criminal law issues. That is a consideration that I am sure the Committee is well aware of and that is traversed the submissions made so far to the Committee.

The statutory cause of action, if designed, would therefore give consideration to the precepts of open government and the interests of the public in receiving information to ensure appropriate transparency and accountability. Again I reference government-held information. Any statutory cause of action should recognise and support that complementarity of information access in the privacy regulation regimes. Citizens of New South Wales, as I have heard the Committee comment, would be better served by a complementary and cohesive regime. Likewise, I would also support the notion that accessibility is very important in any cause of action.

Finally, depending upon the approach taken, it might be informed by considerations of statutory oversight. For example, the ALRC's report into the serious invasion of privacy in the digital era recommended the extension of existing powers to investigate complaints and include complaints about serious invasions of privacy more generally. The Committee concluded in relation to my colleague's evidence that careful consideration should be given to how to ensure access to remedy and redress and also to ensure appropriate capability and resourcing for the ability to access any statutory cause of action.

CHAIR: Thank you very much. We will commence questions.

The Hon. LYNDA VOLTZ: Thank you for appearing today, Ms Tydd. In your submission you raised the following problem:

> Other situations could involve invasions of privacy on social media. A determination of jurisdiction in this scenario could present significant legal issues …

How would this not be resolved if we used legislation similar to that used in commercial surrogacy, where offences were being committed overseas but it was based on residency status in New South Wales?

Ms TYDD: There are many ways of overcoming those issues, and I am sure the committee is aware of some of those issues. One of the other possible solutions is the approach taken under the Australian consumer law where at the time of developing that legislation consideration was given to where the breach occurred, for example, or where the transaction for the sale of goods took place. So there are definitely legal avenues to ensure that those issues are addressed, and they are matters that would be considered in developing a course of action.

Mr DAVID SHOEBRIDGE: When something is published on the internet you have got a global breach, on one view. Have your turned your mind to a kind of jurisdictional definition? The Deputy Chair has proposed residency—

The Hon. LYNDA VOLTZ: I have not proposed that; I am saying that is a way it has been dealt with in the past.

Ms TYDD: That is not something that the IPC has extended or that I have extended thought to, but there are possible remedies and I would agree that there are a number of avenues to consider as to how that might be addressed. I would suggest perhaps the Department of Justice may also be well placed to provide a response to that question.

The Hon. LYNDA VOLTZ: But you do see the Privacy Commissioner having a role. I do not know if you heard the evidence of the Privacy Commissioner when she was just here—

Ms TYDD: I did hear some of it.

The Hon. LYNDA VOLTZ: She suggested that she has no recourse other than consultation. Do you think that the Privacy Commissioner is one area that should be empowered to be able to act in regard to these breaches?

Ms TYDD: I would certainly acknowledge the limitations of my positions. I am not an authority in relation to the Privacy Act. I would, however, take guidance in relation to that, and certainly if the committee was of a view to recommend, and those recommendations were progressed, around jurisdictional issues, that would be something that in my capacity as the IPC I would be actively pursuing.

The Hon. LYNDA VOLTZ: I note that you have come forward in regards to the GIPA Act itself. The GIPA Act, I know that you state that it is about a system of open, accountable, fair and effective democratic government—you may have missed some of my speeches lately—

Mr DAVID SHOEBRIDGE: In due course.

The Hon. LYNDA VOLTZ: In due course you will. The reality is that there would not be many occasions where information would be released by a government that would breach someone's privacy. Where do you see within the GIPA Act that that would be possible, given the way the GIPA Act already has within its definition that it is not in the public interest to do so?

Ms TYDD: That is a question that is absolutely germane to the issues and goes to the issue that I highlighted of seriousness. Under the GIPA Act the protection of privacy is something that must be considered. In terms of the number of applications that are dealt with where the outcomes might deal with a provision under the Act that deals with judicial consideration and individual rights, which goes to the heart of privacy, there are an increasing number of applications made to access personal information of an individual or of someone else's. So they are an application made under the GIPA Act, and its reporting, I would absolutely concede, is pretty global, for information of that nature.

Under the GIPA Act the decision maker must weigh up those factors. Your question goes to the heart of what would dominate in the release of information, and clearly decision makers are very conscious, and there is not statistical evidence to demonstrate that they are not very conscious of protecting and upholding those privacy rights and balancing those against the interest in releasing information.

The Hon. LYNDA VOLTZ: For example, I have spent four months trying to get a GIPA and possibly the only personal information that would be on it would be the name of the person from an organisation who would constitute a third party, but that person has a right to dispute my application and therefore I do not get the information because they have disputed whether that should be released.

Ms TYDD: There is provision, of course, as I have indicated, for consultation. They may well in those instances—and I will not discuss any matter that may prejudice particular outcomes—but if the factors in favour of disclosure are outweighed by the factors against disclosure, only in those circumstances should information be withheld under the GIPA Act.

The Hon. LYNDA VOLTZ: But they still would not release it anyway because the third party would be entitled to the review period, would they not?

Ms TYDD: The review period certainly applies, but it may be released following the expiration of the review period.

Mr DAVID SHOEBRIDGE: Privacy as against the overriding public interest in producing and publicly disseminating public documents is undoubtedly an area of tension in freedom of information in New South Wales. Do you think it is an increasing area of conflict?

Ms TYDD: I would say that the GIPA Act provides machinery, mechanical solutions to addressing those conflicts; for example, the redaction of information, which may go to the heart of the issue that you were raising.

Mr DAVID SHOEBRIDGE: I could give you a dozen blacked-out pages that I got from the University of Sydney recently relying upon the privacy public interest as a consideration. I am just asking you: Is it an increasing issue. Is it a de minimis issue? How do you see it?

Ms TYDD: The figure I could give you that may indicate that it is not increasing, and certainly from my vantage point just looking at the IPC's work at this stage, in the last financial year our staff were required to consider a number of matters—I think close to 90 matters—in which those issues of personal privacy arose. At no stage did they make a recommendation to me that they ask the agency to review its decision not to release but to withhold information. In those instances—can I explain it a little more helpfully for you? The agency decided not to release and, on review, we did not ask the agency to reconsider for release.

Mr DAVID SHOEBRIDGE: Was that 90?

Ms TYDD: Correct—in relation to all of the files that we have seen.

The Hon. LYNDA VOLTZ: There were none that were overturned?

Ms TYDD: Correct. We do not have the power of overturning—

Mr DAVID SHOEBRIDGE: There is none even where you recommended a review or a reconsideration?

Ms TYDD: Certainly we do recommend a review and a reconsideration on the basis of how those decisions were made and the explanation provided. The law in this regard is maturing and that judicial consideration is providing more guidance in relation to how redactions can occur.

Mr DAVID SHOEBRIDGE: I just want to be clear—I may have misunderstood you. There were 90 occasions where your office was asked to review a decision by a government department not to release information because of privacy considerations and on not one of those occasions did you recommend the release of the information, on a review. Is that what you say?

Ms TYDD: I can be very clear in stating, and my colleague is here with me, we do recommend reconsideration but we have not recommended utilisation of section 94, which goes specifically to saying to the agency, "You must reconsider in relation to the provision of personal information". We have used other powers which asked them to reconsider on other grounds; for example, the proper application of the public interest test.

Mr DAVID SHOEBRIDGE: I might ask you to take it on notice and perhaps give us a fuller explanation. That would be very helpful.

Ms TYDD: Certainly.

The Hon. BRONNIE TAYLOR: Thank you very much for coming in, Ms Tydd. In your submission and in your opening statement you mentioned the fact that we need to look at something that is low cost so people can bring action and will not be disadvantaged, which is a question we asked Dr Coombs. I am just asking you what models you think are possible low-cost methods to bring an action and would that be the NSW Civil and Administrative Tribunal [NCAT] that you were supporting that you mentioned before? We would like to hear from you what you think the benefits and the limitations of those are.

Ms TYDD: In relation to NCAT I would need to declare that I have had a long history of working within the tribunal systems and I am a strong advocate for tribunal systems as a low-cost dispute resolution forum, particularly given that they also have at their disposal other means by which dispute resolution can take place—mediation, conciliation, et cetera. In that regard I particularly reference some of the work of NCAT in relation to the former Consumer, Trader and Tenancy Tribunal, which was an incredibly accessible tribunal of which I had occupied a role as a deputy chair for a considerable period of time.

The ability to apply those alternative dispute resolution mechanisms within a framework that enables you to uphold an outcome, to enforce an outcome, has considerable merit. That is one option. There are other options, but in relation to conciliation in that environment, decisions can be made that reflect the views of the parties and that uphold the law and that, therefore, are enforceable. Other methods that are adopted in relation to different types of disputes are more mediation models, and I am sure the committee would be aware of

mediation models, and they can have an effect. Some of the issues that I am aware the committee is considering are that threshold of seriousness—what does seriousness mean at law and, therefore, what are the appropriate fora to consider a seriousness threshold test and, therefore, provide redress?

Mr DAVID SHOEBRIDGE: What do you think? How would you define "serious"?

Ms TYDD: The sorts of examples that the Committee was articulating earlier were, in my view, quite serious matters.

Mr DAVID SHOEBRIDGE: But other than in an ad hoc illustrative fashion, what sort of principles should we look at when we are looking at "serious"?

Ms TYDD: It is more than at law some of the tests that may be involved, that it has to be material and that it has to have a significant adverse impact. Case law around those sorts of phrases would describe the seriousness. It may be a matter for this Committee to further consider those sorts of definitions.

Mr DAVID SHOEBRIDGE: Are you suggesting it should be partly subjective, not an objective test? The initial threshold, should it be subjective, insofar as the person who has been affronted by it, should their views be what determines seriousness or should it be an objective thing so that what a reasonable person thinks is serious? It is a key threshold point. What do you think?

Ms TYDD: I cannot bring, with authority, a perspective on that. I think that is a matter that perhaps Justice and other submissions may better traverse than my submission.

Mr DAVID SHOEBRIDGE: Because you gave examples of both subjective and objective considerations for seriousness. Do you think it should be both?

Ms TYDD: At this point that is a question I am happy to take on notice but there will be a range of views in that regard.

CHAIR: Thank you for appearing today. You will have 21 days to respond to the questions that you have taken on notice. The secretariat will provide you with a copy of that. There may also be additional questions that Committee members would like to forward through. They will be sent to you as well.

(The witnesses withdrew)

(Short adjournment)

HANNA RYAN, Vice President, New South Wales Council for Civil Liberties, and

STEPHEN BLANKS, President, New South Wales Council for Civil Liberties, affirmed and examined:

CHAIR: Before we commence with questions, would either or both of you like to make an opening statement?

Ms RYAN: I would like to. I thank the Committee for the opportunity to give evidence to this inquiry. The starting point for our submission is that while some of the technologies that might be discussed in the context of this inquiry may be new, the issue of privacy law reform is not a new issue. This debate has been had before, both in this jurisdiction and others within the country, over and over again.

In this inquiry we argue that the Committee should have regard to the extensive work done by other bodies, most recently the Australian Law Reform Commission [ALRC], in considering the issue and in making its recommendations. Looking at the conclusions of some of those other bodies and the submissions to this inquiry, we would suggest that the New South Wales Council for Civil Liberties' [CCL] position approaches being a consensus position. As we submitted to the ALRC's Privacy Law and Practice inquiry in 2011, privacy is an important human right, no doubt valued by all Australians, and an essential element of a liberal democracy. That expectation of privacy persists, even as technology evolves.

The privacy of Australians and people in New South Wales is currently inadequately protected by a range of different laws and we submit that we need a statutory cause of action to protect the right to privacy. There are differences of opinion about the details of this cause of action. The CCL position on details such as what the fault element should be and whether the public interest should be taken into account in the liability phase or the defence phase can be found in the appendix to our written submission, which was our submission to the 2011 New South Wales Law Reform Commission inquiry.

Because we think that the argument for a statutory cause of action to protect privacy has already long ago been fought and won, our written submission focussed on three issues. The first was the pragmatic question of whether New South Wales should be a first mover on this issue. The second was how New South Wales should respond specifically to the issue of revenge porn, which was singled out as an important technological challenge in the media release accompanying the announcement of this inquiry. Finally, the importance of other options for people whose privacy has been violated apart from litigation and approaching the courts.

On the first issue, the argument has been made, including by the joint media organisations in their submission that New South Wales should not move alone on this issue. We acknowledge the validity of this concern and we agree it would be ideal for the Commonwealth to legislate or to have a national privacy law reform scheme. However, we urge this Committee to be pragmatic. The political reality is that the Commonwealth is not going to move on this issue and we would point to the Commonwealth Attorney-General's refusal to consider the ALRC's recent recommendations. We argue that the object of national consistency is not so valuable that we should abandon privacy protection in this State because of it. We point to the fact that there already is a discrepancy between jurisdictions in Australia given that Victoria and the Australian Capital Territory [ACT] have human rights protections which include privacy. For New South Wales to engage in reform would not be an obstacle to national privacy law reform later, especially if New South Wales followed the ALRC's recommendations. We would encourage New South Wales to be a leader here.

On the issue of revenge porn, we acknowledge that it is a serious issue and we note that some politicians in other jurisdictions have sought to address it using the criminal law. We make the point that any criminal law would not preclude civil remedies being made available to victims of revenge porn. A civil cause of action would allow a victim to claim remedies such as damages and vindicate the interest in privacy. Any interest in criminalising revenge porn should not deter this Committee from recommending a statutory privacy cause of action.

Finally, we would encourage the Committee to contemplate out-of-court mechanisms for resolving privacy breaches. There are gaps in the help that the Office of the Australian Information Commissioner [OAIC], on a Commonwealth level, and the Information and Privacy Commission [IPC], on the New South Wales level, can offer, which we have detailed in our submission. We think a victim of a privacy breach should have more formal options available to them than the stress and cost of litigation. We note that in their submissions the New South Wales Law Society and the NSW Information Commissioner suggested an

increased role for the commission of being able to determine or conciliate complaints about conduct that falls within the proposed cause of action. We also adopt the suggestion by Mr Shoebridge that the NSW Civil and Administrative Tribunal [NCAT] might be considered where the privacy breach is committed by a government agency.

As a civil liberties organisation our interest is not just in privacy. We are also strong defenders of the right to freedom of expression which can come into conflict with the right to privacy. We think that a public interest element to this cause of action will be sufficient to protect that interest. We note that although the media organisations have opposed a statutory cause of action in their submission, any action under the breach of confidence as it currently stands, or other forms of privacy protection, do not have a public interest defence. Finally, we would urge the Committee to have regard to the idea of a bill of rights because a statutory cause of action in this area would just address one among many of the important human rights that are currently under protected in this jurisdiction. Thank you.

<7>

The Hon. LYNDA VOLTZ: In regard to the Privacy Commissioner, at the moment he can deal only with complaints but has no ability to take any action in regard to invasions of privacy. In what kind of regime would you envisage the Privacy Commissioner? There are different types of invasions of privacy; there is the nude photo that is sent without consent or hacking into Facebook and leaving an appropriate quote on someone's Facebook page. They can be different types of offences. Certainly the sending of sexually explicit photos is in a league of its own, I would have thought. What do you envisage as the role of the Privacy Commissioner?

Ms RYAN: I think any statutory cause of action would have to encompass both what has been called intrusions upon seclusions—things like images of a sexual nature and also information privacy. So it would encompass a range of different kinds of breaches of privacy. The suggestion that was made, I think, by the Law Society of New South Wales would be that the Privacy Commissioner would have the ability to conciliate any complaint that arises in a situation that would be covered by the cause of action. On that approach the Privacy Commissioner would have the ability to conciliate any number of different kinds of breaches of privacy.

The Hon. LYNDA VOLTZ: But only conciliate, not arbitrate?

Mr BLANKS: We would support the original model for the Australian Human Rights Commission which has a complaints taking ability; an ability to dismiss complaints that are trivial; an ability to conciliate complaints which it uses as a first instance attempt to resolve matters without the need for formal proceedings; an ability to conduct formal hearings or inquiries; an ability to make determinations; and, ultimately, which now the Human Rights Commission does not have, the ability to make determinations that can then be enforced by the courts. I think it is worth looking at putting in place a similar model, which is a tried and tested model and well understood, for the New South Wales Privacy Commission.

Mr DAVID SHOEBRIDGE: Another option would be to require a compulsory conciliation before the Privacy Commission, and a certificate before you could commence proceedings in NCAT. We see that model in certain other jurisdictions.

Ms RYAN: I think that is how the Fair Works Commission works in the Commonwealth jurisdiction.

Mr DAVID SHOEBRIDGE: Yes.

Ms RYAN: That would certainly do something to address the complaint that litigation is only accessible to the wealthy because you would have to engage in low-cost discussions first.

Mr DAVID SHOEBRIDGE: The other option would be if there was a conciliated outcome that was agreed and signed up to, that outcome could have the effect of law and could be enforceable?

Mr BLANKS: Those are useful options but I do not think they should necessarily be used to close off the possibility of court action, particularly where breaches are serious breaches, not limited to individual cases, situations where a government agency is not involved. I think there would be difficulty giving NCAT jurisdiction in situations where government agencies were not involved.

The Hon. LYNDA VOLTZ: Or where the Government decided to legislate to make it a crime?

Mr BLANKS: Yes. A statutory cause of action for privacy would run separately from any criminal sanctions that might apply to the same conduct. But there will be many cases of privacy breaches which do not, engage in any criminal regime.

The Hon. DAVID CLARKE: Your organisation supports a statutory cause of action. Is there any jurisdiction that you would like to point to that provides a model that you feel is an appropriate one for New South Wales?

Ms RYAN: I think it is only Canada that would have a comparable statutory cause of action. The reason for that is that other jurisdictions with privacy protections, those protections arise in the context of more wholesale human rights protections. So the United Kingdom as a Human Rights Act and that kind of thing.

The Hon. DAVID CLARKE: Do you say that what you are proposing, apart from Canada, is not to be found anywhere else?

Mr BLANKS: It arises because New South Wales and Australia do not have a comprehensive human rights protection legal system where individuals are able to take action where their human rights have been breached. Where jurisdictions do provide those remedies, privacy is protected and individuals have rights of action in respect of privacy breaches as one of the numerous human rights that will be protected.

The Hon. LYNDA VOLTZ: For example, if Australia had a human rights bill that replicated other nations, such as the United Kingdom, then it would be covered within that bill? Is that what you are saying?

Mr BLANKS: Certainly that would provide a framework for covering it. It may make a separate statutory cause unnecessary. I have not carefully researched a lot of other jurisdictions but from a general perspective in jurisdictions where individuals have the right to pursue infringements of their human rights, including privacy, there would be less need for a separate statutory cause of action.

The Hon. DAVID CLARKE: In the present situation in Australia do you point to Canada as a model?

Mr BLANKS: Canada has human rights legislation as well, so I am not exactly certain. Ms Ryan may know more about this.

Ms RYAN: I think we would appreciate the opportunity to respond to this question in writing. There may be jurisdictions in Canada that have that kind of stand-alone cause of action.

The Hon. DAVID CLARKE: Will you take that question on notice because you are proposing a statutory cause of action and if you can provide the Committee with models that would be comparable to what you would be looking to in New South Wales we would be interested in knowing about it.

Ms RYAN: Just to add to what I will probably say in writing. Even if there are not a number of models that we can point to where this has happened internationally I think the Committee cannot be too troubled by the fact that this would be relatively novel just because of the amount of extensive research and work that has been done in this area by the Australian Law Reform Commission, the NSW Law Reform Commission and the Victoria Law Reform Commission that this would not be just a shot in the dark but it would be based on years of research.

Mr DAVID SHOEBRIDGE: Will you comment on the position that has been put by the broadcasters Free TV who say that Free TV does not support any broadening of the scope of breach of confidence remedies for serious invasions of privacy. They say that in this context they are of the view that equitable actions for breach of confidence should be left to develop at common law on a case-by-case basis and the introductions of legislation is unnecessary. What do you say to that proposition?

Ms RYAN: I have two responses to that. The first is that leaving the common law to develop is unclear and unpredictable. By its nature it has to develop on a case-by-case basis and that is not an ideal situation for this jurisdiction to find itself in. My second response is that it is actually not necessarily a media organisation's best interests to just leave it to breach of confidence, because breach of confidence does not have any public interest defence. I would look at the recent example last year, I think, of where New Matilda published emails of an academic and then that academic took them to the Federal Court to sue them, in part, under breach of confidence. That action did not proceed to conclusion but if it had there would have been no public interest

defence. We would see this statutory cause of action as actually being preferable because it would incorporate a public interest element.

Mr DAVID SHOEBRIDGE: Should it oust the common law breach of confidence or an equitable breach of confidence action? Should it exclude that so as public interest is always being considered in these cases?

Mr BLANKS: I think a breach of confidence action is better thought of in the commercial context because obligations of confidence normally arise in the context of commercial relationships. Although the media have raised the issue, it is not the most common issue that arises for the media. Private organisations have a legitimate interest in protecting confidentiality of commercial information. I am not sure that a public interest defence necessarily is appropriate in those situations.

Mr DAVID SHOEBRIDGE: Which highlight's Ms Ryan's submission that when you are talking about broader public interest matters the existing equitable remedies are not well crafted?

Mr BLANKS: That is right. The fact is that the common law has failed to develop a satisfactory protection for privacy. There are plenty of cases. We could take it on notice and provide you with some examples where judges have described the state of the common law and said why they are not prepared to, as judges, make new common law to protect things which the existing common law just does not protect.

Mr DAVID SHOEBRIDGE: Those who say we should wait for the common law always point to *Australian Broadcasting Commission v Lenah Game Meats*, the 2001 case where the High Court said that they are not going to say that there is a tort or a remedy now but they are also not going to say they never will have one. If we are referring back a time 14 years ago when we got an ambivalent statement from the High Court as though the common law will respond, hoping for a common law response is hope over reality, is it not?

Mr BLANKS: I think that is correct. There have been plenty of opportunities since 2001 for the courts to develop general principles of protection of privacy and they have explicitly refused to do so.

Ms RYAN: I think there has only been something like two lower court decisions since Lenah Game Meats that have taken that statement and tried to enforce a right to privacy. That is hardly a development of the law.

Mr DAVID SHOEBRIDGE: Your organisation seeks to have a broader statutory remedy than was put forward by the Australian Law Reform Commission, particularly on issues such as whether or not recklessness and intentional actions should be a requirement or whether or not negligence should be sufficient to found an action. Will you expand on that a little?

Mr BLANKS: I will give you an example of a Federal government agency admittedly, not a New South Wales agency. The Department of Immigration last year published details of 10,000 or so asylum seekers in circumstances where those personal details were available on the internet for anyone to view. There must have been a human error somewhere but that occurred as a failure of complex IT systems which resulted in that publication. There has been litigation in relation to that in the Federal Court. That is an example of where there can be very serious consequences for breach of privacy and unwarranted disclosure of personal information in circumstances where there may have been no negligence and no easy ability to find recklessness or other breaches. It is simply the fact of publication and the danger that individuals are put into as a result of the publication that ought to result in a remedy.

Mr DAVID SHOEBRIDGE: The notorious Ashley Madison case would be a case in point. There are currently actions against Ashley Madison in North America but, as I understand it, there are no actions here. It would appear the cause of action is founded upon negligence or a failure to protect as opposed to some kind of recklessness or wilfulness on the part of Ashley Madison in its record keeping.

Ms RYAN: I think in those situations of mass data breach or where there is a big set of data that has been lost control of you are never going to be able to meet the standard of recklessness or intention. As big data develops that kind of risk grows ever more. I think it is worth responding to it.

Mr DAVID SHOEBRIDGE: Probably one of the most serious breaches would be one of those mass data dumps and an organisation that fails to protect its data, often very deeply personal data. Do you believe the

law should cover that so a negligent failure to protect people's personal and private information should be roped in to a cause of action?

Mr BLANKS: I would not suggest the cause of action be limited to situations where there is negligence able to be established. I think our submission is that it should be a broader cause of action which focuses on the disclosure and the consequence rather than exactly how it occurred.

The Hon. DAVID CLARKE: Because there could be consequences for virtually anybody in the world. Someone could be fiddling around on the internet, press the wrong button and the material goes out. What happened with those 10,000 asylum seekers could happen anywhere at any time quite innocently.

Mr BLANKS: Yes.

The Hon. DAVID CLARKE: It could be as a result of a mistake by one of millions of people out there.

Mr BLANKS: Yes.

The Hon. DAVID CLARKE: It is a very big issue, is it not, just that question alone? How do we deal with it?

Mr BLANKS: That is right. That is why I think the cause of action has to be broad enough so that there are not artificial hurdles put in the way of people who suffer detriment as a result of a privacy breach from having a practical remedy.

The Hon. DAVID CLARKE: Where do you put the balance?

Mr BLANKS: One of the balancing items would be seriousness. That is, we are not suggesting that this be opening up floodgates to trivial claims. There should be a threshold of seriousness. As everybody has suggested, there should be a range of defences available not built into the liability aspect but as defences which would provide protections for legitimate breaches.

CHAIR: You mentioned a threshold in relation to seriousness. Do you have a suggestion on that? I am happy for you to take that on notice if you need to.

Ms RYAN: I think that is in our submission in the appendix. Maybe we do need to take that on notice.

Mr BLANKS: It probably depends on where the matter is being dealt with. If it is in the courts, because of the expense involved it is really a matter for serious cases. A lower threshold might apply in cases which go down a conciliation stream before the Privacy Commissioner, but the Privacy Commissioner should have an ability to reject at the outset claims which are trivial. There does not have to be one standard across all the different parts.

The Hon. LYNDA VOLTZ: One of the defences, which I think was proposed by the Law Society, was young persons. I assume by that they meant persons under 18. Given the nature of the people that there are major concerns about in the use of new technologies such as Snapchat, Instagram and Facebook, should being young be a defence or should that be left to a process where it can be decided? One of the biggest concerns is the way young people use that media.

Ms RYAN: Do you mean that they have said that a defence to the cause of action be that the defendant—

The Hon. LYNDA VOLTZ: Was either a child or a young person. I assume they mean by "young person" someone who is between 16 and 18.

Ms RYAN: That is presumably getting at the context where someone is sexting or whatever and they are 15 and they do not know any better. It seems to me that that should be taken into account, but I do not know whether it should be a strict defence or whether it would be better left to the discretion of a judge based on the context. I come back to the Chair's question about the seriousness, on page 14 of our submission we have said

that we would have the threshold as being a serious invasion of privacy that is offensive to a person with ordinary sensibilities rather than being highly offensive.

Mr DAVID SHOEBRIDGE: One of the arguments used against this comes again from the submission from Free TV Australia. They say:

> Increasing the regulatory burden on broadcasters by introducing a statutory cause of action for serious invasion of privacy will have a number of detrimental economic consequences.

One of them they cite is that it will:

> Require organisations to increase their investment in protecting against such actions by way of reviewing current practices, staff training etc

From a public interest point of view, that kind of organisational change would seem to be the most beneficial thing we would get out of moving in this direction. What do you think?

Mr BLANKS: I agree with that, and I do not think it is a legitimate excuse for the way Parliament ought to consider public policy. It is legitimate for the community, as a matter of standards, to require standards of broadcasters that conform to community standards. If that imposes costs, of course broadcasters have licences to broadcast so they have all sorts of costs imposed as a result of being granted a licence. It does not seem to me that costs imposed by any change that might come about in this area would impose an unreasonable burden.

Mr DAVID SHOEBRIDGE: If a broadcaster had to review its practices so that it no longer engaged in serious and highly offensive breaches of someone's personal and private information, that would seem to not be a bad thing.

Mr BLANKS: Yes, that is right.

Mr DAVID SHOEBRIDGE: I would like to ask you about one other point—that is, in terms of a tribunal or a court to determine these matters. What we do not want is for it to become like the defamation laws—that is, a rich person's pleasure. I noted in your earlier evidence you were saying that if the party purportedly at fault is a Government organisation then it could go to the NSW Civil and Administrative Appeals Tribunal [NCAT] but if it is a private versus private dispute then the NCAT would not be the jurisdiction. Could I ask you to take on notice whether or not you think NCAT might be able to be given that jurisdiction as a potential avenue in New South Wales, or perhaps you can answer that question now?

Mr BLANKS: I cannot answer it now, or I would have to answer it with a question—that is, does NCAT have any jurisdiction at the moment for private disputes? I am not aware of any.

Mr DAVID SHOEBRIDGE: No, but it has an array of jurisdiction from the professions all the way through to government information.

Mr BLANKS: Yes, that is right.

Mr DAVID SHOEBRIDGE: Does the NSW Council for Civil Liberties have a policy position about whether or not NCAT's jurisdiction could be extended to deal with a private individual and a private organisation or two private individuals having a dispute determined?

Mr BLANKS: We do not have a policy position on that, but we will take it on notice and come back to the Committee on that.

Mr DAVID SHOEBRIDGE: Thank you, and could you include in your answer whether or not you think that might be a cost-effective venue.

Mr BLANKS: Yes, my experience with the NCAT is that it is no cheaper than a court—at least in the sort of matters I deal with.

The Hon. LYNDA VOLTZ: That is good; you can express that when you take it on notice.

The Hon. DAVID CLARKE: And, in taking that on notice, could you make any suggestions with regard to alternatives if you come down on the side of the negative on NCAT.

Mr BLANKS: Yes.

CHAIR: Thank you very much for coming today. For any questions you have taken on notice you have 21 days in which to respond. If there are any additional questions arising from Committee members, we will also send those through to you. Thank you very much for appearing here today.

(The witnesses withdrew)

(Short adjournment)

PROFESSOR BARBARA McDONALD, Professor, Faculty of Law, University of Sydney, and

PROFESSOR ROSALIND CROUCHER AM, President, Australian Law Reform Commission, sworn and examined:

MR JARED BOORER, Acting Principal Legal Officer, Australian Law Reform Commission, affirmed and examined:

CHAIR: I welcome you all to this inquiry. Would anyone like to make an opening statement?

Professor CROUCHER: Thank you. The Australian Law Reform Commission [ALRC] inquiry, which forms the essence of our submission to this Committee, was a specific inquiry that looked at designing a cause of action in relation to serious invasions of privacy, but it also looked at the issue of serious invasions of privacy more generally. The issue of whether or not there should be a cause of action was in a sense the result of a previous ALRC inquiry on privacy that concluded in 2008. We had recommended in that inquiry the introduction of such a cause of action but it was in a fairly at large sense. So the specific project that Professor McDonald led as the Commissioner of the ALRC last year was to design the statutory cause of action for serious invasions of privacy. But there were a range of other matters that we traversed in that report that are raised in your terms of reference, hence we thought it was a good idea for us to make a submission in relation to our work—to bring it to this Committee's attention and to make ourselves available. I am grateful that Professor McDonald was able to join us, as she was the commissioner leading it, and Jared Boorer worked very closely as the senior legal officer working on that inquiry at the time.

The Hon. LYNDA VOLTZ: In evidence to this Committee the term "revenge porn" has been used a lot. In your submission you refer to "the intentional infliction of emotional distress". The term "revenge porn" has a very narrow definition—for example, taking someone's photo when they are naked and sending it or any naked photo. Is the expression "the intentional infliction of emotional distress" the correct or broader term that should be used?

Professor CROUCHER: If I may answer first and then invite Professor McDonald to address it. The matters that you have raised touch on two broad things. One was the particular cause of action that we designed, which has a very high threshold and involves intention, which is one of the matters you alluded to, but we also traversed the limitations currently within the action for breach of confidence where currently those kinds of revenge porn cases would sit. We were at pains to provide a possibility of amending the particular breach of confidence laws in themselves in the event that the principal element, which is the statutory cause of action for serious invasions of privacy, were that not to be introduced.

We also had some very specific recommendations in the areas of breach of confidence to address some of the current limitations of the law. It is still a matter of evolving jurisprudence, principally in the equity jurisdiction, and it has particular limits, especially in relation to the limitations on what compensation may be available. There have been some nudges, one in Western Australia after our report and in Victoria, towards expanding the common law via the equitable action. But at the moment that is still fairly embryonic jurisprudence and we suggested in relation to the breach of confidence area, quite apart from any statutory cause of action in privacy, that there was a need for some amendment there. But perhaps with respect to the specifics of your question may I ask Professor McDonald to address those?

Professor McDONALD: You are quite right that the term "revenge porn" is a very particular type of invasion of privacy, and it certainly would be encompassed within a more broad civil action for serious invasion of privacy. It is already, of course, known and there have been actions in law for what would be called revenge porn because generally speaking it is some sort of image or information obtained during a relationship of confidence, such as a personal relationship. So there have been cases for decades where people have taken action to stop the revelation. The trouble with the internet is that generally speaking it is up there before you can stop it, so then the question is: What is the remedy after the event? The equitable jurisdiction, which is also concerned with things like trade secrets as well as personal secrets, has not developed a well-accepted remedy of compensation for emotional distress, which is the most common consequence of an invasion of privacy. People do not generally suffer economic loss or personal injury or actual psychiatric illness—they might do—but generally speaking they suffer just mere distress. The law is always very reluctant to give compensation just for distress in many other contexts, but it clearly is a remedy which should be given, I think, for that sort of action or revelation of personal information.

Now if the statutory cause of action were not introduced with a broad action, there would still be a way that the law in a particular State could be changed to allow the courts to grant that remedy. Recommendation 13.1 of our report recommends that appropriate State or Territory legislation could be amended to provide that remedy. This would go some way to giving victims of revenge porn a way to bring action themselves. The other way to look at it, of course, is to look at criminal penalties for that sort of behaviour. There are pockets of criminal liability for this sort of conduct. It is not apprehended violence, so somebody cannot go and get an apprehended revelation order. So it is not violence. They may not have used the telecommunications network to harass someone, so it would not fall in the criminal penalty there. So there are gaps in the law. One way would be to look at harassment. England and New Zealand both have more protection from harassment than we have. Harassment can be by that sort of revelation.

The Hon. LYNDA VOLTZ: In New South Wales, for example, you could make it a crime to transmit a naked picture of someone without their permission?

Professor McDONALD: You could.

The Hon. LYNDA VOLTZ: You could make it a criminal offence?

Professor McDONALD: Yes, you absolutely could do that. I would tend to think that you would want to look at the subject matter more broadly than naked pictures because the person might not be naked but it might still be a very personal detail, for example. There would have to be care given to what you are actually trying to protect here. Really what you are trying to protect is private information that has been revealed in the course of a relationship because it may not just be the images of somebody naked. There might be other information that people are using against their former partners in a manipulative way.

The Hon. LYNDA VOLTZ: So you could have your statutory responses and you could have some things falling within the Crimes Act in the more serious cases?

Professor McDONALD: You could. If you did have a criminal offence, that might also—depending on victim compensation schemes—then give the victims some ability to claim compensation. But victim compensation schemes tend to be limited to more serious types of offences.

The Hon. LYNDA VOLTZ: The Parliament has recently had some debate about that.

Professor McDONALD: It is good to think of a way where the victim can take action themselves rather than having to rely on the police to do it.

The Hon. LYNDA VOLTZ: I want to ask about one other element of your submission. In terms of defences you recommend an exemption for children and young persons. Will you define what you mean by "young persons"?

Professor McDONALD: This was something I have to say that came up quite late in the piece of our inquiry. We had quite a few discussions with the Children's Commissioner at the Human Rights Commission and we are very conscience that anecdotally we are told that children or young people—so under the age of, I do not know, it could be 16, could be 14 or could be 15—are sending images of themselves without a consciousness of how this could be an invasion of someone else's privacy, where it can lead to, and you cannot get it back once it has been sent. We were concerned at the idea that a 14-year-old would be suing someone else for invasion of privacy at that age. Children can be liable for a tort—there is normally not much point in suing them because they do not have assets—but we felt that there needed to be some recognition that these things are going on and it is only when a person gets to an age where we can expect them to have that sensibility that they should be liable to pay compensation for what they do.

The Hon. LYNDA VOLTZ: Do you have a legal definition for a young person?

Professor McDONALD: We did not suggest one. We suggested that the definition should be consistent with other legislation dealing with young people.

The Hon. LYNDA VOLTZ: Is it someone under 18 or someone under 16?

Professor McDONALD: That is a matter for debate, and the Committee would need to look at consistency with other legislation, but I would have thought it would be under 16 or possibly under 14. Under the Minors (Property and Contracts) Act 1970, 16 is the age at which a young person could give consent to medical treatment, for example. There is an awareness in other legislation that at certain ages, well under the age of 18, young people begin to have sufficient consciousness to take responsibility for their own actions.

The Hon. LYNDA VOLTZ: I am saying this because I have two teenage daughters. These actions on the internet can cause great distress to teenage girls. They become easily distressed. I used the example earlier that if someone wrote something nasty about me on the internet I would ignore it; if someone wrote something nasty about Miss 15, she would cry for the next 50 years. It would be devastating for her. I understand the ability not to sue, but is that not the crucial age where we want to change the social norm? That is the age where some of the worst offences occur.

Mr DAVID SHOEBRIDGE: But you do not want to take that to the Equity Division of the Supreme Court.

The Hon. LYNDA VOLTZ: No, I do not want to take that to the Equity Division of the Supreme Court.

Professor McDONALD: It may be that there needs to be another sort of complaint mechanism. The Office of the Children's eSafety Commissioner has been introduced by the Federal Government with that idea. There are ways of complaining to that body, and that may be a better way to deal with young people.

The Hon. LYNDA VOLTZ: Using a different mechanism, yes.

Professor McDONALD: You need to be very careful about criminalising the behaviour of young people.

The Hon. LYNDA VOLTZ: I am not suggesting that we lock up 15-year-olds.

The Hon. BRONNIE TAYLOR: I also asked this question of the Privacy Commissioner. I do not have a law background. Because there is no deterrent in place, there is no line in the sand. The issue is not whether someone is 15 or 16 or whether one person will respond online at ten times the volume of the other person's responses. The issue is that people are out there doing this. It is having serious consequences for young people. Because there is no deterrent, do you think that it has been allowed to go on? It is very easy to cut and paste something and share it on the internet. There is no deterrent within the system.

Professor McDONALD: We have had feedback that one of the benefits of having a statutory action for serious invasion of privacy would be that it would have a normative effect on behaviour. Schools, and the Children's Commissioner from the Australian Human Rights Commission, have said that they would like to be able to tell pupils that it is against the law to seriously invade other people's privacy. It is not so that people can rush off and sue but so that there is a law that people can point to and say, "It is not lawful to do this sort of thing." The question then is what the consequence should be, depending on the age of the person.

The Hon. BRONNIE TAYLOR: We need to acknowledge that there has been a lot of education about this, along the lines of: "Do not send that. Think about what you are doing. It will be there forever." But it is still happening and we are here today.

Professor McDONALD: Yes. It is a new method of bullying that is very serious.

Professor CROUCHER: Teenagers need to have a sense that they can get into trouble.

The Hon. LYNDA VOLTZ: That is right. That is why I was worried when I saw it there as a defence. The teenage years are possibly the age where education works best. I take your point: It is about changing the social norm.

Professor CROUCHER: The normative quality of it.

The Hon. LYNDA VOLTZ: That is right.

The Hon. BRONNIE TAYLOR: They need to know that it is unacceptable.

The Hon. DAVID CLARKE: My question is to anyone who would like to answer it. You say that you have provided a legal design for a statutory cause of action. You were asked to do that. Did you look to a particular jurisdiction for inspiration, and were there any jurisdictions that you wanted to avoid?

Professor McDONALD: Yes. At the design stage and the elements stage we drew on the law that has been developing in the United Kingdom and in New Zealand. They are two countries where the common law has developed a remedy or an action for invasion of privacy without waiting for Parliament to do it. The English courts have been able to do it because the United Kingdom became a signatory to the European Convention on Human Rights. The United Kingdom introduced a Human Rights Act in 1998, which required their government bodies, including the courts, to give proper recognition to the European Convention on Human Rights, which requires protection of privacy and protection of freedom of speech in the public interest.

The English jurisprudence in the courts has developed significantly since about 2000. The Naomi Campbell case was the famous case that started it. The United Kingdom has developed a very effective law on serious invasions of privacy. It is concerned mainly with the misuse of private information but also with the other primary method of invading privacy, which is called intrusion into seclusion. That is where somebody sets up a video camera to film somebody in the shower or follows them around, or something like that. The English jurisprudence has developed in that way, through the courts, so they do not need a statutory cause of action. They had an inquiry about that. It found that they did not need it because they have already developed the action.

In New Zealand the courts have developed a tort of both misuse of private information and intrusion into seclusion. In both countries, certain elements have been recognised as important. First of all, the person must have a reasonable expectation of privacy in the circumstances. Justice Gleeson, in our High Court, referred to that in a case called *Australian Broadcasting Corporation v Lenah Game Meats* in 2002. There is quite a lot of agreement by judges, lawyers and commentators around the world that the threshold is whether the victim has a reasonable expectation of privacy in the circumstances. That is a matter of judgement and it depends on many factors, but that is the starting point.

We spent a lot of time looking at how to balance public interest. If you design a cause of action on invasion of privacy a lot of people will be affected by it, particularly the media, who are very concerned. Commercial businesses, which have private information, were very concerned too about becoming subject to this new action. Then there are all the other contexts in which it arises. Revenge porn is one; neighbourhood disputes with closed circuit television cameras is another. There are so many contexts in which privacy is an issue. We recommended a similar approach to that taken in the United Kingdom, which is that a person would be able to sue only if they convinced the court that there was no countervailing public interest.

Public interest is a threshold point that needs to be considered in determining whether there has been a serious invasion of privacy, because lots of private information is revealed. Our defamation laws used to give more protection until the uniform Defamation Act came in in 2005. It used to be that, as well as proving that something was true, in New South Wales you also had to prove that publication was in the public interest. That used to look after privacy significantly. The change in the defamation law opened up the ability of the media and others to publish true information with a defence for doing so. Defamation law no longer protects privacy in that way. There was very much a need to balance public interest in designing the action.

The other factor we were explicit about was the fault element. That was something the New South Wales Law Reform Commission left open when it designed a cause of action some years ago. That was part of the concern that people had about a cause of action. If you do not know when you will be subject to it, or what fault is required, then it leads to great uncertainty and unpredictability. We recommended that the fault requirement be intent—the intention to invade someone's privacy. That includes recklessness. You cannot hide behind your own moral inability to see the problem.

Intent is looked at subjectively and, to a certain extent, objectively—that is, whether a person would realise that their actions would invade privacy. We thought that was important because if you leave open the fault element then it will involve a lot of people in actions. In the negligent tapping of "reply all" to an email or sending an email to the wrong person you might reveal private information mistakenly, but should you be sued for that? We were a bit concerned about that. Our brief was to find a remedy for serious invasions of privacy and we felt the serious ones are the ones where people are doing it deliberately or recklessly.

The Hon. DAVID CLARKE: And that is being handled well in the UK?

Professor McDONALD: In the UK there is not a fault element in that way because theirs is not a statutory action. But I have to say that I have not seen a case where that is an issue in the UK, because usually the complaints are about something like revenge porn, which is clearly deliberate, or usually the complaint is somebody actually setting up cameras and so on in a certain way or it is the media publishing something and they intend to publish. So fault has not really been an issue in the cases, but we felt that if you are going to have a statutory action you had to be clear upfront.

The Hon. DAVID CLARKE: Did you look at Canada?

Professor McDONALD: Yes, we did look at Canada.

The Hon. DAVID CLARKE: What was your view there? Thumbs up or thumbs down?

Professor McDONALD: Some of the provinces in Canada have introduced torts of invasion of privacy and I think, generally speaking—I cannot remember offhand—there is a fault element in their design.

The Hon. DAVID CLARKE: Were you impressed by what they had there?

Professor McDONALD: Yes, I think it has been quite effective and, in fact, it has not led to a flood of actions for invasion of privacy in those provinces where it has been introduced. The media and others put up the view that this would open the floodgates to litigation, and that has not been the experience in the Canadian provinces that have introduced this.

The Hon. DAVID CLARKE: Can you provide us with a list of those provinces that you are referring to?

Professor McDONALD: Yes, absolutely.

The Hon. DAVID CLARKE: You can take it on notice if you wish.

Professor McDONALD: No, it is actually referred to in footnote 15 in chapter 7. Paragraph 7.19 of chapter 7 deals with the statutory torts found in four Canadian provinces. It is set out in our report, and also in chapter 3 in the overview of current law we also make some reference to what is happening internationally. Perhaps I will have a look for that while we are waiting for the next question.

Mr DAVID SHOEBRIDGE: Improving the current remedy at tort or providing an equitable remedy is all well and good for Naomi Campbell, but most ordinary residents in this State cannot afford to pay for some whispering, bow-tied barrister to take their case to the Equity Division of the Supreme Court. Surely we need to be able to come up with a much more practical remedy than that and recognise that unless we are going to leave this to just vindicating the rights of wealthy, there needs to be a better venue than our standard courts.

Professor McDONALD: I would say two things to that. The first thing I would say is that celebrities can have their uses sometimes, because what Naomi Campbell has done has clarified a legal remedy for the United Kingdom, which is of benefit not just to celebrities but to the ordinary person. So to a certain extent, once you have an action like that which someone has taken, if they have a right to privacy certainly ordinary citizens do and it can be protected.

Mr DAVID SHOEBRIDGE: But if you turn up to a lawyer, they say, "Well, if you have got 60 grand to throw in the kitty then we will talk to you", that is not much of a remedy for most people.

Professor McDONALD: Exactly, and we were very concerned with that. That can be dealt with, of course, as to the jurisdiction of who has the power to hear these sorts of complaints and give a remedy. We are, of course, constrained by our constitutional constraints as to who has the power to order these things. We had discussions with the Australian Communications and Media Authority [ACMA] about a more effective complaint mechanism against the media, for example. At the moment the complaint mechanism there is merely that—a complaint; there is no ability of the ACMA to give any sort of financial remedy, whereas if you go to the Privacy Commissioner, the Privacy Commissioner can recommend a financial remedy, which can be

enforced in a Federal court. There are some gaps and I agree with you; we looked very carefully at alternative dispute resolution and who could have this power. But it is quite a complex constitutional issue.

Mr DAVID SHOEBRIDGE: New South Wales does not have the complicated constitutional issue in terms of the separation of powers with the courts to the same extent as the Commonwealth. Should we be looking at, as one of the key parts of any statutory reform, making sure that the remedy is available to people with ordinary means?

Professor McDONALD: Yes, absolutely. There are various ways you could do that, I think. Obviously, jurisdiction could be given to the civil tribunals at the Local Court stage for relatively simple matters. For neighbourhood disputes, which are a very common problem with CCTV footage, we recommended in our final chapter that there be a low-cost dispute mechanism, say, in the Land and Environment Court, no costs, such as with dividing fences, the same sort of thing, that there should be a mechanism there. I think those are probably the key ways that we would suggest.

Mr DAVID SHOEBRIDGE: One of your recommendations is the idea about the fault element, that the invasion must have either been committed intentionally or recklessly. I will give you the example of the Ashley Madison case where an organisation—and I am not asking you to form a final conclusion about it—the allegation is that the organisation was negligent in properly protecting the privacy of thousands of people. That negligence meant that it was accessed by a third party and then distributed to the world. Is it okay that there is no statutory remedy there?

Professor McDONALD: It is not to say there is no remedy.

Mr DAVID SHOEBRIDGE: No statutory remedy proposed to uncover it.

Professor McDONALD: That is right, but people who have given their private information to a website like that, which has promised confidentiality, clearly there are contractual obligations there and equitable obligations of confidence.

Mr DAVID SHOEBRIDGE: You might have pressed that "agree" button with five pages of detailed records, which you said were waiving all those rights.

Professor McDONALD: Yes, and that is a consumer protection point, of course, that people are very ready to accept privacy policies which really are non-privacy policies when you read them carefully. But also the Privacy Act would cover the activities of Ashley Madison in Australia because it is an entity with more than a $3 million turnover, so it is bound by the principles of the Commonwealth Privacy Act if it operates in Australia.

Mr DAVID SHOEBRIDGE: I am talking about giving people a statutory remedy in those circumstances. Your model would not give them a statutory remedy in those circumstances.

Professor McDONALD: No, our model would not, that is right, because really we were concerned that if you give people a remedy in that sort of situation, that is going to affect the remedy you can give to other people who are the subject of deliberate invasions of privacy. For example, if you opened up fault to negligence or even what is called strict liability, where you do not even have to prove fault, then it would not just be Ashley Madison who would be caught in the web of actions for invasion of privacy; it would be a whole range of people who negligently revealed some information about someone.

Mr DAVID SHOEBRIDGE: Could you not put a statutory obligation on, if they are a larger organisation, their amassing data of a particularly confidential nature? Could you not give them a statutory obligation to protect that data, and if they failed to protect that data that could be an entrée to the statutory remedy?

Professor McDONALD: Yes, and I suppose if you did that you would then have to think about what sort of damage are you going to remedy in a situation like that. If the people have suffered economic loss or psychiatric injury, they would already have, I would think, a very good action in negligence anyway.

Mr DAVID SHOEBRIDGE: They just may be distressed and humiliated.

Professor McDONALD: But if it is distress, possibly it would open to a lot of class actions for distress, I suppose, and certainly the class action lawyers were very interested in that sort of remedy being available in those sorts of issues. But there are many situations where people suffer distress from terrible negligence on the part of other people. You just have to look at our civil liability legislation in New South Wales; it requires a recognised psychiatric illness. So if somebody, for example, witnesses their child being killed or injured or imperilled by another person's negligence, there is no action for their emotional distress in that situation—our statutory law says that there is no action. So we really do need to consider whether or not we are giving such priority to an invasion of privacy to allow that when we do not give that remedy to other people who suffer distress from other people's negligence in very serious situations.

Mr DAVID SHOEBRIDGE: But do you not see that with the accumulation of this mass data and tens of thousands, hundreds of thousands of persons' private information gathered in one place that unless there is some remedy for the breach of it, unless there is some remedy for the negligent protection of it, then just as with a teenager, where is the stick to improve the behaviour, to stop this behaviour in the future? That one breach is going to cause substantially more damage than even a serious breach that affects just one individual.

Professor McDONALD: I can see that, but I do think you have to consider how this would sit in our other laws as well. I suppose that is a personal view on my part. But I think you do have to see privacy within an appreciation of our other laws which restrict people from bringing action for mere distress in very serious situations.

Mr DAVID SHOEBRIDGE: But they tend to be individual cases. It is an appalling thought, the distress someone would suffer from the negligent killing of their child if they do not suffer a psychiatric injury and they cannot prove the damage, that is an individual or a small caucus of people who are impacted by that. We are talking here about organisations that, through their negligence, can cause distress to tens or hundreds of thousands of people. We are talking about a unique, specific issue here.

Professor CROUCHER: If I may make a suggestion. There is already considerable management of information requirements that are reflected under the privacy principles in the Federal Privacy Act which places quite a high threshold of responsibility in relation to information management and also specifies a range of authority that the Privacy Commissioner may have with respect to those things. There is also the communications authority that Professor McDonald referred to.

I think, when one looks at these matters as lawyers and law reformers the issue is not wanting to make something be a universal panacea for all of the problems that arise in relation to information mismanagement. There are specific gaps in the law that we were concerned to address in the report that we did. It does not lessen the issues that you have raised, Mr Shoebridge, at all but it is not necessarily this particular action or enlarging the breach of confidence action that might resolve all things for all situations.

So when we were looking at this particular issue, we were mindful that other aspects of law deal with some of those egregious problems to which you referred. It is ensuring that the mischief that we were wanting to redress was covered in an appropriate way but not necessarily pressing it into service beyond that particular mischief that we were asked to look at. I am not suggesting that the concerns you raised are minor; they are indeed most significant but there are other aspects of law, both Federal and State, that are aimed at dealing with some of those big data management problems.

Professor McDONALD: Perhaps I could add a rider on one point, that the breach of confidence action is actually a strict liability action so that Ashley Madison, for example, would be already strictly liable under equitable law for the breach of their customers' confidence. And so that if the law were changed to allow a remedy for emotional distress for any breach of confidence of private information, then that actually would have the same effect as a statutory action for invasion of privacy.

Mr DAVID SHOEBRIDGE: That is the whispering bow-tied barrister avenue for review, isn't it? That is an equitable remedy. It is expensive and hard to access for ordinary citizens.

Professor CROUCHER: There is also the normative element of law that we were talking about before and that is where I think the greatest argument is really in support of the kind of filling of the gaps that we were looking at.

The Hon. BRONNIE TAYLOR: I may have missed this because I am not a lawyer but I would like to ask you something. My impression from your submission is that you were suggesting that we need to look at a Federal Act, rather than doing something through our State law. So I am wondering why you think that it needs to be introduced at a Federal level and what would be the negatives—and there are lots of benefits—to having State laws? Can you explain that to me, as a lay person?

Professor McDONALD: Yes. I suppose we are a Federal law reform body so one of the issues that we have seen from our defamation law, for example, and our civil liability regimes and many other regimes that affect people around the country, is that there is enormous cost in the variation of laws and lack of uniformity. For example, we have a chapter on surveillance devices, pointing out the enormous disparities between what you can do in New South Wales and what you can do in Victoria. We felt that, if there is to be an action, it should be the same for anyone living in Australia. It should not depend upon which state you live in. That is not your concern. I know that your concern is the other laws of New South Wales. But from a holistic point of view, it would be preferable for law to be uniform around Australia. That can happen in two ways: either by Federal legislation, if the Federal Government has the power to do it, as we suggested they did; or it can happen by uniform laws, such as the uniform defamation laws which happened, after decades of disagreement, but there is now a uniform system.

The Hon. BRONNIE TAYLOR: But because it has not happened Federally, it obviously is a big issue because here we all sit and we have all had examples of that, I am sure, in our own lives and in our families. Do you think that perhaps if New South Wales took a lead that that may be a very good thing and that that may encourage other states, or perhaps the Federal Government, to look at that?

Professor McDONALD: Well it may well do, as it eventually did for defamation law. Eventually the States did get together. You could use the Standing Committee on Law and Justice to try to encourage the other states to join with you.

The Hon. LYNDA VOLTZ: Or the Council of Australian Governments [COAG] process.

Professor McDONALD: Yes, or one of those processes, I agree that would be very good. The South Australian Law Reform Institute is looking at the same issue. I assume you are aware of their inquiry and submissions and so on. They are also looking at it and I am sure that, if New South Wales took the lead, perhaps it could be with South Australia. What I think is very important is that it is uniform.

The Hon. LYNDA VOLTZ: We have done that with legislation in the past. Work health and safety is one example, where the states had a common regime, so that you could cross borders to do that.

Mr DAVID SHOEBRIDGE: What the Hon. Bronnie Taylor was progressing was that, if we wait for a uniform national outcome, it may never happen.

Professor CROUCHER: You could take the initiative.

Mr DAVID SHOEBRIDGE: New South Wales could do two things: It could take the initiative to start trying to get a national uniform law; or it could take the initiative by legislating and then seeking to bring others on board afterwards. There is nothing inherently wrong with that second option, is there?

Professor McDONALD: No, there is not and it would have the effect of making New South Wales the privacy capital of Australia, in terms of privacy litigation because the tort is committed where the material is downloaded, for example. The applicable law is where the tort is committed so that if something happens in New South Wales or the information is downloaded in New South Wales, then there will be jurisdiction there.

The Hon. LYNDA VOLTZ: There is significant research already. It is not like we are starting with the underlying research and commitments. There has been considerable research in this area already.

Professor McDONALD: There has.

Mr DAVID SHOEBRIDGE: And if we wanted to put something forward that was more likely to be nationally adopted, probably a good starting point would be what your commission has turned up with after doing a national consultation.

Professor CROUCHER: Indeed and the detail that we provided, which was one of our main tasks was to design that cause of action, you get the detail that enables people to decide—particularly Parliamentarians—it makes it easier so you know what you are voting for.

Mr DAVID SHOEBRIDGE: You are saying you have to pre-chew it for Parliamentarians?

Professor CROUCHER: No I would not suggest anything like that. That is your suggestion Mr Shoebridge, not mine. Because people know what they are getting, it is not as abstract. The 2008 report commended the idea, with some precision, but it commended the idea. What we were asked to do was to put flesh on those bones. So you get a very thorough consideration of it. Yes, it is designed as a Federal statute, or the suggestion was that, because that was our brief. But as you appreciate, the Federal statute of course can then trickle down by virtue of vesting of jurisdiction in the State courts under the Federal Act. But New South Wales can certainly lead the way.

South Australia was the leader in a lot of earlier legislation, like the equality of children and various other legislation of that ilk and then the other states followed, and you ended up with essentially uniform legislation. So uniformity can be achieved in many different ways. It obviously makes it easier, both for those who suffer and for those who assist in the suffering, through the courts of law. But it can be achieved in a range of ways. Certainly this is a really serious issue. It has been identified nationally. It is crying out for some leadership, and that can be done by the State Parliament as well as by the Federal Parliament.

CHAIR: Professor McDonald made a comment about making New South Wales the privacy State. What would happen in a situation where you have residents whose privacy has been breached and they reside in New South Wales but the act of downloading or transferring the images occurred in another State or Territory?

Professor McDONALD: I have not looked at this so this is just my off-the-cuff reply.

CHAIR: I am happy for you to take it on notice.

Professor McDONALD: I might have the law wrong on this. It might be something I need to take on notice. Generally speaking, if it is a tort the law that is applicable is where the tort was committed. But it may also depend on whether or not, when the New South Wales Parliament enacts it, the intention is that the law applies outside New South Wales. As long as you are a New South Wales resident, or you have some connection, it does not matter if it occurs in Western Australia; it is intended to have some operation. I am a bit fuzzy on that aspect.

The Hon. LYNDA VOLTZ: When you take that question on notice would you look at the New South Wales legislation regarding commercial surrogacy which is exactly that—extra territorial offences for residents of New South Wales?

Professor McDONALD: Exactly, that is right. And it has been considered by the High Court in relation to the extra territoriality of the Civil Liability Act, for example, so there is a case that deals with it. The point is that it will certainly protect people where this occurs in New South Wales. That is obviously the starting point. It will occur in New South Wales, according to a case called *Dow Jones & Co Inc. v. Gutnick*, where the publication is downloaded. If it is downloaded in the jurisdiction then it is published and it occurs here.

CHAIR: Thank you for appearing before the Committee. You have 21 days within which to respond to any questions taken on notice. Additional questions may also be sent to you and again you will have 21 days following receipt of those.

Professor McDONALD: Thank you and good luck with your project. We are glad that you are interested in it.

(The witnesses withdrew)

(Luncheon adjournment)

NICOLA HENRY, Senior Lecturer, Legal Studies, La Trobe University, and

ANASTASIA POWELL, Senior Lecturer, Justice and Legal Studies, RMIT University, affirmed and examined:

CHAIR: Would either of you like to make an opening statement before we commence with questions?

Dr HENRY: We would like to start by thanking you for inviting us to give evidence. Unfortunately, our colleague Dr Asher Flynn was unable to attend today's hearing. We want to also point out that we are not lawyers; we are socio-legal and criminology academics. We are at the beginning of a revenge pornography project funded by La Trobe University, which is exploring the scope and impacts of criminal legislation, and it is also exploring the prevalence of revenge pornography by conducting the first Australian national survey on revenge pornography. Dr Powell and I are also in the final stages of our Australian Research Council discovery project, where we have been looking more broadly at technology-facilitated sexual violence and harassment. We released some results of that study just recently that we are happy to speak about today.

Mr DAVID SHOEBRIDGE: Can you tell us the results of your study?

Dr POWELL: We just recently released a report—in fact, since our submission—which I will be happy to provide afterwards, which details the findings of our study. The study included a survey of 3,000 adult Australians. Our study was focused on adult experiences—it does not cross the experiences of children and young people—and it was about a range of experiences of technology-facilitated forms of sexual violence and harassment, only some of which might be considered invasions of privacy. It included a range of criminal harms—threats, violence, stalking, domestic violence-related harms, gender and sexually based harassment—as well as questions around the threat or distribution or actual distribution of nude or semi-nude images without permission. One of the key findings from that national survey is that we found one in 10 Australian adults reported that a nude or a semi-nude image of them was sent to others without their permission.

Mr DAVID SHOEBRIDGE: One in 10?

Dr POWELL: One in 10.

The Hon. LYNDA VOLTZ: That is within the age group though?

Dr POWELL: That is within the age group of 18 to 55-year-olds, adult Australians. It was a survey of 3,000 Australians. It was quota sampled, if you want this information in terms of the census data to mirror representation both across gender and age brackets, so we do have population-relevant findings across those demographics. One in 10 reported that they had experienced this particular behaviour. Unfortunately, we do not have the context of the circumstances in which those images were taken—whether it was, for example, by an intimate partner or by friends and family or in other circumstances by an unknown person with unauthorised access. We are conducting further research through our revenge pornography study to do that.

Mr DAVID SHOEBRIDGE: Is your sample statistically reliable? What degree of confidence do you have about that?

Dr POWELL: This finding is significant to the 0.01 level, if that makes sense. So it is very robust finding. It is based on a very large dataset that is comparable to the Australian demographic for that age group, according to Australian Bureau of Statistics [ABS] data. We are very confident of that finding. The other factor that makes us confident is that the prevalence data we have found compares well to international studies on sexting behaviours, where images have been shared with others. It also compares with studies in Australia on the sexting behaviours of young people that have found similar numbers. Between 6 per cent and 10 per cent of young people have had their image shared, sent on or shown to another person.

Mr DAVID SHOEBRIDGE: Have you broken it down in age demographics within the 18 to 55 range?

Dr POWELL: Not for that item specifically. I do not have that data in front of me, but I can take that question on notice and provide a breakdown of the data.

Mr DAVID SHOEBRIDGE: Thank you. I appreciate it.

Dr POWELL: We did find overall that behaviours were more prevalent amongst the 18 to 24 age group. I will look at particular items to respond to that question.

The other major component of our study that I would like to highlight is that we conducted 30 interviews with a range of law enforcement stakeholders and professionals. That included Victoria and Queensland police, but some of the trends may be relevant in New South Wales. We also interviewed a range of women's legal service providers and domestic and sexual violence support service providers about the kinds of cases that they were hearing about from women seeking support. Those interviews raised many concerns about the way that images were being used in situations of sexual and domestic violence. I can give a number of examples of cases that they told us about. I do not know how useful that is for the Committee.

CHAIR: That is fine.

Dr POWELL: For example, legal services told us about women who had given consent to an image being taken but then the threat of distribution of that image was used to harass and control them. The stories we have heard from women's legal service providers in particular are that women are reluctant to report domestic violence to police. They are reluctant to apply for intervention orders because they are fearful that the image will be sent to their family and friends through their social network. The impact of that threat carries a lot of weight if they are in a domestic violence situation.

The Hon. BRONNIE TAYLOR: Thank you for bringing that up. It is important to note that the threat of further action is intimidating for women. That is a great point. From reading your submission it is clear that victims suffer terrible psychological harm. How do you think bringing forward a claim will assist in addressing the harm? Court action is very public, which is often a problem for victims of domestic violence and sexual assault. These people have experienced harm and then have to go public with it. What do you think about that? Could that have further psychological impacts? Is there a way around it?

Dr POWELL: I will comment on our findings in relation to harm and then invite Dr Henry to comment on the legal problems that that throws up.

The Hon. BRONNIE TAYLOR: That would be great.

Dr POWELL: The nature of the harm is poorly understood in the wider community. There has been a minimisation of the impact of the release of an image. The attitude is: Yes, that might be embarrassing but it ultimately is not a big deal. That is not what we are finding in our research. I cannot say it is one in 10, but a proportion of women experience that as a form of coercive control. They are shamed and humiliated by those images. It carries different weight in different contexts. For example, it has come to our attention through our interviews with women's domestic violence service providers that there are cultural values and layers around this.

An image might not be humiliating, shameful, embarrassing and distressing for one woman but for another it might be. For example, if an image is taken of a woman without her religious headscarf, the threat of that being distributed in her community could carry great weight. She may not want that aired in a public forum. It is a valid point that the process of justice may mirror the harm of having the image distributed in the public forum. There are concerns about whether victims should have additional protections—for example, to not be named and to have cases heard in a closed forum—because of the distress. Victims have also described to women's services, particularly sexual assault services, the experience of knowing that a sexual or explicit image is being circulated out there on the web, in the public sphere.

Mr DAVID SHOEBRIDGE: Just the threat of it happening is a concern.

Dr POWELL: Yes. They may be aware of the possibility of it happening but not know whether the threat has been carried out. It is a form of sexual violation that they carry with them as they go about their day. Victims have said that if someone looks at them strangely in the street they wonder whether that person has seen that image. This is not a one-off harm with an end point; it is something that victims carry with them.

Dr HENRY: I will add to what Dr Powell said about the impact and the importance of anonymity for victims who have experienced these behaviours. One issue is victim blaming. When a victim has taken the

image there is victim blaming—that is, the suggestion that he or she should not have taken that image in the first place. That is another reason victims might be reluctant to report to police or pursue civil proceedings. Another issue is when the public are aware that the images are out there on the internet somewhere. That might invite further harm to the victim, knowing that other people could go to those platforms and view those images.

Regarding the legal response, in civil and criminal realms, to the harms of so-called revenge pornography, we argue that there needs to be a range of options available to victims. There should be specific criminal offences that victims can report to police so that crimes can be prosecuted. We also support a statutory cause of action for serious invasions of privacy. We do not favour one option over the other. We think that both options are important because some victims prefer to use civil means to access particular remedies, including take-down notices—that is, having the images removed. Some of the remedies available in civil law might not be available in criminal law. We support a range of civil and criminal options for victims to address the harms of revenge pornography.

Mr DAVID SHOEBRIDGE: You said that the case studies you have looked at have been of women involved in domestic violence. Women's Legal Services have put forward a proposition to include powers within apprehended violence order proceedings. New South Wales has the Crimes (Domestic and Personal Violence) Act 2007. The powers would allow take-down orders, non-publication orders and orders directing people not to make good on threats within domestic violence proceedings. Do you think that might be a useful remedy for the people you have been talking with?

Dr POWELL: I do not have intimate knowledge of the law in New South Wales and the structure of the intervention orders. We have heard from domestic violence services that women are often too ashamed to disclose that there is an image. They find it difficult to request a condition in an intervention order that encompasses the image. Including it as one of a set of options in the legislation would be a proactive measure.

Mr DAVID SHOEBRIDGE: From your observations, is training police part of the solution as well?

Dr POWELL: Absolutely. We mentioned in our submission our support for a range of legal and non-legal options on this issue. This is a social issue. It is connected with broader issues of violence against women. It is about equity and respect. We can take a range of measures more broadly. That includes awareness raising and training for police and for providers of women's services, sexual and domestic violence support services, so that they are able to advise women on the available avenues for taking action and accessing support.

Police have told us that officers have a diverse knowledge of the way technology is used. A victim who elects to report to police could receive a variable response, depending on the skill level of the officer they report to. We have heard from legal and women's services and the police that there is a variable response that reflects the skills and knowledge of police. They are not necessarily equipped to take technological forms of abuse seriously. They perhaps minimise them and do not see them as real threats or real harms. They also may not know how to collect that evidence and present it as a robust case in a criminal sense. Certainly there are other avenues that we would suggest.

Mr DAVID SHOEBRIDGE: Sorry to go back to your figures again. You said one in 10 adults 18 to 55 have been a victim of—

Dr POWELL: Have had a nude or semi-nude image sent on to others without their permission.

Mr DAVID SHOEBRIDGE: If we were to break that up into gender, male and female, how does that impact on the figures?

Dr POWELL: Our finding was across both men and women for that figure. So that is both one in 10 women and one in 10 men.

Mr DAVID SHOEBRIDGE: So it was the same.

Dr POWELL: It was the same across genders. We asked some subsequent questions about the impact in terms of distress that was caused and also actions that were taken and what we found was that men tended to report lower distress and impact and they tended to not have taken action in response to the behaviours; for instance, not reporting it to a service provider, not reporting it to police, not seeking other advice. Whereas what we found was that women were much more likely to have made a complaint, to have shut down their account

and withdrawn from their participation in social networks, if that is where the harassment had occurred, and that they were much more likely to report experiencing distress.

We cannot say from our data what the reasons are for those differences, and that is part of what we are further exploring in our subsequent study—to understand better what are the different ways and contexts in which men and women are experiencing these behaviours; but they are certainly both experiencing this situation of images being sent on without their permission.

CHAIR: In your research did you ask about people's understanding of what they can do to address the issue and people did not understand or you did not do that survey?

Dr POWELL: No. Unfortunately, we did not ask them about their understanding of what avenues were available to them. That is certainly something we will be looking at in future research.

CHAIR: Did you ask people about receiving naked images, or was it purely just on having theirs sent on?

Dr POWELL: Our study was purely about victimisation experiences. That is further research that we are now conducting to look at a range of other perpetration behaviours as well.

Mr DAVID SHOEBRIDGE: In terms of your research in the area, how are you finding, say, the larger telecommunication parties? What, if any, role do they play in this in terms of having a ready response to complaints and proper complaints handling and resolutions internally?

Dr POWELL: We have not consulted particularly with those service providers so I cannot speak from that perspective, but this has come as an issue in a number of ways, one of which is a barrier that police have talked about in terms of both the time and the expense of pursuing action against social media companies and that being a barrier to them pursuing action in particular cases. For example, in revenge pornography it might be possible to use Commonwealth laws around telecommunications—using a telecommunications service to threaten, menace or harass. But to gather evidence for that might involve police needing access to Facebook data that shows that it was a particular user at a particular time, that it did, in fact, post that image, and still needing to prove that it was the actual person at the desk at the time posting that material. So there are a number of barriers of cooperation, but also the time that that takes to put in those orders for requests for information.

Mr DAVID SHOEBRIDGE: You have dealt with the Victorian police and the Queensland police in particular. Do they have, say, a skilled unit that assists more general duties police to do those inquiries or is it better to upskill the general duties police? How do you see it?

Dr POWELL: Police members have specifically raised to us their own concern that their cyber crimes unit and their central computer investigations unit is not well enough resourced to deal with the scale of these types of offences. Their resources, as was described to us by police, are very small and they tend to be prioritised to, for example, major task forces on child sexual exploitation material, as one example, and other very serious offences. So it has been suggested to us that either there needs to be further resourcing in that area or that there needs to be other mechanisms and tools for police at the local station. I do not have the expertise to comment on which of those would be the best way forward.

CHAIR: I just have a question in relation to your recommendation number 10, looking at prevention strategies. You particularly comment on tools for individuals to take action as bystanders. Could you elaborate a little bit more on if you have any specific suggestions in relation to educational programs or where things might work, particularly internationally?

Dr POWELL: We made a number of comments around prevention. One is that of course we have seen some prevention campaigns in Australia as well as internationally that are focused particularly on sexting amongst young people. Unfortunately, and this has certainly been the subject of other government inquiries including the Victorian parliamentary inquiry into sexting, some of those campaigns have had a really problematic framing of the issue. They have basically taken a don't sext approach, don't send an image, and, unfortunately, whether it is young people or adults, I do not think that is a very effective prevention message. It is impractical for a start in that technology is so much a part of people's sexual experiences and lives nowadays that to say don't participate is almost to say don't participate in sexual encounters.

But also it has a problematic message in terms of placing all the responsibility with the victim and placing absolutely no responsibility with people who send on those images, whether it is a partner under a revenge pornography circumstance or whether it is a peer group or a community who received the images and continued to send them on. That is where our comment in relation to bystander approaches really comes in because this is not just about educating people to say, "You as an individual don't send it on" as the partner who may receive the image and encouraging people to maintain that trusted privacy, but also to say that if a peer sends that to you, do not continue to send it on because you are then participating in the further humiliation and shame of that victim.

Mr DAVID SHOEBRIDGE: The shame should be in sending it on, not being the victim of it, and we cannot passively allow it not to be the case.

Dr POWELL: I think unfortunately what we have seen in the public discourse is that when cases are reported in the media and victims do come forward they get a very mixed response and too often they do get a very shaming victim-blaming response.

Mr DAVID SHOEBRIDGE: "We told you not to"—that sort of response.

Dr POWELL: Yes. That itself can create a barrier to people coming forward and reporting, because they do not know that they are not going to get that negative response when they report. So improving community conversation and awareness around the nature of the harms and where the responsibility for those harms lies I think is an important mechanism not just for a prevention approach but also for encouraging victims to come forward and seek support and make use of remedies that are available to them.

Mr DAVID SHOEBRIDGE: A number of Law Reform Commission reports have suggested that there should be a serious, proper statutory remedy for breaches of privacy. Your research tends to suggest that the people who are most affected by breaches of privacy, at least in your sub-class of data, tend to be women. The bulk of police and legislators tend to be men. Do you think that there is a minimising of the reality of the distress that has been caused?

Dr HENRY: We have not done a specific study around the minimisation of the kinds of responses from law enforcement officers or lawyers regarding these behaviours, but anecdotally there seems to be some evidence to suggest that victim blaming is happening and that the failure to introduce criminal legislation or the failure to introduce other measures might well be a reflection of the minimisation surrounding revenge pornography and other forms of technology facilitating sexual violence and harassment. Dr Powell mentioned before that there is some concern that police officers, when victims report to them, are not taking those claims seriously. So whether or not it is a reflection of some kind of double standards around gender and sexuality we are not quite sure, but it would seem that it is an issue.

Mr DAVID SHOEBRIDGE: Maybe it is men applying their standards to women, because one of the most interesting things I got from your data was that men and women are reporting the same amount of the sexting or the images, but that it is the response that varies greatly.

Dr HENRY: Absolutely. One of the problems is that if a woman who has had a sexually explicit image distributed without her consent, the ramifications of that, the impact of that, might be vastly different to a victim who is a male. Of course, it might not be and we would be clear to say that impacts can be very diverse and not all victims are going to respond in the same way. But certainly there are the kind of social constructions around gender and sexuality that exist in our society that make the distribution of internet images without consent quite problematic.

Dr POWELL: As an example, a sexual or semi-nude image of a man might certainly be humiliating, embarrassing and shameful but what we are seeing is that women are so judged on their sexuality, on their sexual reputation, and in quite moralistic terms, that they are then often the targets of subsequent harassment, shaming and exclusion on the basis of that. The example that has come from some international studies in the United States is where a woman's image has been circulated without her consent and then she has lost friends, family networks or professional reputation and standing because of that. And it is a gendered response, it is something about the way that we judge women based on sexual reputation that ultimately is something the law cannot change but that is something that would have to be addressed through broader work around the prevention of violence against women and the promotion of gender equity as an overarching framework.

Mr DAVID SHOEBRIDGE: Would you table your study?

Dr POWELL: Yes.

Mr DAVID SHOEBRIDGE: Have you published it?

Dr POWELL: Yes, we have released a public report and we also have a number of studies published in academic journals.

CHAIR: You said that you are doing further research now. Do you have a time frame for that? Obviously it depends on when we are reporting but if there was any information you could provide to us, even if it was just for the Committee to be able to use some of that, it might be of use.

Dr HENRY: The revenge pornography study that Dr Powell, Dr Flynn and I are currently engaged in began in September this year. We are hoping to run our first Australian online survey at the beginning of next year. We are hoping to have the results of that study by the middle of next year. We would be happy to share those findings.

Mr DAVID SHOEBRIDGE: It would be hard to report before then.

CHAIR: It will be very useful. Thank you for appearing here today.

(The witnesses withdrew)

KIRK McKENZIE: Chair, Human Rights Committee, Law Society of NSW and practising solicitor,

MAEVE CURRY: Committee Member, Communications, Entertainment and Technology Committee, NSW Young Lawyers, and

CHRISTOPHER JOSEPH CHOW: Chair, Communications, Entertainment and Technology Committee, NSW Young Lawyers and practising solicitor, affirmed and examined:

CHAIR: Before we commence questions, would any of you like to make an opening statement?

Mr McKENZIE: I would. First of all, I would like to say that our submission, which is submission number 15, was drafted by the Human Rights Committee of the Law Society but it is also agreed to by the Injury Compensation Committee. The way in which the Law Society works is that we have about 20 policy committees and people with expertise are appointed to those committees and the society tends to delegate its submission writing to those committees.

I will not address you at length because, as you will have seen from our submission, we are essentially supporting the views—not all but the great majority of the views—of the Australian Law Reform Commission in its 2014 "Report into Serious Invasions of Privacy in the Digital Era". I interpolate that, despite the fact that my young lawyer colleagues to my right produced a report entirely independently of our committee, the two submissions are quite similar.

We would like to focus attention on what we say is one of the key derivations of the need for reform in this area. That is that Australia, including the Commonwealth and State Parliaments, has an obligation under international law to provide effective remedies for breaches of privacy. That arises from Article 17 of the International Covenant on Civil and Political Rights which commits our governments to legislate to prevent a person being "subjected to arbitrary or unlawful interference with his privacy".

Australia had a close involvement in the drafting of the Universal Declaration of Human Rights of 1948, principally because of the activities and interests of a former member of this Parliament Dr H. V. Evatt. But it did not stop there. After the change of government in 1949 Australia had a representative on the 18-person Human Rights Commission which drafted the treaty that I have just referred to, the first draft of which was presented to the General Assembly of the United Nations in 1954. At that time Australia's representative was the Rapporteur of the Human Rights Commission and effectively he and the Chair presided over the first draft of that treaty. That individual was Mr H. F. E. Whitlam, the father of the former Prime Minister. That treaty took 12 years to draft. It was approved by the General Assembly in 1966, with the support of the Australian Government. It was signed on the 13th day of the Whitlam Government but was not ratified until the Fraser Government did so in 1980.

The reason I take you through that short history is because the Law Society says that human rights have been, for 60 years, a joint project. I know there is a lot of controversy as to the extent to which human rights should be incorporated into Australian domestic law but we say that this particular treaty, which was ratified for Australia 35 years ago, is a key source of fundamental rights and that, because of our obligation under international law, for that reason alone it is important to have effective laws on privacy.

The Law Society agrees with the Law Reform Commission that there are some key deficiencies in the current law and, in particular, noting the Committee's interest in the equitable action for breach of confidence, we ask you to note the reference in the Australian Law Reform Commission's submission to this inquiry to the effect that equitable compensation is generally only awarded in Australia to compensate for economic loss, and that courts are not empowered to award damages for emotional distress under that particular cause of action. That is a common law action that is not well-known in the community. There is no other way in which you can activate that other than by taking legal proceedings of a fairly serious nature. Breach of confidence is a reasonably uncommon cause of action in our courts. For those reasons we join the Law Reform Commission in viewing the law as deficient in that area.

Our submission has focused on damages as a remedy but we would like to emphasise that we also support the Law Reform Commission's alternative suggested remedies that are set out in attachment A to our submission, including an account of profits, under which anyone who profits by a breach of privacy has to account for them and or hand them over. They suggest also injunctions could be available, either temporary or

permanent; that there could be orders for the delivery, destruction or removal of material; that there could be an order for publication of a correction; and that the courts should have the power to make declarations. So it is not only damages that we submit are appropriate remedies.

We also understand that there may need to be caps on damages to stop compensation schemes getting out of control. We have seen legislative action in the past 20 years which places caps on other compensation schemes. This is not so much a scheme, I guess; nevertheless it might be appropriate for the Parliament to think about caps. I think the view of the Law Reform Commission is that this would best be approached on a national level, but the national Parliament has not done so.

In view of the fact that the New South Wales Parliament has the power to introduce such legislation, it should not be afraid of doing it. It could well take a lead in this area. It was not so long ago that the New South Wales Parliament was the most important Parliament in this country. The Premiers of this State until World War II practically exercised more power than the Prime Minister. The Parliament still has that power—it has not been taken away. This is the sort of legislation where, if the New South Wales Parliament took heed of the Law Reform Commission's recommendations and implemented an appropriately judged Act, it could well provide a lead to the other States and Territories. We do make some individual recommendations later in our submission, but perhaps I have said enough.

Mr CHOW: We would both like to make a brief opening statement on behalf of the New South Wales Young Lawyers' Committee which for ease I will call the CET committee—the communications, entertainment and technology committee. First, the CET submission is authored by a number of CET members. The CET committee has 550 members so obviously the views of the members vary dramatically. Trying to put together a submission that addresses all those views can be rather challenging. The particular authors all have their own areas of expertise and we anticipate that there will likely be questions that you put to us that we will need to take on notice to go back to those people.

The second point I would like to make is that in the experience of quite a number of the CET committee members it is apparent that there is a disconnect between the protection the law currently offers and the understanding our clients and our peers have of the protection that would be offered in a serious invasion of privacy. I think that is one thing that needs to be addressed. The only other comment I have—and I make this comment with due respect to the larger social and legal issue relating to the serious invasions of privacy—is that the clients and the people that have the means to fight a serious invasion of privacy battle are still also facing the same grey areas of the law that are not addressed properly at this stage as far as we are concerned. I think it should be noted that there is a need for even those people who currently cannot seek the right protection looking to the defamation laws and copyright laws and other breaches of confidence to try to protect what is ultimately a serious invasion of privacy.

Ms CURRY: I have a couple of points by way of introduction, and I thank you for the invitation to do so. First, by way of completeness, I am a practising barrister which I should have stated earlier in the piece. Privacy is a notoriously nebulous concept, and that I believe is the difficulty that is presented in trying to protect us from serious invasions. It is a basic human right, as has already been pointed out, and it is necessarily an individual right deserving of legal protection, perhaps now more than ever because of the impact that the internet and emerging technologies have had on the capacity for us to lose control over this right to privacy.

Importantly, our privacy legislation must be adaptable to emerging technology and unforeseen examples of privacy invasion. The equitable cause of action of breach of confidence does not cover the field of conduct. I understand that is the position of all but three of the submissions to this inquiry—that being that another statutory cause of action is necessary to do that because the equitable cause of action is inadequate to address the wide-ranging and far-reaching harms to victims of this type of harm, and the need to deter perpetrators from engaging in this type of behaviour.

Just as the law must develop to keep up with the social norm, so too must the social norm be developed by the law. I think that is an interesting concept that applies here in particular where we have an issue that could be addressed by the law but that currently is being addressed by perhaps some examples that have been given previously by education and that may not be enough. Coupled with making the conduct unlawful, even if does not apply to people of a young age, having the additional backing of that behaviour being recognised in law as unlawful, in combination, could have a deterrent effect, which ultimately is the missing piece in the legislation that currently applies to privacy laws in Australia.

The CET committee submits that there is a need, as I have said, to introduce the statutory cause of action for serious invasion of privacy. In particular, the committee endorses the recommendation of the Australian Law Reform Commission in that it would be split into two concepts of invasion of privacy—that being the misuse of personal information and intrusion upon seclusion. Additionally, uniform national law would be ideal but, as has been discussed, there is an avenue for New South Wales to lead the way, after consultation with other jurisdictions, so as to avoid conflating the uncertainty that already exists.

The final point I wish to make is to clarify our written submission at about paragraph 4.3 where we address the issue of whether the cause of action should relate only to wilful and intentional acts or whether it should also include negligent acts. This has been the subject of a question from Mr Shoebridge in relation the negligence of Ashley Madison, for example, and whether those types of acts should be caught by the statutory cause of action. In response to that we would say that a statutory cause of action perhaps would only apply to wilful and reckless acts and perhaps it is more appropriate that negligent acts or accidental acts be covered by other legislation. In particular, if we are looking at introducing criminal offences for conduct constituting a serious invasion of privacy it would be consistent with other criminal offences at both a State and Commonwealth level to include an element of intent.

The Hon. LYNDA VOLTZ: In submission No. 25 you state "... whether liability should only be imposed where the plaintiff had a reasonable expectation of privacy in all circumstances." Can you explain what you mean by that? I have read the next chapter relating to types of activities caught by the Act.

Ms CURRY: That is an endorsement of the recommendation provided by the 2014 Australian Law Reform Commission inquiry, which is a safety net, to use that word—whether or not the conduct in the circumstances could have been reasonably expected to have been covered in terms of whether or not there was a reasonable expectation in the particular circumstances of that case that there was a right of privacy or that there was a relationship of trust in existence. It is related to whether or not it is wilful or reckless conduct and whether or not there is going to be a fault element attached to the statutory cause of action. It also goes to whether or not the test will be objective or subjective. Having this element of proportionality and reasonableness, which would be an element of a subjective test, would ensure that some types of conduct which objectively may fit the purpose looking at all the circumstances, if there has been consent, for instance, and if that was not a specific element of the offence then it would not be caught by the cause of action. That is what I understood.

Mr CHOW: We do make a reference to *C v Holland*, a recent New Zealand case that actually addresses some of those issues. I am not specifically familiar with those but I am aware that the submission talks to those particular elements, one of them being infringing a reasonable expectation of privacy. If we were to look closely at the way in which it was addressed in the New Zealand case it would give some background to that particular element.

The Hon. LYNDA VOLTZ: How does that cover the example of someone who has given consent for a photo at some point and then years later someone reproduces it?

Mr CHOW: I am going to have to take that question on notice.

Mr DAVID SHOEBRIDGE: They are quite different things, are they not?

Ms CURRY: They are separate, yes.

Mr DAVID SHOEBRIDGE: You can consent to the image being taken but the issue about a reasonable expectation is what is then done with that image.

Ms CURRY: Yes, it follows through.

The Hon. LYNDA VOLTZ: That is the explanation I would like to hear.

Mr DAVID SHOEBRIDGE: Can you explain the difference? You might consent to having a photo taken but then there is a reasonable expectation that if that photograph has been taken in an intimate setting in a bedroom it is not going to be put up on Facebook immediately thereafter. Can you explain the limitation you are proposing, which comes out of the Australian Law Reform Commission?

Ms CURRY: The consent to whether or not the photo was taken in the first place would be a separate issue to whether or not you expect—therefore implicitly consent to—its future distribution past the first point of it actually being taken. There are circumstances where you might have taken that photo of yourself and it has somehow fallen into the hands of somebody else and they have made a decision independent of your knowledge or consent to pass it along. It is at that juncture that this issue of reasonableness comes into play. We look at whether it was reasonable to expect in the first place that your right to privacy would have been respected at that point in time.

The Hon. LYNDA VOLTZ: Mr McKenzie, in your submission you state that your committee has some reservations in respect of recommendations 9-1 and 9-3 because it may enable the defendant to raise potentially spurious public interest issues and there would then be a requirement on the defendant to show a countervailing public interest. Would not the judge or a person adjudicating be able to decide about spurious public interest issues? Could you elaborate on why you are so concerned about that area?

Mr McKENZIE: We are concerned about that area because often a complaint about an invasion of privacy is inevitably going to be made against either a large public or private body and they would have the resources to defend these matters. If they do not have the onus of proving their defence then they could, simply because of their resources, prevail. Our view is that the onus should not be reversed in those circumstances. We just see that there is a potential for spurious public interest issues to be raised. Without being critical, I notice the media organisations that have made a submission to this inquiry have done so in very general terms.

Mr DAVID SHOEBRIDGE: They say there is no problem, nothing is broken and there is nothing to see.

Mr McKENZIE: There does not seem to be any problem from their point of view, but there is a great lack of specificity to their submission. I read it out of interest just to try to discern what their real issues are. I am not too sure that they are as well expressed in those submissions as they should be. I think in this digital age there is a problem with large organisations using the resources that they have to head off—

The Hon. LYNDA VOLTZ: We have just heard evidence from Latrobe University that one in 10 people have had an image of them reproduced. Overwhelmingly, that is not being done by the media. It is done by individuals. To an extent the Committee is really looking at what is described as revenge porn, although I do not like the term. They are images that are transmitted to cause emotional distress.

Mr McKENZIE: Yes. In our view, although the complainant would have the overall onus of proving their case, if you have a specific defence then the orthodox view of lawyers is that it should be the defendant who has the onus of establishing that defence.

The Hon. LYNDA VOLTZ: At the initial point they do, do they not? The way I read your submission is that it is on the plaintiff to refute those issues once they are raised in court.

Mr McKENZIE: Yes, but we are just concerned that the onus does not shift.

The Hon. LYNDA VOLTZ: I get what you are saying.

Mr DAVID SHOEBRIDGE: You are okay with having an element of the cause of action that the public interest in privacy outweighs any countervailing public interests, but should the onus be on the complainant in proving that the public interest is in favour of vindicating their rights or should the onus be on the defendant in proving there is some public interest?

Mr McKENZIE: If the defendant raises that as a defence or excuse then in our submission it should be their onus to establish that. But I am not suggesting for a moment that is not the complainant's overall onus to prove their case.

Mr DAVID SHOEBRIDGE: The Law Reform Commission did not include public interest as a defence. It said that as part of the element of proving the cause of action you have to satisfy the court that the public interest in privacy outweighs any countervailing public interests. That is going to be awkward, is it not, if you have to prove it in your cause of action?

Mr McKENZIE: Yes, we respectfully disagree with that particular finding.

Mr DAVID SHOEBRIDGE: But there are obviously cases where public interest would be compelling and should be a key part of the considerations. For example, if a predominant political figure is meeting with a prominent and controversial corporate figure in private they may have an expectation that their privacy will be respected. You should not intrude on their seclusion on the basis of the privacy principle but there may well be a strong public interest in getting that information out.

Mr McKENZIE: In the circumstances I do not think it would be too difficult to establish that defence.

The Hon. LYNDA VOLTZ: But perhaps in the example, say, of a member of an upper House who puts on a bra and starts snorting cocaine at a private party it might be more difficult?

Mr McKENZIE: Yes.

The Hon. LYNDA VOLTZ: I was thinking of the example in England not of anyone in our upper House.

The Hon. BRONNIE TAYLOR: My question is to Mr Chow and Ms Curry from NSW Young Lawyers. I note in your submission that you acknowledge that any legislation we may look at recommending should not impinge upon the right to freedom of speech. Could you elaborate on how there can be a balance between freedom of speech and the protections against invasions of privacy.

Ms CURRY: One way of addressing it is to ensure that certain defences are available, which are already available in actions in defamation, for example—qualified privilege, absolute privilege and so on. That goes some way to protecting the public interest. Perhaps another way would be to introduce what we were just talking about—a balancing exercise between countervailing public interest considerations. That really would be an exercise for a judicial officer to engage in. I imagine it would be done on a case-by-case basis, as evidenced by the examples already given—in one there was a strong reaction and in the other there was an even stronger reaction. So it would be difficult to define in the words of the statutory cause of action for that reason.

The Hon. BRONNIE TAYLOR: Mr Chow, did you have anything to add?

Mr CHOW: No, I do not think I am able to add anything at this stage at least.

Mr DAVID SHOEBRIDGE: I have not seen anybody anywhere support giving these privacy rights to non-natural persons—these should be limited to human beings. Are we all of one mind on that?

Ms CURRY: Yes.

Mr McKENZIE: Yes.

The Hon. LYNDA VOLTZ: Sorry, that was me. I was asking Mr Shoebridge what a natural or living person was.

The Hon. BRONNIE TAYLOR: Mr Shoebridge, did you steal another question? You have to stop doing that.

Mr DAVID SHOEBRIDGE: I was just trying to clarify that.

The Hon. LYNDA VOLTZ: I asked why a natural person is not a living person.

Ms CURRY: It is both though, isn't it, because natural rules out corporations and living rules out being able to action a cause of action once somebody has passed away.

Mr DAVID SHOEBRIDGE: There is dispute about whether the cause of action against somebody should survive their death, and there is also dispute whether or not the cause of action that somebody had should survive their death. What is your view about those two issues?

Ms CURRY: Consistent with defamation, I would suggest for consistency, in particular where you can across different legislations, that that be unable to survive the death of the plaintiff.

Mr DAVID SHOEBRIDGE: Even if proceedings have been commenced?

Ms CURRY: Yes, even if proceedings have been commenced. I say that, and we do address this in our submission, because the right to privacy is a personal right and that is its foundation. It is arguable that it dies with the person. If the person's estate was able to continue that claim, it would be difficult in most circumstances to prove the damage after the person is no longer with us.

The Hon. LYNDA VOLTZ: I have an example—what if there was an image being circulated of your daughter or son who had died. There would still be the ability to humiliate and distress other members of that family by the continued circulation of that image.

Ms CURRY: Yes, but in this circumstance it would have been commenced by that individual, being the plaintiff who has now died.

Mr DAVID SHOEBRIDGE: If you were being humiliated in that way, through somebody abusing an image of your spouse or child, you would have your own independent cause of action in those circumstances, arguably.

Ms CURRY: Arguably.

The Hon. LYNDA VOLTZ: Wouldn't consent then become an issue? Fundamental to the offence would be that you did not have consent.

Mr DAVID SHOEBRIDGE: What about the circumstance where you are being humiliated and the intent is to cause harm to person A by distributing humiliating images of their partner. Should the cause of action extent to that?

The Hon. LYNDA VOLTZ: You could take that question on notice; you do not have to answer it here and now.

Ms CURRY: That would be best taken on notice. It is an interesting area.

CHAIR: Another issue, which has come up in other submissions, is in relation to surveillance cameras and accidental recording, in particular with security cameras on a person's home. They could be motion sensor activated and could accidentally film neighbours. Another issue is the use of drones. Do you have any comments to make in relation to those issues and the privacy laws surrounding that?

Mr McKENZIE: I can say something on that. I think the difficulty is probably best seen if you look at the submission from Mr Greg Piper, I think it is submission No 3. He refers to two cases where essentially someone has trained cameras on the front yard or back yard of their neighbour and the neighbour has felt oppressed. The surveillance devices Act of this Parliament, although it prohibits audio recording without consent, does not prevent video recording without consent. Although we did not address that issue in any great detail in our submission, it struck me, upon reading that submission, that it really is something of a problem. I think submission No. 1 also referred to a 2010 Victorian Law Reform Commission report on surveillance devices. I have not had a chance to look at that but it might be something to keep in mind.

CHAIR: I am happy for you to take that on notice. Mr Chow, would your committee have any comments to make in relation to that? I am also happy for you to take that on notice.

Mr CHOW: I think that would be the safest course of action, thank you.

Mr DAVID SHOEBRIDGE: Someone suggested that the tort of nuisance might be available in those circumstances. Could you also take that on as part of your response?

Mr CHOW: Sure.

Ms CURRY: Yes, or trespass; it could well already be covered in those fields.

Mr DAVID SHOEBRIDGE: One of the primary concerns that I personally have, and I think it is shared by a number of people, is that we do not come up with a remedy that becomes the exclusive domain of the wealthy—we do not want to only come up with rights that can only be vindicated by wealthy and powerful individuals. Your submission pretty much adopts the Australian Law reform commission submission which talks about courts being the primary place where these rights are vindicated. We all know from experience that that is often a hideously expensive process and it excludes most ordinary Australians. What about a non-court remedy—either in a statutory tribunal or by giving the Privacy Commissioner certain remedies and powers. How do you feel about that?

Mr McKENZIE: There are difficulties with enforcement if you give it to a nonjudicial body. The reason I raised the reference in the submissions to other remedies is because I understand that that is a real issue. I note the rather impressive submission of the Women's Legal Services NSW.

Mr DAVID SHOEBRIDGE: Which is what I was going to go to next, so I am happy for you to address that now.

Mr McKENZIE: I cannot speak on behalf of the law society about that because we have not really considered that submission as a body, but speaking personally I was struck by the detailed recommendations about apprehended violence changes that might be appropriate. The difficulty with the local court jurisdiction in that respect is that the local court is already overloaded with apprehended violence cases. It is actually difficult for them to deal with them at any great length. It is not an easy problem to resolve.

Mr DAVID SHOEBRIDGE: Would you like to take that question on notice, take it to the committee and then bring it back to us.

Mr McKENZIE: Certainly, thank you.

The Hon. LYNDA VOLTZ: Also within that, one other witness raised the Australian Human Rights Commission as a model that has gone down that track.

Mr DAVID SHOEBRIDGE: What are the views of the NSW Young Lawyers about having a tribunal apart from a court, increasing the powers of the Privacy Commissioner and, finally, of the women's legal service solution of giving additional powers to the local court when domestic violence orders are being sought?

Mr CHOW: I would like to just briefly touch on the point of the delays in trying to solve these various problems. These can lead to a further postponement of the introduction of any laws that properly at least touch on this idea of serious invasion of privacy. As I mentioned in my opening statement of course there is a bigger issue of actually making it available to the public at large. It is a very important factor. Those people with the means are also missing out on the opportunity to protect their privacy. I think it needs to be again just noted that if these delays continue then we are delaying certain rights of people for the purpose of trying to, I guess, fix a problem that might take many years to actually fix properly. I think that those delays need to be considered very carefully. If there is an answer that at least can be resolved in the courts for those who do have means I think that should be considered.

The Hon. DAVID CLARKE: Is that something that you can apply your minds to and take on notice? Can you also give some thought to that? It will complement a very good report from the NSW Young Lawyers.

Mr CHOW: We certainly would be happy to make further submissions in relation to that position and the way in which that may be addressed if the Committee would like us to.

The Hon. DAVID CLARKE: That would be very helpful.

Mr DAVID SHOEBRIDGE: Essentially what you are saying is we need to do something—legislate, or get it right somehow.

Mr CHOW: That is exactly right. I think it is a great opportunity for New South Wales to really lead the way in this particular of the area of the law, as has been mentioned all morning, and I do think that there is some significant merit in just saying that we have to do something about this sooner rather than later and at least give some people the opportunity to fight the fight.

The Hon. BRONNIE TAYLOR: In evidence to this Committee it has been said that there is no framework or line in the sand and people are getting away with doing these things. Education is not enough and—as I think you said in your opening statement—if we combined something with that then we will have that line or framework that we do not have at the moment.

Ms CURRY: That is right. Once there is a statutory cause of action or a criminal offence both covering the same type of conduct then we have issues of general and specific deterrence. Another witness raised some issues earlier that that could lead to some additional problems for victims, in particular victims of this concept of revenge pornography, in having to relive the harm in a way they have gone through in order to seek the justice that this statutory cause of action would achieve for them, but even still having the law there can be enough because—to use your analogy—it draws the line in the sand and sets the standard of behaviour that is acceptable. Right now that is unclear. Sending out messages—remembering the old adage that rules are made to be broken—and making them a "no hat, no play" rule at school, whether or not that sinks in and changes behaviour across the community is a different question and that is where legislation really plays a part.

The Hon. BRONNIE TAYLOR: It is my non-legal analogy but it is coming through very clearly. We might be looking at a precaution rather than a reaction. That is a very powerful thing; it is like a preventative measure.

Mr DAVID SHOEBRIDGE: It is what the Law Reform Commission referred to as the "normative value" of laws that create new norms in society. The Law Reform Commission has a draft bill—from its 2014 report—that is basically ready to go. If we were to put that through the New South Wales legal translator and turn that into a New South Wales bill it would be a very good starting point, would it not?

Mr CHOW: I think that is absolutely right. A good starting point is a good way to put it.

Mr McKENZIE: We would say that, yes.

Ms CURRY: There is a sense of urgency to agree with that statement for sure. To be ahead of the curve is not a bad thing.

Mr DAVID SHOEBRIDGE: Everyone says we have got to be careful of having a patchwork quilt of law. At the moment we have not got any cover at all. So the first patch would be a good start, would it not?

Mr CHOW: Absolutely.

Ms CURRY: We have the mechanisms in place to make changes once laws are passed. It is a matter of getting them passed in the first instance before you can really see what the problems are. We can speculate and do nothing or we can have a go.

The Hon. LYNDA VOLTZ: One of the things about legislation is that you can always go back and refine it.

Ms CURRY: Those mechanisms are in place, yes.

The Hon. DAVID CLARKE: Mr McKenzie, following on from what Mr Shoebridge has just said—namely, there is a bill virtually waiting to go there—the Human Rights Committee of the Law Society has expressed reservations about some of those provisions or recommendations. Is that something you would like to take on notice and consider further?

Mr McKENZIE: I think I have addressed most of the reservations we expressed in relation to the question I was earlier asked about the shifting of the onus of proof. Unless you want me to, I do not think it is necessary for us to say anything more than we have actually said.

The Hon. DAVID CLARKE: You are in agreement with that?

Mr McKENZIE: At the edges we have a few differences in detail but nothing more than that. There was one other thing I was going to refer to in response to the question from Ms Voltz about revenge porn. There is currently a bill before the Federal Parliament called the Criminal Code Amendment (Private Sexual Material) Bill—I think it is an Opposition bill. The Law Council of Australia, the peak body of the legal profession

nationally, has just this month made a submission to Mr Tim Watts, MP, who is the shadow Minister concerned about that bill. I have a copy of that submission, which I can make available to the Committee—it might be useful.

The Hon. LYNDA VOLTZ: That would be good.

Document tabled.

The Hon. LYNDA VOLTZ: I should clarify that I do not like the term "revenge porn".

Mr McKENZIE: You did make that clear. That is how the Law Council refers to it in its submission.

Mr DAVID SHOEBRIDGE: I think the point that Mr Clarke was getting to—which is where my question was—is that you said you would have reservations around the edges of the Australian Law Reform Commission's bill. But if the Law Society was sitting there and you had a choice of either that bill or the current state of play, would it be a hard choice?

Mr McKENZIE: No.

Mr DAVID SHOEBRIDGE: Or would you comfortably say, "Get the bill".

Mr McKENZIE: We would be quite comfortable with the bill as it is; we would just suggest some tinkering with some of the provisions. I think the other matter that Mr Clarke may have been addressing was that we have suggested that gross negligence could be a ground for a privacy breach rather than just intentional recklessness—that is the other point we made.

Mr CHOW: May I quickly ask, are you all aware of the mandatory injunction that Chanel Ten sought against the *www.dailymail.com* last Friday?

CHAIR: No.

Mr CHOW: I would direct your attention to that because this was precisely on the breach of confidence issue. It was an urgent injunction that was brought by Chanel Ten.

Mr DAVID SHOEBRIDGE: This is the reality television show?

Mr CHOW: The reality television show.

Mr DAVID SHOEBRIDGE: To say they were exclusive.

Mr CHOW: Exactly right.

The Hon. BRONNIE TAYLOR: *The Bachelorette*?

Mr CHOW: *The Bachelorette* photos. It is incredibly relevant because it is essentially unprecedented as far as I am aware in terms of the nature of the injunction that was granted. I think it would be worthwhile considering even the notion that it was granted in the first place based on breach of confidence. The arguments were very loosely based on that unquoted precedent from English law.

CHAIR: Thank you for appearing before the Committee this afternoon. You have 21 days in which to respond to any questions taken on notice and to any additional questions that the secretariat may forward to you on behalf of Committee members.

(The witnesses withdrew)

ALEXANDRA DAVIS, Solicitor, Women's Legal Services NSW, affirmed and examined:

LIZ SNELL, Law Reform and Policy Coordinator, Women's Legal Services NSW, sworn and examined:

CHAIR: Thank you very much for coming this afternoon. Would you like to make an opening statement?

Ms SNELL: Thank you. We thank the Committee for the opportunity to appear today. Women's Legal Services NSW is a community legal centre that aims to achieve access to justice and a just legal system for women. Amongst our specialist areas we provide legal services relating to domestic and family violence and sexual assault.

Over the past few years we have seen a significant increase in technology-facilitated stalking and abuse—that is, the use of technology such as the internet, social media, mobile phones, computers and surveillance devices to stalk and perpetrate abuse on a person. In particular, we are seeing a concerning trend of technology being regularly used against women by perpetrators as a tactic within the wider context of domestic violence. We support a New South Wales and Federal statutory cause of action for serious invasions of privacy that includes damages for emotional harm other than a psychiatric illness. It is important that this be as accessible as possible and that there also be other accessible options.

Ms DAVIS: The problem is manifold. There are three main hurdles that women in these situations face. The first is criminal laws. While some existing offences are broad enough to capture technology-facilitated stalking and abuse, we are not seeing them used. There are also gaps and deficiencies where the law has not yet caught up—for example, in relation to non-consensual sharing of intimate images.

The second challenge is police attitudes and evidence-gathering capabilities. There is an urgent need for training to overcome the common attitude that technology-facilitated harassment is somehow less serious and less harmful than behaviours in person and that proving that the offender is responsible is somehow more burdensome when technology is involved. The third challenge is access to remedies and support. There is a need for a quick, accessible way of obtaining a take-down order. There is also a need for specialist services that are trained to assist women to access comprehensive planning for the safe use of technology and to remove spyware from devices.

While there is already scope for apprehended domestic violence orders to be used by women experiencing technology-facilitated stalking and abuse, the laws are being applied inconsistently in these circumstances. We believe that the Crimes (Domestic and Personal Violence) Act 2007 should be clarified to better capture these behaviours and that amendments should be made to allow for take take-down and delivery-up orders. We note that this legislation has been under statutory review since 2011. We urge updated consultation and an exposure draft bill that contemplates the realities of technology-facilitated stalking and abuse.

We see technology as a double-edged sword. Although it is used to harass and intimidate women, we should not underestimate its ability to protect, support and connect women who are experiencing or have escaped domestic violence. It is not appropriate for victims to be told to stop using social media or to change their number or block the other party's phone. We need actions and remedies that will hold the perpetrator to account. Technology can also be used to assist in evidence gathering. With this in mind, we recommend that consideration be given to establishing an encrypted electronic device in all New South Wales police stations that could be used to quickly and cheaply scan a person's device for spyware or malware and allow police to access social media without firewalls and to extract relevant data in an admissible form. We believe that a joint strategy in civil and criminal law is necessary to combat this new frontier of violence against women.

CHAIR: Thank you. We will commence questions.

The Hon. LYNDA VOLTZ: I know this is a complex area. I have looked at the scenarios in your submission. This problem has been around for a long time. Obviously a national approach to it would be good, but that has not happened. If New South Wales introduced legislation to address the issue, would you see that as a stepping stone to a national approach? It is not going to solve the problem in the first scenario in your submission, though, is it? That was the story of Susan, whose partner created a fake Facebook account in her name.

Ms SNELL: I think there are a range of remedies that we would be seeking. For example, Alex has talked about the Crimes (Domestic and Personal Violence) Act. That would be one. Obviously that is a State-based piece of legislation and we would want there to be a few amendments in there, particularly around the positive power so that there can be take-down orders and deliver-up orders. That could happen now as one option. In terms of statutory cause of action, we would support both the New South Wales one and a Federal one precisely for the reasons that you are talking about in so far as we could be waiting for a considerable time for a Federal one so it is important to act now and have a New South Wales one. So yes, I think we would agree in terms of that.

The Hon. LYNDA VOLTZ: Because at some point someone has to start something.

Ms SNELL: Just on that point: it would be useful if there could be conversations across the jurisdictions in the hope that there could be uniform legislation, but that is a bigger question.

The Hon. LYNDA VOLTZ: That is another issue we have raised with some other people who have made submissions. There is a mechanism known as ministerial councils where the Ministers all meet every year or every second year and look at the legislation. So it is a matter of once you have got the legislation, getting it on to the agenda for a ministerial council.

Mr DAVID SHOEBRIDGE: Can you tell the committee about your rationale for including remedies in apprehended domestic violence orders and domestic violence proceedings? What is the rationale for having that remedy available in that manner?

Ms SNELL: For us it is important about it being an accessible remedy. We believe, given the majority of women that we are working with are women who are experiencing domestic and family violence and often AVOs might be a relevant part of their proceedings, AVOs are also, as we have talked about, in a Local Court, which is a more accessible avenue than perhaps a statutory cause of action would be, and we would see it as being a part of those proceedings; so it is an already existing proceeding and making that amendment in the legislation would give the court the power to make take-down orders and deliver-up orders. But the fact that it is a more accessible remedy is one of the reasons why we would argue for that to be. I think part of that would be in terms of education. On the one hand it is useful to have it in one space so that it is easy to access; on the other hand, it is also useful to have multiple different kinds of remedies. But I think primarily it is about that it be accessible.

Mr DAVID SHOEBRIDGE: And women are already involved in these proceedings. These are common issues that arise in these proceedings. In terms of a socially efficient way of responding to it this is perhaps one of the most socially efficient ways of responding to it. Is that right?

Ms SNELL: That is right.

Ms DAVIS: It is quick and would be cheap and we now have a lot more provisional orders being made by police on the spot where they suspect that a domestic violence offence may occur or has. They could also put in applications at that stage, or at any stage, for a take-down order.

Mr DAVID SHOEBRIDGE: In terms of the women who are coming to you for assistance, what proportion of them are facing these kinds of issues? What proportion of them would be benefited by having these kinds of remedies available?

Ms DAVIS: A huge amount. For example, this week I did a law clinic and had eight clients; five of those clients presented with issues of technology-facilitated stalking and abuse. That is just one day of a given week. So it is a huge issue and it is tangled up with other legal issues that are happening. It is often not just the one thing in isolation; there are often other things going on in the background as well. But it is a huge issue and there is no clear solution at the moment.

Mr DAVID SHOEBRIDGE: A number of people have suggested that we should consider an additional criminal offence. Your submission refers to section 578C of the Crimes Act and I think the one instance that you refer to it as being used is in *Police v Usmanov*, but that offence requires proof of the publishing of indecent articles. Can you explain to the committee what your concerns are about having a criminal remedy dependent upon a phrase "indecent articles"?

Ms DAVIS: Indecency in itself kind of refers to a victim-blaming state of mind. To say that the actual publication of the material is indecent, the language and semantics around that is almost importing that what the victim did was the indecent act, and it is detracting from the fact that this is actually something that has been done to her and she has been wronged. On top of that, most indecency offences traditionally are about being against the community standards. So what is that message that we are sending if this is something that is coming under an indecency offence? In other jurisdictions indecency is more narrow and it captures things such as where there is also violence or excrement or things that are against community standards more obviously than simply a woman taking a photo of herself which has been shared non-consensually. That is the real harm that has been done here, not her having an indecent photo in the first place.

Mr DAVID SHOEBRIDGE: One potential remedy for that would be to have a criminal offence that focuses upon the really offensive behaviour, which is not the original image or being in a position where your image is taken, but the criminality should relate to the sharing of it and the harmful sharing. Is that what you are saying?

Ms DAVIS: Yes.

Ms SNELL: The non-consensual sharing, yes.

CHAIR: In your submission you talk a little bit about the collection of evidence and you said that in your experience an individual police officer lacks the understanding of the technology involved or the rules of evidence and can be embarrassed in investigating the matter. Do you think that is a lack of understanding or is it a resource issue or is it both, and do you have suggestions on how that could be addressed?

Ms DAVIS: It is definitely both. So, speaking to individual police officers, there is a real inconsistency when you have matters in what they will tell you they are capable of and what they are not. But when it comes to matters going through court being investigated, charges being laid and the prosecution needing to build a case, there are a lot of issues of the admissibility and the form of the evidence. For example, if you have Facebook offences and women doing screen shots of that, if the person charged has a good defence lawyer they will bring up all sorts of challenges to that evidence and it will not be admissible. Those circumstances also depend upon access to justice and whether that person has representation because in some of those matters they do not. In terms of the actual evidence, perhaps Ms Snell may have something to add.

Ms SNELL: Could you repeat the question?

CHAIR: It is in relation to whether or not the police lack the understanding of what the technology is or what the laws are around it or is it that they just do not have the time and resources and therefore it is not being pursued properly?

Ms SNELL: As Ms Davis was saying, it is both. We think there needs to be continuous training with police about the nature and dynamics of violence. Ms Davis has already referred, in her opening statement, to how it seems as though technology-facilitated violence is treated as a lesser form of violence and we would challenge that. Also we think police would benefit by having training about the law itself and Ms Davis can speak to that possibly in a minute. The other area is in technology and we totally agree with you in terms of resourcing. There is the training issue and it is our experience that police do not seem to understand the technology and the gathering of evidence. But also, in terms of resourcing, another limitation is that we have been told it is expensive to gather such evidence. That is why one of the proposals we have put forward is about having a mechanism at the police station where a woman can go in with her device, meet a police officer and, through that, be able to gather an admissible form of evidence.

Ms DAVIS: The idea is that it would be prompted, so that there is less chance that the evidence is not in an admissible form and that it is something that could be useful to lay charges so that the matter does not simply disappear. As Ms Snell said, there are issues around the costs of evidence. One of our suggestions also was that there be a review by the Australian Communications and Media Authority [ACMA] into those costs that are under the Telecommunications Act, sections 313 and 314. While a carriage service provider is not to profit—and also not to incur any costs—police stations have reported to us that different providers charge different amounts. It also depends on the evidence one needs to get. If one had, for example, a device that was able to scan the evidence off the device and to also narrow down the scope of what needed to be found, police could save money. For example, if they needed to get something to do with telecommunications such as historic

sheets of a certain month or where the calls were from they could make it a little more targeted. They would not have the need to go on a fishing expedition which can cost a lot of money.

CHAIR: What is the device you are referring to? Is it something that is already out there?

Ms DAVIS: We have sort of made it up as something that could be developed. But when you see the technology that already exists, and the things that we are capable of, it does not seem like such a stretch to have something like that developed. Our suggestion is that something along those lines should be looked into or considered as a possible avenue.

Mr DAVID SHOEBRIDGE: Are you talking about capturing, say, text messages or the phone history but you are also talking about capturing somebody's Facebook page as well? Something more sophisticated than just a screen shot?

Ms DAVIS: To an extent. When it comes to Facebook, some police stations have told us that they cannot access Facebook within a police station because of firewalls that are in the police station. If that is an issue, this could be used to access that.

Mr DAVID SHOEBRIDGE: They should get on to the Shoalhaven Local Area Command Facebook page, as one example.

Ms DAVIS: Facebook has told us that there are informal mechanisms that police officers have access to but most lay officers that we talk to have no idea what we are talking about. Those mechanisms can be used to access subscriber information and basic information with Internet Protocol [IP] addresses and the names and emails that were used to set up that account. That could be helpful, for example, for apprehended violence orders, for the balance of probabilities, rather than actual beyond reasonable doubt, if it was a criminal charge.

With this issue of firewalls, if you had this mechanism and it was something that the police could access, a person could log into their account and the police officer could look at it themselves. Not only could you possibly get some form of evidence through technology that is beyond our engineering capacities, but also you would have the witness statement of that officer, looking at the content of that and being able to give oral evidence in court that could be cross-examined on.

The Hon. LYNDA VOLTZ: I am not sure that, in terms of technology, it quite works that way. Metadata would capture the IP address and would show you the page you looked at, what date you looked at it on and the account name but you will not necessarily capture the image itself. I would have thought that, if you had the screen shot, metadata would give police the ability to issue a warrant on the provider under the powers that have been introduced and they would be provided with information as to which account accessed that page on which day anyway.

Ms DAVIS: With Facebook we have been told that when they need the admissible evidence it needs to go to the State headquarters first. They need to get a subpoena, I suppose, for the actual company of Facebook in the United States. It is a long process that takes a lot of time, costs a lot of money and is not very accessible. Even when we are talking about phone records, I had one officer explain to me that they get 20 of these complaints a day and might take on five matters to investigate per month because they simply do not have the resources or the money to be looking up metadata or to find the evidence that is going to be admissible when it goes through to charges.

Mr DAVID SHOEBRIDGE: We are told that metadata does not capture the content of web pages but just the address and who was accessing it at particular times, particularly if someone is putting the offensive, intimidatory or harassing material on Facebook. What you are suggesting is that, for the test of balance of probabilities, having a police officer sight it, take screen shots of it, annex it to a statement and say, "I saw this on a particular day" might be a relatively low-cost way of getting to the balance of probabilities?

Ms DAVIS: Yes.

The Hon. LYNDA VOLTZ: Would they not just seize their computer and phone and that would provide them with information. At the end of the day, unless you take it back to the factory settings and wipe everything, it is all there.

Ms DAVIS: There are some issues about passwords and access but also we have had clients where the police refused to do that because of the costs and because running computer forensics is done by certain crime units. Those sorts of matters are usually reserved for indictable offences and things that are considered more serious than, for example, a breach of an Apprehended Violence Order [AVO] or a stalking or intimidation offence.

The Hon. LYNDA VOLTZ: I understand that it is about the seriousness and where the police are putting their priorities but that is about a police resourcing priority issue as opposed to the ability to grab the information which would be needed.

Mr DAVID SHOEBRIDGE: To address the bread and butter continual complaints that police stations are getting and not being able to deal with because of the cost of it being a Rolls Royce forensic approach, you are suggesting that they should be exploring ways of more cost effectively getting the evidence to assist in Apprehended Violence Order proceedings?

Ms DAVIS: Yes.

Mr DAVID SHOEBRIDGE: Have you had any willingness from the police when you have approached them with these ideas? What has the exchange been?

Ms SNELL: I do not think we have had the opportunity to do that yet.

Mr DAVID SHOEBRIDGE: Perhaps a recommendation from this Committee urging them to look at that would be the way forward?

Ms SNELL: Yes, that would be helpful.

The Hon. LYNDA VOLTZ: And if some of these offences became covered by criminal codes within themselves, that would certainly focus their attention perhaps more than issues that may not. For example, if there was an offence for transmitting naked photos of people and it became a criminal offence, it might make it easier.

Ms DAVIS: You would think so but we already have, for example, the Commonwealth Criminal Code which has the offence of using a carriage service to harass, intimidate or menace which is a criminal offence. Arguably some of these things would fall under that but we are not seeing those things being used. We are not seeing computers being seized for those sorts of analytics to be run on the computers.

Mr DAVID SHOEBRIDGE: The Committee heard interesting evidence from Dr Henry and Dr Powell from the La Trobe and RMIT universities earlier. They did a national survey of some 3,000 respondents and found that of people aged between 18 and 55 approximately 10 per cent of respondents—and it was statistically valid for the Australian population—had been the subject of harassment or sexting, or that sort of digital offence. But that the experience of men and women in regard to how they responded to it was starkly different. Women seemed to suffer more damage and anxiety from the same behaviour than men. Could that differential experience be part of the reason why our predominantly male police force is not responding in the same way that you would expect, or in the way that you would hope to protect and vindicate the rights of your women clients? When you show them an issue, you show them an image, you tell them about your client's experience and they might interpret that predominantly through male eyes and do not see the same level of offence or experience the same anxiety as your clients do.

Ms SNELL: I think it would be fair to say that we certainly face some challenging attitudes from police at times. As we said before, this type of technology facilitated abuse seems to be treated as a lesser form of violence so that is certainly part of the challenge in how to respond to the issue.

Ms DAVIS: I think as well that a lot of the harm is compounded by outdated expectations of women and other sorts of attitudes towards women, which makes the victimisation experience different to how it may affect men.

Mr DAVID SHOEBRIDGE: This would only be anecdotal evidence, but do you notice a difference between how male and female police officers respond to your clients when these concerns are raised?

Ms DAVIS: To be honest, I have had varied responses no matter whether it is a male or female officer. I still have female officers saying inappropriate things to my clients; they just tell them to get off Facebook or to ignore it. I think it is an attitude of minimisation across genders but probably more harnessed by males who might see this as a lesser issue and through the consumption of women anyway it seems more normalised.

Mr DAVID SHOEBRIDGE: Do you urge an education program targeted at police so that they become aware of the genuine distress that these things cause to women?

Ms SNELL: Definitely. When we talk about a better understanding of the nature and dynamics of domestic violence, that would certainly be a part of it.

CHAIR: Do you have evidence, or has anyone sought your advice, in relation to the misuse of surveillance devices or drones and an invasion of privacy? It is just another aspect of our inquiry.

Ms DAVIS: Surveillance devices is a really common issue; drones not so much. But we have a lot of clients where, for example, surveillance devices have been set up in their home without them knowing. We have clients who are separated under one roof, where they are still living with a perpetrator but in separate locked away bedrooms, and they find surveillance devices in their private rooms. But when they have called police the police have not taken action. For example, under the Surveillance Devices Act if it is an optical surveillance device then it is to do with the trespass, or going into property without consent. Even though you could argue that that space is occupied by a person, it is not with consent because of that occupation with the police not seeing eye to eye with us in some of those circumstances, and then you have women with no redress.

Also with surveillance devices you have a lot of spyware and GPS tracking and often the things that are most insidious are the things that we commonly use, Find my Phone in your iPhone or things that are linked up through Cloud computing and children being given devices that already have things on them. And while all of that should be covered by the Surveillance Devices Act as tracking devices as well as data monitoring devices we are just not really seeing any action being taken. One of the challenges as well is that a lot of women will suspect something is on there but how do they prove it? Many of these things can be remotely removed from the phone and are not detectable. We do not have services or things such as a device at a police station to plug it in to scan and to see whether it is there. Whilst individual companies and private entities might offer that sort of forensic scanning it comes at a cost and it is not easily accessible by our clients.

Mr DAVID SHOEBRIDGE: You have given scenarios where women are the subject of intrusive and obviously intentionally intrusive surveillance. Are there any instances where women have put surveillance devices in to protect themselves? Do we need to be careful of that in any statutory remedy?

Ms DAVIS: Yes, we need to be very careful of that because we have a lot of clients who will use technology to protect themselves—whether that is downloading an app on their phone so that they record conversations because they might have an apprehended violence order against a perpetrator who has a "no contact" order. If he repeatedly calls a woman, she wants the evidence and the intimidating things that he is saying so she records those conversations. There are exceptions in the Surveillance Devices Act for listening devices for when you are protecting your lawful interest, but we still need to be really careful about it. There are other instances when women might want, for example, those sorts of cameras and things in their houses because they are terrified that the perpetrator is going to try to break in. So we need to be really mindful that these technologies, while they are also being used to perpetrate violence, can be the things that assists our clients.

Mr DAVID SHOEBRIDGE: In your experience have there been any instances where your clients have found themselves facing an actual or potential prosecution because they have taken those kinds of steps to protect themselves—either recorded a conversation or installed a surveillance device? Have they ever been the subject of any threats?

Ms DAVIS: Not so much. It has been relevant before with how evidence has been collected for cases.

Mr DAVID SHOEBRIDGE: Whether it is admissible?

Ms DAVIS: Yes and whether section 138 of the Evidence Act would apply; whether that has been illegally or improperly obtained; and whether that value outweighs the way that it was obtained. We have not had any clients who have had charges against them for those sorts of things but we still need to be mindful of it, especially for a lot of our clients who, on changeover of a child, they might feel very unsafe and want to be able

to record what is going on as a protective mechanism for themselves. There are challenges sometimes by perpetrators that what you are doing is not legal but we have not had clients prosecuted that I am aware of.

Mr DAVID SHOEBRIDGE: In those circumstances when you have a changeover happening, the woman is very concerned about her personal safety, there may be no outstanding orders and she decides that to protect herself she will record what is going on. If she is recording the sounds and her former partner objects to it, is she in legal peril in those circumstances?

Ms DAVIS: It depends where it is. A lot of changeovers are happening in McDonalds and in public spaces and for listening devices it needs to be in private conversations. So in those circumstances she should be fine anyway. It is only an offence if it is a private conversation in that circumstance. There are certain things and precautions have to be taken also to keep women from stepping over any legal boundary.

CHAIR: You mentioned that there are instances when there have been no remedies for a woman once she has been turned away by police. What advice do you give these women? Can they continue or should they walk away frustrated with the system?

Ms DAVIS: It is difficult. We try to explore whatever avenues we can. It depends on the type of technology that facilitated the stalking and abuse. Sometimes we will be able to do advocacy for a private AVO application and certain additional orders that might make her feel safe—so drafting one for her particular circumstances. It is difficult with some forms of redress—for example, if you are trying to seek victim support—because you need to have something either that was intimidating or stalking or a personal violence offence. Intimidating falls within a personal violence offence for that person. We will explore those avenues and non-legal avenues. For example, if it was an image being shared non-consensually, there are different ways to try to get that taken down including by contacting webmasters having found that image online. We have certain technology safety planning things that we go through with our clients by virtue of going through legal advice and the different steps they can take. They often end up feeling lost and as if their problem is not legitimised by the law because they might not have redress or the perpetrator may not be held accountable.

CHAIR: I read about an overseas case of a girl whose friend took a photograph of her in the shower and a number of years later it went online. What advice could you give that client, although she is not Australian?

Ms DAVIS: Once it goes online you need to find where it is. If you cannot find where it is you cannot prove that it is out there or start different steps you need to take to try to get it taken down. There are certain ways of doing this—for example, a WHOIS search to find out who the webmaster is of a website. The advice we give will depend on whether it is in an Australian or overseas jurisdiction. If she had taken the image herself there is possible scope to use copyright law but that solution is ill-fitted to that sort of problem. Once the image is found she would then need to contact the police to get them to assist in any way they can. Under the current laws in New South Wales it would depend on whether the image was taken consensually or not—that will make a huge difference, which should not be the case because it should be about whether it was shared with consent. Voyeurism provisions and surveillance device provisions might be relevant if it was recorded without consent, but if it was taken as a joke or for a partner and it was passed on then it depends. She might be able to go down the route of publishing an indecent article. It also depends on whether the police take action and her civil remedies will be quite limited at this stage, which is why a statutory tort would be welcome.

Mr DAVID SHOEBRIDGE: Whilst you say it would be good to have a remedy in the apprehended domestic violence setting you also think that a statutory remedy is an important element. Do you adopt the Australian Law Reform Commission's proposal as a good starting point?

Ms SNELL: It is a good starting point but we also raised some concerns about a variety of aspects of that including in their principles, for example. We wanted to especially articulate around balancing of principles that the right to equality and freedom of violence be a part of that. In their last principle, which talks about shared responsibility, we have some concerns about how that may play out in a domestic and family violence context where you should be holding a perpetrator to account. If the focus is on telling someone to change a password, there may be complications if the male has control of finances and the computer so that would not be a simple thing to do. We accept the principle but with those concerns. We do support other elements, such as the seriousness of it. We certainly support remedies in terms of apology, injunctive relief, take-down orders, compensation et cetera. We particularly support the idea of having damages for emotional distress beyond psychiatric illness because we are aware that emotional distress presents in a variety of forms. In short, it would

be a good starting point and an exposure draft would be useful for further comment once it goes through the system.

Mr DAVID SHOEBRIDGE: In terms of damages, a number of people have suggested that you should be looking at a scale similar to the Defamation Act, which attaches to the maximum damages under the Civil Liability Act for a personal injury. Is that the kind of regime you are looking at or do you think if we had a statutory course of action a more modest form of monetary damages might be appropriate?

Ms SNELL: In damages we would want to see a range including punitive and exemplary damages. We will take your question on notice.

Mr DAVID SHOEBRIDGE: I would be more than happy for you to do so. In your submission you talk about concerns about limitations, as you see it, in the definitions under the Crimes (Domestic and Personal Violence) Act that prevent that Act from responding to the full range of stalking and limitation of your clients. Can you talk us through those definitional imitations?

Ms DAVIS: Under section 16 of the Crimes (Domestic and Personal Violence) Act for the court to make an AVO they need to show that the protected person has fears and reasonable grounds for those fears of a personal violence offence or stalking or intimidation by the defendant. Then you have to home in on the definitions of intimidation and stalking. The definition of stalking is quite limited and specific to physical forms of stalking. That will not capture things like GPS tracking and using technology, so it is a bit outdated. Then you have to rely upon the definition of intimidation. There are three different parts to section 7. There is harassment or molestation and we think harassment should be wide enough to capture many of these things but it is not necessarily being interpreted that way. It is open to discretion and different readings so one of our suggestions is having a non-exhaustive list of things around harassment to make it clearer and the addition of unauthorised surveillance. That would capture things such as checking emails and messages and GPS tracking. Our recommendation is based on the equivalent Act in Queensland and its definition of unauthorised surveillance.

CHAIR: Unfortunately we have run out of time. You are asked to respond to any questions you have taken on notice within 21 days and any additional questions members have will be sent to you by the secretariat with the same 21 days in which to respond. Thank you very much for appearing before us today.

(The witnesses withdrew)

BRUCE BAER ARNOLD, Director, Australian Privacy Foundation, and

DAVID VAILE, Vice-Chair, Australian Privacy Foundation, affirmed and examined:

CHAIR: Would you like to make an opening statement?

Assistant Professor ARNOLD: The Committee will have encountered claims that there is no need for law reform because the media can be trusted to self-regulate or, more importantly, that people do not care about their privacy. A decade ago Australia read the claim that privacy is a middle class invention by people with nothing to worry about, the sort of people who "believe in unicorns and the tooth fairy". The writer said that normally those people would have every right to live in their moral fog but not when their confusion permeates the feeble minds of lawmakers and puts the innocent at risk. The Australian Privacy Foundation does not believe that members of this Committee or indeed the Supreme Court are feeble minded. You, like your relatives, your friends, your associates and electors, do care about privacy. Most importantly, you can do something about invasions of privacy. We invite you to do so.

The New South Wales Parliament does have the power to effectively address serious invasions of privacy that occur within the State irrespective of whether those invasions occur in cyberspace using technology such as smartphones or involve traditional offences such as peeping Toms. We advocate practical and widely applicable remedies for serious invasions of privacy so that the people of New South Wales do not have to involve the police in most cases. You should not pass the buck to Malcolm Turnbull and expect the Commonwealth to solve the problems of New South Wales. The *News of the World* outrages by the United Kingdom arm of Australia's largest media group demonstrated that media self-regulation is sometimes ineffective. As a personal comment, I note in passing that Mr Murdoch has not resiled from those abuses.

The Foundation calls on the Committee to recommend law reform that specifically deals with serious invasions of privacy. That reform has been proposed in detail by the NSW Law Reform Commission. It has been proposed by the Australian Law Reform Commission. It has been proposed by law reform commissions and parliamentary committees in Victoria and other jurisdictions. Put simply: it is not new, it is not frightening; it is quite achievable. The foundation, for example, has noted the Victorian Parliament changed its law to protect minors and adults from so-called revenge porn. That is just one example of a serious invasion of privacy. Proposals for dealing with serious invasions of privacy have been under consideration for a decade. They provide for necessary precautions to avoid trivial matters and to protect other interests such as the public interest in political communication.

The Foundation also alerts the Committee that meaningful law often requires timely and positive action by watch dogs. That means State agencies must be properly resourced and positive. There is a fundamental difference between an effective watch dog and a snoozing poodle. The State Parliament cannot solve all privacy problems. The Foundation accordingly calls on the Committee to urge the New South Wales Government to work with the Commonwealth and other States to develop a seamless, effective national privacy regime that extends from data breach and dating sites to drones and misuse of global genetic databases. Foundation Vice-Chair David Vaile and I are happy to answer questions about our submission.

Mr DAVID SHOEBRIDGE: The starting point for many submissions, and it is really the starting point for yours, is the Australian Law Reform Commission's recommendation and its draft bill. If this Committee did nothing other than recommend that that bill with appropriate changes to modify the statutory regime in New South Wales became law would that be a significant step forward?

Mr VAILE: I had the pleasure and the honour to be on the advisory panel for the Law Reform Commission's work there. I heard quite a lot of the discussions in particular with various interested parties, including a lot of the media lawyers and others with that. Certainly what came out of that was it did not please everybody, it was not perfect. But, as with the previous exercise in 2008, we had three or four years going towards a very similar end. It has come out to a conclusion that I think will actually balance most of the interests and will certainly be a great step forward from the absence of any individual personal enforceable remedy that we have now. The short answer is yes.

The Hon. DAVID CLARKE: Do you have any reservations at all?

Mr VAILE: If the choice was is that a great step forward or a useful step forward with all its foibles—

Mr DAVID SHOEBRIDGE: If the options were to leave the law as it is or legislate for the draft bill in New South Wales is it a difficult choice?

Mr VAILE: Not really.

Assistant Professor ARNOLD: No.

Mr VAILE: As for your question, there is nothing that would sort of complicate that question.

The Hon. DAVID CLARKE: Did you see the Law Society's submission?

Mr VAILE: Unfortunately, I have not had a look in detail.

The Hon. DAVID CLARKE: I just wondered whether you had looked at their submission. I think they had one or two reservations.

Mr VAILE: I know they are very careful and very detailed in their considerations.

The Hon. DAVID CLARKE: But as far as the foundation is concerned you have no reservations that come to mind?

Assistant Professor ARNOLD: The overall package should move forward. I think what is significant and the reason that I probably bored the Committee by citing the number of reports that have been done over at least the last decade is that there is a strong feeling certainly within the overall legal community within Australia and certainly among consumer advocacy organisations that we should move forward. We are not getting strikingly different reports from these various bodies. So, yes, as with any law reform, inevitably there is some disagreement on minor points but the overall thrust, the overall message is to do it and do it now.

Mr DAVID SHOEBRIDGE: That is almost the exact sentiment that the Young Lawyers expressed. They said to just do it. The basic structure has been set out time and time again. When you keep sending it off to expert bodies that have the skills and they keep coming up with the same answer surely legislators should respond.

Mr VAILE: It felt like groundhog day in the 2014 inquiry because in fact we could have cut and paste a lot of our observations and discussion from our 2007 and 2008 submissions and they could have cut and paste a lot of the results of that. One thing I might observe is that often privacy is posed as an individual interest that is against other sorts of group interests, commercial interests or government interests. I have been on a number of very interesting roundtables and symposia where you actually get quite a lot of support from not particularly policy-oriented people from business or IT security or the banking sector. They are expressing not exactly a delight to be exposed to the threat of overarching new things to worry about but they actually quite like the idea that those shonky businesses or the ones taking the shortcuts or who are cheating or who are doing the wrong thing will face some exposure to either the individual being able to seek redress or an active regulator. It is quite surprising that they see that as putting a floor under the market and encouraging competition on price and products.

Mr DAVID SHOEBRIDGE: Competition on fair terms.

Mr VAILE: Fair terms and that sort of thing, not on "can we work out how to sell your stuff to somebody or can we use some other shonky practices."

Assistant Professor ARNOLD: Globally we are seeing a market for trust. There is some recognition that it is in the interest of large businesses and small businesses to move to best practice, to be seen to be doing the right thing by your customers and by your partners.

Mr DAVID SHOEBRIDGE: The Australian Law Reform Commission's fault model is based upon recklessness or intentional actions. What that does not pick up is the negligent actions of companies such as Ashley Madison. They are large corporates, they have a capacity to put in place protective measures for information and they failed to do so. Even if we did not extend the scope of liability through negligence at large

but we simply said if you are a large corporate or a business entity and you are gathering this information for business purposes you will be exposed to liability through a negligence path. Do you see some merit in that?

Mr VAILE: In my view if there was something to improve or tweak that would be one of the first places to start. It is a problem if you do nothing and say, "Oh, dear, how did that happen? We lost all your information. We did not mean to lose it. We were not trying to sell it. We were not being deliberate about that, we just did not care enough. We did not get the proper technical advice or talk to the insurers." I have recently had assistance from the global data risk insurer from AON, the largest insurer, trying to understand what they would be saying to businesses in terms of the responsibility to look after this.

When there is no possibility that no matter how gross the negligence is you won't be called up on it, it encourages not caring that much. I think it should be a high threshold. It is, you should not be a trivial test. Gross negligence from large corporations that have the benefit of technical, legal and actuarial advice, there should be an involvement that they did not take enough care. The result has occurred, people have been hurt or the information is out. Like in many other areas there is probably a high level of negligence.

The Hon. DAVID CLARKE: What can happen is easily foreseeable?

Assistant Professor ARNOLD: Yes. What we are seeing with the online data breaches is that it is highly predictable that breaches will occur.

The Hon. DAVID CLARKE: There is a responsibility there to ensure as much as possible that there are no the breaches?

Mr VAILE: I will go further than that. I have been talking lot to IT security researchers, to people working in government related security and malware about their understanding and responses to malware. In doing that they have been tracking the terms of the battle and the tide is turning. The capacity for 100 per cent or guaranteed perimeter security, basically keeping the people you do not want in out, the chances of doing that have been declining over the last couple of years. We see that on the global stage where you would be hard pressed to find any single entity, whether business or government, who could put their hand on their heart and say, "Don't worry, it's safe. We have done the right thing and no-one can get in."

The realistic result of where we are at the moment—because the intruders only need to be 0.1 per cent successful to find the hairline crack in your defences whereas the defenders have to be 99.9999 per cent good enough—the result is likely to be that breaches are almost inevitable at some stage. That is not in every case and not perhaps in the next five minutes or five years in a particular circumstance. But rather than saying “We never thought it could happen, We are not going to take any precautions or crank up the security so it is world's best practice, “the proper realistic approach would be to say: no protection at the moment can guarantee that so as well as investing more in the defensive side of it we should look at ways to mitigate the harm when it happens such as, maybe we don't join things together, maybe we don't keep the credit card, maybe we encode or encrypt or fragment, maybe we do not ask some questions. There are a whole range of things we can do.

The Hon. DAVID CLARKE: To do as best as you can in the circumstances.

Mr VAILE: Yes.

Mr DAVID SHOEBRIDGE: But if you cannot protect it do not collect it should be a starting principle.

Mr VAILE: That should be a principle that is high in the consideration. There may be reasons why you might do that but it certainly should not be something someone has never heard of.

Assistant Professor ARNOLD: If it is reasonable for you to recognise that your protection is almost certainly going to be breached you should flag that quite clearly. Some consumers may well say, "I can cope with that." Others might say, "Oh, no, I am not going there".

Mr DAVID SHOEBRIDGE: This kind of liability through negligence you would not suggest you extend that to the local P and C. We are talking more about corporate entities that have the capacity to take meaningful steps and have an obligation to take meaningful steps because of their size and scope?

Mr VAILE: I think so.

Assistant Professor ARNOLD: Yes.

Mr VAILE: The standard of negligence needs to be reasonably high, because just not quite doing the right thing should not be enough to cause you trouble.

Mr DAVID SHOEBRIDGE: The Law Society proposed gross negligence.

Mr VAILE: Gross negligence or one step below gross negligence. That is a reasonable line. It means you can still have bad things happen. It takes into consideration If you try to do the right thing, if you have taken some precautions and it turned out not to be enough, or it is a new hack that no one has discovered until yesterday—we hear all about these zero-day things, which unfortunately everybody who finds nowadays tends to hang on to rather than reveal—that is not a problem. But if you should have known about it, if you are on a massive scale, if the breach is exactly the same kind that hit all of the security personnel in the United States or Ashley Madison—

The Hon. DAVID CLARKE: There would be a general understanding in the industry that there are some things that can be stopped and others that cannot. We are not talking about those things that cannot be part of the gross negligence. There is an understanding of what can be done and what cannot be done, isn't there?

Mr VAILE: It is a moveable feast. It is a constant struggle and exactly what is possible and what is not possible moves from time to time.

Mr DAVID SHOEBRIDGE: It is Darwinian almost, isn't it?

Mr VAILE: And that is the sort of thing, if this was to come about, you would ask: when did it happen and what was known? There is massive investment in IT security protection but also in dealing with data in ways that make it less dangerous when it is hacked. These are not weirdo matters for a few mad professors, there are massive industries looking at that. You can get the advice.

The Hon. DAVID CLARKE: It is ascertainable what is negligence and what is in the moving feast area?

CHAIR: At point 15 in your submission you refer to surveillance devices and surveillance cameras. It ranges from the accidental neighbour that films the neighbour in the pool to the surveillance device, as mentioned by a previous witness, with regard to domestic violence where devices monitor ex-partners. In your submission you said there are issues in relation to apparent reluctance to inform the public about the law in relation to surveillance devices. Could you elaborate on the term "apparent reluctance"? What are those challenges and how can they be overcome? It is the first paragraph, point 15, final sentence.

> **Mr VAILE:** I think there is a lot of work that the police and law enforcement have to do and there are a lot of laws that are not enforced and a lot of laws that do not come widely to notice. One of the things that you might do, for instance, would be to run a campaign so that everyone—every child, every elderly person and every businessperson—knew that there was a range of surveillance devices laws. So things like a camera or a telephone or some of those ordinary devices can in fact be used not only to breach people's rights but also to commit offences. There is not really much of a campaign like that. I think it is partly because there is no-one with a particular responsibility to do that and everybody has other responsibilities.

Assistant Professor ARNOLD: Ultimately the foundation is urging some fairly practical measures. We are not being doctrinaire. One thing that strikes me, both as a Foundation director and as an academic, and certainly as someone who deals with people who are about 30 or more years younger than me, is that there is a real misunderstanding or lack of understanding about privacy—about what you can and cannot do—in Australia. Journalists in particular seem to be often quite confused.

So one of the main thrusts of our submission is that, yes, if you have the relevant number of votes in the chamber then you can pass laws but we need to do more than that; we need to do things like run a public education campaign. It would be quite achievable and would possibly alleviate the need for some litigation. For example, making people aware that street photography in most venues in New South Wales is not illegal. It is

not illegal, generally, to own and operate a small drone, subject to the framework for how we characterise a drone and where it is flying—for example, you cannot fly it over a defence facility. Is it legal to record a phone conversation? If you ring me up, can I record that conversation without telling you?

CHAIR: Just on that, do you think the existing surveillance laws are adequate? If not, what should be done? What improvements need to be made that you would you recommend to this Committee? I am happy for you to take that question on notice.

Mr VAILE: We are happy to take that on notice but I would start off by saying that if we had a generic and overarching capacity to respond to serious intrusion then in some circumstances that may help us—if it was a deliberate abuse or something like that.

The Hon. BRONNIE TAYLOR: Going back to before the last question, you were talking about education. I do not have a legal background but one of the things that has come through loud and clear today is the fact that if we were able to pass legislation in terms of what was recommended by the 2014 law reform report, that would almost provide a deterrent.

Mr VAILE: Yes.

Assistant Professor ARNOLD: Yes.

The Hon. BRONNIE TAYLOR: So with that new legislation and with an education campaign it would actually give the education campaign validity.

Assistant Professor ARNOLD: Yes.

Mr VAILE: Yes, that is right; and, to give you an example, the awareness that there is no enforcement or there is no likelihood of something coming about means that people in the IT security area say it is very hard for them to go to the boss and say, "There's a requirement here. If you do not do the right thing, we will eventually get audited and there will be a problem." It makes it very difficult to say, "Give me a budget, give me a line item and give me a little program to do this; and we can have compliance checks." They are actually saying that, rather than having a vague and fluffy sort of area without much precision, it would actually help them—in the same way that we treat financial information very seriously; and there are auditing processes and controls in a lot of other areas. If you aware that there is real risk of enforcement and if it is a matter of reputational impact then it is much easier for all of those people within an organisation to justify these things.

The Hon. BRONNIE TAYLOR: From what I am hearing, and the way I am interpreting it, it sounds as though there is a powerlessness for victims here. It is sort of like when reprimanding your child for doing something wrong—you cannot give an empty threat. This is like an empty threat now and we actually need to have something to back it up with.

Mr VAILE: Yes, and I would imagine that this will probably not result in much litigation. It is just about the awareness that it is there.

The Hon. BRONNIE TAYLOR: Although lawyers love litigation.

Mr VAILE: Yes but most of this will be by ordinary people and it is very expensive to do that. But just having the possibility there that it may occur and the possibility of reputational risk is something that insurers and governance-level people have to take into account.

The Hon. BRONNIE TAYLOR: I have one more question. You just made the point about it being very expensive, and this is something that has come up today and that Mr David Shoebridge has brought up constantly. Do you think there needs to be the capacity in what we do to ensure that it does not necessarily need to go through a court system but could perhaps could go through a tribunal system—in terms of the fact that we do not want this to be open just to those who can afford to take the action; it needs to actually be able to cover those who cannot afford to do so. In terms of lawyers and barristers that would probably be a significant issue.

Assistant Professor VAILE: I have worked in the past in the community legal centre and the legal aid area and I am conscious of the massive demand and the incredible work that they do, running on the smell of an

oily rag. Having a range of options, where you start out quite cheap but which ultimately enable you to bring the full force of the Supreme Court or whatever to bear if necessary would be the best result. For instance, a tribunal style approach maybe with certain limitations would help those with more limited circumstances.

Mr DAVID SHOEBRIDGE: Some people might want to go to an empowered Privacy Commissioner for relatively summary remedy; some people might want to go to a State administrative tribunal for a slightly more robust remedy; and some people may have the money to want to go to the Supreme Court or the Federal Court for the full Rolls-Royce treatment. Whatever we produce should allow people to scale up depending on resources.

Assistant Professor ARNOLD: If you are going to do that then you have to make sure that the Privacy Commissioner, or whichever agency it is, is enthusiastic and properly resourced. At the national level there has been substantial research done now. At the national level there are substantive criticisms about the performance of what was formerly and is currently the office of the Australian information Commissioner with the privacy Commissioner, who is grossly underresourced. I think his term of office has been an extended for another two months. That sends a fundamental message to all Australians about what the Commonwealth thinks about privacy law.

Mr DAVID SHOEBRIDGE: We had a presentation earlier from the New South Wales Privacy Commissioner. There is no doubt that she is a woman of capacity and drive but of course she is a part-time officer with very limited resources. So are you saying that making sure that there is a proper, well-resourced Privacy Commissioner is part of this?

Assistant Professor ARNOLD: Yes.

Mr DAVID SHOEBRIDGE: And with an ongoing commitment to fund it into the future?

Assistant Professor ARNOLD: Yes.

Mr VAILE: Yes, very much so. The lack of capacity for the Privacy Commissioner to engage is a great impediment. They can, however, contribute even with the resources they have. I am aware of their assistance in a number of areas that were less than sending in the whole cavalry but that nevertheless have been very useful. To go back to the point about litigation and the Supreme Court, an anecdote I can share on a personal note is that of a toilet cleaner out at the University of New South Wales. He was grossly defamed by the student newspaper. It was after I had just left, having been the publisher there many years ago. The new breed of publishers thought that no-one would do that. He was a toilet cleaner. So they did not worry about it and just let it through. He sued them in the Supreme Court of New South Wales. I met one of the editors 15 years later and he said, "It is still going on. We couldn't believe that an ordinary individual was able to do this." In the circumstances that arose it was an absolutely gross threat to this gentleman's livelihood.

Mr DAVID SHOEBRIDGE: You have just proved the point—15 years later it was still going on. You have proved the point that we need to ensure in some way that that is not the only remedy. There must be something much more available, achievable and timely than just that course of action.

The Hon. DAVID CLARKE: He was the exception to the rule—to have been able, in his circumstances, to carry that on. We have to work on something more than the exception to the rule.

Mr VAILE: Absolutely.

Assistant Professor ARNOLD: I think there is another perspective. One reason that action in the Supreme Court is fundamentally important is that it sends a strong message to the rest of the world. A judgment by the Supreme Court, or for that matter by the High Court, sends a strong message to suburban solicitors across Australia. It certainly sends a message to corporate counsel in the organisations about which we are particularly concerned. It may well send a message through the mass media to the P&C committees. I take your point that we need to look after these small entities. However, if they are like the committee that deals with information regarding my favourite toddler, it has private information that includes address, phone, email and health details, and it currently has photographs of both the parents and the child. That is potentially fairly sensitive information. It is not Ashley Maddison territory and it is not my bank account details or genetic data, but there is potential for privacy abuse.

Mr DAVID SHOEBRIDGE: But the cyber security expectations you give to an entity like that are vastly different from those you would be proposing for the Commonwealth Bank.

Assistant Professor ARNOLD: Their responsibilities would be lower, but they surely get the message.

Mr DAVID SHOEBRIDGE: You want them to get the message.

Assistant Professor ARNOLD: They should be getting the message. It is possible that there will be abuse of the data, and you should look after it.

Mr VAILE: And if you cannot protect it, do not collect it. Do you really need those images? Has anyone spent five minutes thinking about the possibility that they could be abused? On the one hand you do not want to discourage people from doing things that are innocuous and perfectly okay, but it is surprising that people may not turn their minds to the possibility that information can be used for ID theft or other purposes. You are not expecting these people to carry out a major exercise, but they should have in the back of their mind that perhaps they should think about it. That would be a useful message.

Mr DAVID SHOEBRIDGE: That is the educative value that the Hon. Bronnie Taylor referred to earlier.

Assistant Professor ARNOLD: If you are a little actor, use a trusted service provider. I am sure that the Telstras, IBMs and Microsofts of the world will be happy to help. If they can make money, they will come and help you rather than Fred who has a server or a PC in his garage and that is how we manage our data—

Mr DAVID SHOEBRIDGE: There is a PC in the basement from the Secretary of State.

CHAIR: Mention has been made of the definition of "serious invasion". Do you have a view on that? I am happy for you to take that question on notice if you want to confer with other members of the foundation.

Assistant Professor VAILE: We will take that question on notice. It is important that it not be trivial and minor or of limited impact or projection of risk onto the individuals. However, the danger is that if you have too many barriers or set it too high it will apply to virtually no-one. It needs to be about a real impact and a potentially serious matter. One of the other problems is that individual circumstances vary and the significance of a breach, being exposed or a family secret coming out can be different. Some people have the hide of a rhinoceros and do not care. Other people might be experiencing a moment of personal distress or it might be a matter with a deep family history. We might think it is relatively trivial, but it could be important. In one sense is it important that whatever the definition is it should be tied to the impact and potential of the act or breach, rather than the fact that it is less than $100,000.

Mr DAVID SHOEBRIDGE: So it should not be an entirely objective test; there should be a subjective element in terms of seriousness?

Mr VAILE: It has to have some subjective element to enable a person for whom it is a really serious matter to make a case.

Mr DAVID SHOEBRIDGE: So it cannot be a wholly subjective test. Surely there needs to be an objective element to it.

Mr VAILE: Yes. It cannot be simply someone saying, "I am very sensitive and everything is terrible."

Mr DAVID SHOEBRIDGE: "How dare you show me in that tie!"

Mr VAILE: That is correct; although it is not a very nice tie.

Mr DAVID SHOEBRIDGE: It is better than mine.

Assistant Professor ARNOLD: That has been a thrust in almost all, if not all, of the reports over the past decade. There must be some degree of reasonableness. There must be a credible reasonableness rather than the lowest common denominator.

Mr VAILE: This is not like defamation, where you are thinking of damages and the level of monetary harm to reputation or impact, and that is the measure. It is something that is probably harder to quantify in terms of seriousness and whether remedies may need to be more creative.

Mr DAVID SHOEBRIDGE: If you are talking about an objective standard, you would talk about a person in those circumstances with those characteristics as well, because that is obviously as important, is it not? A 44-year-old male may have totally different concerns about having images shared than a 22-year-old female.

Mr VAILE: It is useful to take those characteristics into account, but it is not the whole answer. You are a big boy, you are 44 and you are a bloke, you should handle it. There may be some people for whom, because of their circumstances, history, culture, business associations or whatever, it is more significant. There may also be some young woman who will brush everything off despite the fact that you might think it was a humiliating personal slur.

CHAIR: Thank you for appearing before the Committee. Any questions taken on notice should be answered within 21 days. Any further questions members may have will be sent to you, and they should also be responded to within 21 days. I thank the people in the gallery for being here today.

(The witnesses withdrew)

(The Committee adjourned at 5.07 p.m.)

IN-CAMERA **PROCEEDINGS BEFORE**

STANDING COMMITTEE ON LAW AND JUSTICE

INQUIRY INTO REMEDIES FOR THE SERIOUS INVASION OF PRIVACY IN NEW SOUTH WALES

_____

At Sydney on 30 October 2015

_____

The Committee met in camera at 1.50 p.m.

_____

PRESENT

The Hon. N. Maclaren-Jones (Chair)

The Hon. D. J. Clarke
Mr D. Shoebridge
The Hon. B. Taylor
The Hon. L. J. Voltz

Evidence in camera by **WITNESS A**, sworn:

CHAIR: Thank you for accommodating this change to give your evidence predominantly in camera. Hansard will prepare a transcript, which will be sent to you. Anything that you want redacted or would prefer to remain confidential can be accommodated. This is an opportunity for you to make a statement and for us to ask some questions. What you have gone through is absolutely terrible. We thank you for coming forward and putting in a submission. We will not follow a formal structure in the way questions are asked.

The Hon. LYNDA VOLTZ: We would actually like to hear your story.

WITNESS A: I am pleased that you want to hear my story.

Mr DAVID SHOEBRIDGE: But ultimately the issue of confidentiality is a matter the Committee will determine. Your views will be central to that but the final decision about confidentially will be made by the Committee.

WITNESS A: And no doubt you will appreciate that I am rather tenacious.

Mr DAVID SHOEBRIDGE: We have already got that sense, which is probably good.

WITNESS A: Okay. The facts: I am a mother, a wife, I have a -year-old and I have a career as a high school teacher. . If anyone was going to be given this journey and understand the full ramifications of just how awful it could be, it was me. Whilst I did not in any way anticipate that this should happen or could happen, I firmly believe that health facilities in particular should have known that this was coming. They should have had procedures in place and there should be some way that a person can gain control, because for 10 months I had no control. All I had was what I found on the internet and by asking questions. No-one was able to direct me in any way and tell me how I should approach this situation.

last year I went in for a very routine check-up as I have a family history of uterine cancer. During the time that I was sedated, I was completely knocked out with my legs in the air, the nurse charged with looking after me took a phone out of her pocket, a non-sterile phone, and took a single image at 9.13 a m. I know this because forensics has recently been able to gain access to her phone. I had to write a letter to her and ask her to produce the phone. That was because the police were unable under the current legal system to go and knock on her door and ask her to hand it over so that she could prove that she had done what she had said she would do, which was that she had deleted it soon after she had shown the two colleagues at her workplace.

It took 10 months for me to find out whether that image was ever going to turn up in my life again. I have seen the image. Whilst I have been given reassurances that that image will be very difficult to retrieve, nonetheless it is retrievable. She has deleted it, but not at the time she said she deleted it. The metadata showed that she deleted it four days afterwards. I have no metadata to explain how many other people she showed this photo to. The only reassurance I have is that she did not transmit that to her Facebook account and it was not uploaded to a computer and manipulated in some way but, nonetheless, I have seen the image; it is definitely me and it exists. I have to live with that for the rest of my life.

Whilst I know that that image is locked up in secure storage at the forensic laboratory—they are the people that do all the police work— and I can tell you I am terrified not for me but for my son. When he is a teenager if this issue comes up to harass him that is when the real harm will occur to me and really to him. I have got a deep desire to make sure that when this happens again, because I am sure it has happened before, that there are very strict controls placed around the way in which the situation is handled. It took the hospital five weeks to notify me that this event had occurred.

Mr DAVID SHOEBRIDGE: If she deleted the image four days later and the hospital did not notify you until five weeks later how is it that you have seen the image?

WITNESS A: My gynaecological surgeon rang me and said, " , we've already told you that the pathology results came back negative. You do not have cancer, but something else happened." She told me what had happened. Five minutes after her phone call the hospital rang and said, "This has occurred. We are very

sorry. We would like you to come in for a meeting." That meeting did not happen for six months. It was impossible to get her name or her location. To put my extreme distress into some perspective, the last conversation I had with that nurse before they sedated me was about where I lived and where I taught. She told me that she lived in that area and that her kids went to school there. So for about three months I went to work every day wondering whether I was teaching her kids.

As you can imagine I went to the police straight away and I contacted my solicitor. It took six months of asking the hospital to write a letter to the nurse to produce the phone. Unfortunately, they sent it to an incorrect address. My solicitor was able after some time to send another letter. She found the correct address through the electoral roll. She sent the letter. Some weeks later we made contact with the nurse and she said, "Yes, I will do that." She personally got the phone to the forensic people in Sydney, and they were able to actually forensically examine that phone and to find what they found.

The Hon. BRONNIE TAYLOR: Did you find out that the nurse in question took the photo from your gynaecologist?

WITNESS A: Yes, the hospital asked her to ring me and advise me.

The Hon. BRONNIE TAYLOR: But how did the gynaecologist know that the photo existed?

WITNESS A: That is where the big problem is. They did nothing. There were two nurses who she physically showed the photo to.

The Hon. BRONNIE TAYLOR: So someone reported the nurse?

WITNESS A: Yes, and I actually saw her showing one of the nurses when I was in recovery.

Mr DAVID SHOEBRIDGE: So now you have found out what happened you have worked out what it was that you saw at the time—which you did not realise the significance of at the time.

WITNESS A: I can remember looking across the recovery room and seeing her in scrubs with the other nurse. I thought to myself, "Oh, they have a phone; that is a bit strange."

Mr DAVID SHOEBRIDGE: And you now realise what it was that they were doing.

WITNESS A: I heard the other nurse say, "No, how dare you." I thought to myself, "Well, this is a great place to work," not realising that that was about me.

CHAIR: In your submission you said that you had referred it to the nurses board. Can you talk to us about that process and the outcome that eventuated from that?

WITNESS A: In the first phone call I received from the hospital they said that, because the nurses had made a complaint, they had to advise the Australian Health Practitioner Regulation Agency [AHPRA]. I did not know who AHPRA was. So it took some time for me to realise that the hospital were not actually going to tell me that they had made a complaint formally, what that involved and what my part in that was—they did not seem to really care because I did not find out until six months later that that complaint had been made.

When I rang the NSW Health Care Complaints Commission to inquire as to whether a complaint had been made, initially they were rather cagey. Clearly privacy laws exist to protect people, and they certainly protected the nurse. They gave me very limited information. At the time I did not think to ask for a case number. So I rang back after my initial call and they were really reluctant to talk to me. They referred me to the Nursing and Midwifery Council of New South Wales. I did get my case number eventually.

So I rang the Nursing and Midwifery Council of New South Wales and said, "This has happened. I believe it has been referred to you. What do I do." They were really helpful. I have to say that they gave me some great insights into how I could handle the situation, because up until that stage I thought the police might be able to actually do something—but they were powerless. I made a formal complaint online to the Nursing and Midwifery Council and that took approximately three months to resolve. They recently wrote to me.

As part of what I expected to occur, I wanted the nurse to produce the phone so that it could be proven that she had done what she said she had done so that I had some peace of mind. I would actually like to meet her. I just want to meet her and maybe achieve some kind of forgiveness. I would like to get there but I do not think I am there yet. There might be an apology. I got none of those things. They could not even ask, in the process of interviewing the nurse, her to produce the phone for me. They did not ask her if she would like to have a face-to-face meeting with me, and I have never received an apology letter.

Mr DAVID SHOEBRIDGE: What about the hospital?

WITNESS A: I have nothing in writing from the hospital, other than the letters from their insurance company's solicitor.

Mr DAVID SHOEBRIDGE: So in this case the privacy Act has been protecting the privacy of the nurse?

WITNESS A: Absolutely.

Mr DAVID SHOEBRIDGE: But you, as the victim of this entire episode, have been left without any remedy?

WITNESS A: Yes, that is part of it.

Mr DAVID SHOEBRIDGE: I am just getting this clear in my mind. So the metadata says that the image was deleted four days after she took it. You became aware of it five weeks afterwards when the gynaecologist rang. You say that you have seen the image.

WITNESS A: I have, about three or four weeks ago.

Mr DAVID SHOEBRIDGE: Can you tell us how that happened.

WITNESS A: At the end of September we got the phone—well I did not get the phone but PPB got the phone. They did their forensic analysis and then they wrote a report to say what they had found. There was some questioning from me and my solicitor, going backwards and forwards with them. It was then decided that I needed to view the image to make sure it was me. So I trotted into Hunter Street and went in and had a look. It definitely is me. From that I asked a few more questions around the time and how many times it had been viewed. They were unable to give me that information at this stage.

Mr DAVID SHOEBRIDGE: Who is paying for all of this?

WITNESS A: Me.

Mr DAVID SHOEBRIDGE: Has the hospital made any counselling available for you during any of this, or anything like that? For example, when you went to see the image was there anything available to you?

WITNESS A: I actually cannot talk about the one meeting I had with them. As part of my professional practice as a teacher I have a psychologist I usually meet with once a term. I am now seeing her once a week and I am paying for that myself. I have no choice. But I feel that to ask them for money would be just an insult. And if I wait for them, like I have had to wait for everything else, nothing will get done. The only way that I have been able to get this far is by paying or offering to pay my barrister, my solicitor and the other people working with me in my life.

I know that they are calculating what the cost is to them, because it is far more complicated than anybody thought it would be. They are so many tentacles. I have not been presented with a bill for a couple of months from them. But I have indicated that I am willing to pay that. I am certainly not seeking a payout from the hospital, because dealing with them would just add to my trauma. When we looked at what any possible payout could be, we looked at what it would cost if someone lost a finger, a hand or a limb. I thought $15,000 was kind of a slap in the face; notwithstanding that, with any money that came from them, I feel it would be like a payment for a porno shoot—one that I had never given my permission to participate in.

The Hon. LYNDA VOLTZ: You have sat through most of the evidence today so you have heard some of the evidence put to the Committee about the different avenues we can look at in terms of how to deal with this. What would have been the best way forward for you?

WITNESS A: They ring me on day one—at least 24 hours, 48 hours, or as soon as practicable—and say, " , we are just letting you know that an incident occurred. This is what happened. These are the steps that we have taken. We have examined the phone. We have made sure the photo was deleted. The process from hereon is going to be emailed, sent to you in a letter, and these are the steps that you can take to actually make sure justice is served. You need to know that the police will be involved and, unfortunately, while this is not a personal kind of issue, this is a workplace incident."

The Hon. LYNDA VOLTZ: It sounds to me as if you have almost had to do the investigation yourself?

WITNESS A: That would be a correct assumption.

The Hon. LYNDA VOLTZ: One of the views put forward is about the Privacy Commissioner having an ability to act, but fundamental to that may be the need to review who would investigate in those circumstances. As you say, you had tremendous difficulty. You had to start from scratch with no expertise in the area.

CHAIR: We are over time. If the Committee has additional questions they will be sent to you and the Committee may talk further about you coming back for a second time.

WITNESS A: I have got lots to add. I have three pages of notes from just listening to everyone. I am certainly happy to take those questions. I would also be happy to come back because, as I said at the start, I am tenacious, I am determined.

The Hon. BRONNIE TAYLOR: You are brave.

WITNESS A: I am not brave; I am angry.

Mr DAVID SHOEBRIDGE: If the Committee was minded to refer your evidence and your statement to the Privacy Commissioner for her comment, would you object to that?

WITNESS A: I think that would be very helpful. I have not gone down the path of the Privacy Commissioner because of the six months time—

CHAIR: Has a nurse or anyone told you why she did that?

WITNESS A: No, but I can tell you from what I have found on her Facebook account why. It is because I am an obese person. She likes to shame obese people. This has got tentacles.

The Hon. LYNDA VOLTZ: I am surprised you are only angry.

CHAIR: On behalf of the Committee I would like to thank you for your courage in coming forward. In this inquiry we need people to come forward who are victims of where the system has failed in order to look at ways of addressing that. On behalf of the Committee I express our condolences for what has occurred to you and thank you for coming forward. I hope that the work of this Committee will help in some way to address this issue and to prevent it from ever happening to anyone else in the future.

WITNESS A: I just want to get back to happiness and this is helping me.

Mr DAVID SHOEBRIDGE: We are all with you on that.

WITNESS A: I get that you get it. I know that there are three of you who are nurses—I have done my homework. Thank you.

(The witness withdrew)

(Conclusion of evidence in camera)