NATIONAL PRESS CLUB OF AUSTRALIA

Transcript

Program:	National Press Club Address	Date :	11 Dec 2019
Compere:	Steve Lewis	Time:	12:30:00
Summary ID:	C00081393104		
Item:	National Press Club Address – Paul Fletcher – 11 December 2019		

NATIONAL PRESS CLUB ADDRESS
PAUL FLETCHER 11 DECEMBER 2019

STEVE LEWIS: Ladies and gentlemen, welcome to the National Press Club and today's Westpac Address, the 68th that we've had in this year 2019; tumultuous, a very important year in the political cycle. A very successful year for some, including our guest speaker today. It is our final Press Club address for 2019, and we are very pleased to have Paul Fletcher, the Member for Bradfield, but the Minister for Communications, Cyber Safety and the Arts to address the National Press Club. Paul has just celebrated 10 years in the Federal Parliament, but there is no long service leave for the Minister. Instead, he's got a very, very busy agenda today. He's going to talk to us about what's happening in online safety, how we can keep the internet safer, and how Australia can flourish in this globalised world.

Please welcome, Paul Fletcher.

[Applause]

PAUL FLETCHER: Well, it's good to be here at the National Press Club to speak about how we keep Australians safe online, which has been a priority for our Liberal-National Government. We set up the world's first eSafety Commissioner tasked with keeping all Australians safe online. The commissioner has strong tools to protect children against cyber bullying and to protect Australians, and particularly women, against image-based abuse. But we need to do more. The internet has brought extraordinary economic and social benefits. And as Minister for Communications, I promote the benefits of connectivity every day. But sadly, we also need to recognise that while most interactions online are positive, some will bring danger. We need to recognise and guard against that danger. And as Minister for Cyber Safety, my task is to help build those tools.
Keeping Australians safe, of course, is the first duty of government. But by doing so, we also support the continued growth of an internet we want to be part of. An internet that embraces and enables the best part of humanity and not the worst. Our Government's

approach then is a plan to keep Australians safe online in tandem with all of our other work, to leverage the online transformation of our economy. Our Government and our community has clear expectations about internet safety. Serious online abuse of an Australian is not acceptable, no matter that person's age. Harmful material must be taken down faster. Attempts to send terrorist attacks viral must be stopped in their tracks. Industry needs to step up and take more responsibility. We need smart, new approaches to getting harmful content down when fringe gore sites want it glorified. We are putting the pressure on and keeping the pressure on. Today, I am opening public consultation on proposals for a new online safety act, intended to bring these principles into law. This act will put pressure on industry to prevent online harms and will introduce important new protections for all Australians. So today I want to start by talking about what the community expects when it comes to online safety. Next, I want to speak about the evolving role of Government in helping keep people safe online. And thirdly, I want to explain our plans for a new online safety act.

Well, let me turn first to what the community expects. When people interact in the physical town square, they take it for granted that the rule of law applies. If they are assaulted or defrauded or otherwise hammed, they can go to the police and seek assistance, or they can go to court and seek redress. People expect the same thing when they interact in the digital town square, and yet unfortunately some sectors of the internet industry have been slow to meet the community's expectations when it comes to online safety. I saw this in 2014 when I was working on the legislation to establish the eSafety Commissioner for the first time. The peak body for companies including Google, Facebook and Microsoft was very resistant. In a submission to Government, they said they had, quote, serious practical concerns with the proposed policy. A rapid take-down scheme will at best take five days, much longer than the industry's own processes. The possibility that the policy will push children to undertake risky behaviour on platforms with less highly developed self-regulatory standards and significant likelihoods that the laws will be unable to keep pace with the technological change, close quotes. I'm pleased to say we were not deterred. We implemented the policy and it has worked. And in fairness, I will acknowledge that some of these same companies have developed an excellent partnership with the eSafety Commissioner, with material being taken down, in some cases, within 30 minutes. But there does continue to be a significant disconnect between the expectations of Australians and what is delivered by the internet industry today. And a key manifestation of that disconnect is that many of today's most popular digital products and services have not been designed with user safety in mind. That needs to change.

We need to get to a point where our online highways benefit from the same rigorous approach to safety we see in the global automotive market, where international standards

enforced by legislation, made by sovereign nations, are met by global manufacturers as they supply their vehicles to individual nations within global markets. Our Government expects digital platforms and large tech firms to play their part. The eSafety Commissioner has pioneered a world-leading safety by design initiative, working with industry on a best-practice approach to taking responsibility for the impacts of the products and services they are creating.

We want to go further. That's why today, I'm also releasing the Government's Online Safety Charter, a document that sets out the Government's expectations on behalf of the Australian community of social media services, content hosts, and other technology companies. The charter endorses and expands on the Safety by Design principles. It's based on the premise that behaviour that is unacceptable offline should not be tolerated or enabled online, and that technology companies have a responsibility to mitigate and address any adverse impacts that are directly or indirectly associated with their products or services. It outlines the Government's expectations of service providers, and the steps we expect them to take to prevent their platforms from facilitating online harm. Of course, while we are very clear about the responsibilities of internet companies, it's also critical to equip Australians with the knowledge and tools to engage safely online. The eSafety Commissioner has a strong focus on online safety education, providing training resources in 22 languages to teachers, parents and front line workers. That's why the Safety by Design principles and the charter indicate that platforms should provide tools that empower users to manage their own safety. The charter sends a clear message to industry, and industry has the opportunity to step up and meet Australia's expectations when it comes to preventing online harms. And my strong message to companies in the industry serving Australians is to read it, refer back to it, and most importantly, integrate it into your daily practices. I also encourage companies to continue to work with the eSafety Commissioner on the implementation on the Safety by Design initiative.

Well, having spoken about community expectations, let me turn to the role of government. During the very early years of the internet, when it was essentially a specialised resource for a small number of scientists and academics, many argued that it should be beyond the reach of governments. In 1996, John Perry Barlow issued the declaration of the independence of cyberspace which began, quote, governments of the industrial world, you weary giants of flesh and steel, I come from cyberspace, the new home of mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather, closed quotes. Well, such a non-interventionist approach may have been barely tenable in the early 1990s when very few people were online, and in Australia, less than one per cent of the population. But it was certainly

untenable once the internet became a mass-market consumer phenomenon. And by as early as 2001 in Australia, half the country was using the internet. So the Australian Government was an early mover amongst governments globally. In 1999 we amended the Broadcasting Services Act with the addition of the scheme to regulate online content in Australia. At the time, that legislation was world-leading, but in those early actions, there was a certain lack of confidence. The online content scheme provided for differential treatment of content hosted in Australia and content hosted overseas with no capacity for the regulator to take firm action against the latter. This was based on a view at the time that attempting to impose Australian law on websites hosted overseas was a futile exercise.

Well, since that time, the Australian Government has taken an increasingly assertive approach. In 2015, as I mentioned, we established the world's first children's eSafety Commissioner, a dedicated statutory position with a mandate to keep Australians safe online. We established a legislated cyber bullying take-down scheme which has assisted almost 1600 children. We've expanded the eSafety Commissioner's role since then to encompass online safety for all Australians. We've given the Commissioner power to address image-based abuse, and the Commissioner has since received over 1800 reports concerning over 2500 URLs, and has successfully removed images in around 90 per cent of those cases. The Commissioner has handled increasingly large numbers of illegal and harmful content complaints. It is on track to complete 12,000 investigations into child sexual abuse material this year alone, an increase of 50 per cent on the previous year. And globally, Australia has been a strong voice for online safety.

In 2013, Australia chaired the discussions that led to the UN general assembly agreeing for the first time that the law applies online as it does offline. In 2017, Australia advocate for the inclusion of the online dimensions of tackling violent extreme in the G20 leaders' statement on encountering terrorism. And this year, Prime Minister Scott Morrison played a key role in securing a G20 leader's statement calling on the tech industry to do more to prevent the misuse of their platforms by terrorists.

Over the last 20 years then, governments in Australia and globally have become steadily more engaged in regulating the online environment and this has meant facing up to several challenges. The first challenge, of course, is that the internet has made it much cheaper, easier and quicker to make the kinds of statements that threaten public safety and public order. People have always been able to make statements which are personally abusive, which are designed to dupe or mislead those who read them, or which provide instructions about how to build a bomb or hijack an aircraft or kill yourself. But today, such a statement made online at effectively zero cost to the person making it, can be visible potentially millions, tens of millions, even hundreds of millions or billions of people. In other words,

these harms have always been possible, but the internet greatly magnifies the reach of such harms.

The second challenge is that the internet enables whole classes of new conduct which can harm or endanger others. Today, almost all of us carry smartphones, internet-connected devices which can record sound, take pictures, take videos and can communicate that instantaneously to large numbers of people. The appalling Christchurch mosque attack in March this year, for example, was livestreamed using Facebook, meaning the devastation and violence was not limited to the victims and the witnesses, but spread to enormous audiences around the world.

This simply could not have happened even a few years ago when bandwidth on mobile networks was not sufficient and when sophisticated livestreaming applications did not exist. Now, our government acted quickly to address the emergence of this new harm by introducing legislation and working with industry through a dedicated taskforce to reduce the likelihood of it happening again. As I mentioned before, another new harm we face is the unauthorised sharing of intimate images colloquially referred to as revenge porn - although, I think image-based abuse is a better term. Again, this is something unimaginable even 20 years ago, but today one in 10 Australians has had intimate images shared online without their consent.

I recently met with Noelle Martin, Western Australia's- the Young Western Australian of the Year, a survivor-turned-advocate on the issue of image-based abuse, and it was the work of people like Noelle which led to the Australian Government responding with the image-based abuse scheme that has since helped so many Australians and a significant majority of them being women.

There is a third challenge which the internet presents when it comes to keeping Australians safe. The harms that I've described occur on the websites, social media platforms and other online services used by millions of Australians every day. In the main, these services are based in other countries. So unlike traditional forms of harm, an online perpetrator does not need to be within Australia to impact Australians, and this creates significant complexities in establishing and enforcing regulatory frameworks to protect Australians. If this is a challenge when the services are delivered by legitimate regulated businesses, it is an even bigger challenge if they are delivered by criminals. Nearly all of the illegal content reported to the eSafety Commissioner originates from platforms hosted overseas.

In fact, the reason that Julie Inman Grant, who is doing an exceptional job as our eSafety Commissioner, is not with us here today is because she is representing Australia in Ethiopia at the Global Summit of We Protect, the significant international forum for cooperation

against online child exploitation, and Julie is on the board of that important global organisation.

This is just one example of how we are working internationally to make the internet a safer place. At the same time, we have an extensive program of work across many portfolios within the Morrison Government to establish clear rules and expectations about online content. The ACCC's digital platforms inquiry, for example, looks at the significant competition and consumer issues raised by the dominance of players like Facebook and Google. Before the end of the year, we will announce the Government's response across the 23 recommendations. The Attorney-General is working with his state and territory counterparts to address the responsibilities and liability of digital platforms for defamatory content published online, and I'm working with the Minister for Families and Social Services in taking action to protect Australians against illegal offshore gambling websites, empowering the ACMA to work with internet service providers on a website blocking the scheme with civil penalties and disruption measures.

But the centerpiece of my work as Minister for Cyber Safety is the new online safety act that we have committed to introduce. And today, I'm releasing a consultation paper designed to gather input as we develop that new act. Our plans for the new act draw in part on the practical day-to-day experience of the dangers Australians are facing online today including what they report to the eSafety Commissioner. It might, for example, be a female journalist who has written a story about gender equity in Australian sport and is subject to extreme levels of harassment, abuse and vitriol from a particular individual across multiple online services. Despite contacting the services, that material remains online and today, she has no avenues by which to have that seriously harmful material removed other than contacting the police.

Under the proposed act, the eSafety Commissioner would have the power to have this content remove from the social media services, from websites, and from maps. It might be the case of a 14-year-old boy being cyber bullied. The bully has created a video using Twitch where he says awful and humiliating things about the victim and is sharing the link with all of his classmates. Today, that young boy has to endure that for up to 48 hours. Under the proposed act, the eSafety Commissioner would be able to cut that time in half.

It might be the case of a young woman whose former partner has posted intimate images of her on a so-called revenge porn site hosted overseas. Today, while the eSafety Commissioner can issue a notice to the overseas host to remove the content, if the website ignores the notice, there’s little more the Commissioner can do. Under the proposed new act, the eSafety Commissioner could issue a notice to Google and to Bing to request that the link to the offending page be de-ranked in search results.

So let me describe then the key features of the proposed new Act. First, it will set out what we call the basic online safety expectations. These will draw on the Safety by Design principles, the online safety charter, and of course the feedback we receive from the consultation process I'm kicking off today. Examples of such expectations would include providing tools and processes to empower users to manage their own safety, actively enforcing terms of use, and improving the transparency of online safety efforts. The eSafety Commissioner will have the power to request that internet companies report regularly on what they are doing to meet these expectations. If a company fails to report, it will attract a penalty, and of course, if it fails to meet our expectations, you can expect the eSafety Commissioner to have something to say very publicly about that.

As we committed at this year's election, the Government will also work with industry to develop additional protections for children. We will be asking industry to see that services marketed to children default to the most restrictive privacy and security settings and we will also work with industry on providing information about parental controls and online safety features at all points in the supply chain for products and services marketed to children.

In this act, we are going to further strengthen the existing cyber bullying scheme which is presently limited to social media sites; it will be extended to apply to all of the platforms, the games, the apps that our children are using online, and we also plan to reduce from 48 to 24 hours the time-frame required to respond it a take-down notice, be it for cyber bullying or for image-based abuse.

Now, as I don't need to convince certainly any of the journalists here today, adults are too often the target of serious online abuse, and since June 2017 when the eSafety Commissioner's role was expanded to promoting online safety for all Australians, over 1500 adults have sought assistance from the eSafety Commissioner in response to serious cyber abuse. But the eSafety Commissioner today has no legislative power to investigate adult cyber abuse.

There is a strong policy case for a take-down scheme targeted at the most seriously harmful online conduct, conduct which is already criminalised in the Criminal Code, and the Government therefore proposes to introduce a new scheme directed at serious cyber abuse against Australian adults with its own take-down regime and appropriate civil penalties. This will help to minimise the harm experienced by victims of online abuse who may not wish to go through criminal proceedings, but are very keen to get that material taken down as quickly as possible.

The act will also address several weaknesses in the current arrangements. For example, as I mentioned before, because of the legislation introduced in- some years ago, the actions of the eSafety Commissioner can take to address prohibited content such as child exploitation

material vary depending upon where the material is hosted. If it's hosted in Australia, the eSafety Commissioner can direct the hosting provider to take down that material. But exactly the same content hosted overseas runs up against limitations in the eSafety Commissioner's powers. So we are going to expand those powers so that the eSafety commissioner can focus on having the most harmful types of content removed, regardless of where it's hosted. And this includes child exploitation material, abhorrent violent material, material that incites terrorism or violence and other extreme material as determined by legislative instrument where necessary.

We intend to maintain the current restrictions on prohibited online content which currently include X, 18+ content and R18+ and some MA15 plus material that is not age-restricted. However, through new industry code arrangements there would be a stronger requirement for industry measures to protect users from exposure to this type of content and to expedite remedial action. The government remains concerned with the ease of which children can access pornography and other types of harmful online content. The codes will require industry to provide their customers with optional products that can be used to limit exposure to prohibited online content in their own homes. And the eSafety Commissioner would have a role in these arrangements; the commissioner would need to approve the codes before they came into effect and would investigate breaches of the code.

An important aspect of the new act would be to give the eSafety Commissioner new powers to work with a wider range of players to get harmful online content down quickly. As one example, an investigation last year by Tech Crunch found several third-party apps that enabled users to find groups dedicated to sharing child exploitation material that were available on Google Play. Going to the operators of these apps is one way for the eSafety Commissioner to get the material down, but another way is to ask Google Play to remove the apps. In last year's case, Google Play removed at least six of these apps in the wake of the report.

Google Play is an example of what we are calling in the new act an ancillary service provider. Although it does not host the content itself, it provides or facilitates access to services that in some cases may host harmful online content. The eSafety Commissioner has a high success rate in having intimate images, for example, taken down at the source, but there are rogue websites that do not comply with requests. Thankfully, Google has excluded revenge porn from its internet searches. This approach though is not yet universal and in January, there were concerning reports that Microsoft's Bing search engine could be used to find and suggest child exploitation material. These developments illustrate the potential for third parties or ancillary service providers to play a greater role in tackling seriously harmful online content hosted offshore.

Under the new act, we propose that the eSafety Commissioner would be able to request assistance from search aggregator services and digital distribution platforms to prevent access to seriously harmful material. So if a website systematically and repeatedly allows the posting of cyber bullying or cyber abuse or illegal material despite requests to remove it, the eSafety Commissioner might then ask a search engine to de-list or de-rank that website.

Finally, we proposed to give the eSafety Commissioner the power to direct internet service providers to block domains that contain terrorist or extreme violent material quickly, during an online crisis event such as the Christchurch attacks. This was a recommendation of the Australian taskforce to combat terrorist and extreme violent material online which was agreed to by industry and the government. To facilitate the blocks, the eSafety Commissioner will be able to issue voluntary notices to ISPs and that would be backed up with the power to require action from ISPs. Any such mandatory notices would be subject to appeals and transparency mechanisms to provide appropriate oversight of the exercise of this power by the eSafety Commissioner. And of course, the use of that power would be strictly limited to dealing with online crisis events such as terrorist attacks or extreme violent material.

Well, let me conclude then with the observation that I have been working in this industry long enough to know that some of what I've just outlined will make some industry representatives uncomfortable. But what I've outlined is the next phase of the collaboration that is needed between government and industry to maintain Australians' confidence in the online world, confidence that the internet is a remarkable resource for good, that they and their children can safely embrace into every part of their life. To make sure we success in this effort, I strongly encourage those with an interest in online safety to contribute to our consultation process, and I am confident that through this process we can continue to make the internet a safer place for Australians. Thank you.

[Applause]

STEVE LEWIS: Thank you, Minister. I think it's fair to say that the entire tech industry is listening with intent to that speech. And thank you for outlining some of the key features of the Online Safety Act.

Can I ask you the first question? You have put the tech industry on notice. You have flagged that the eSafety Commission and Commissioner will be a much, much more powerful regulatory body than it currently is. Would you envisage- what are going to be the enforcement powers? Are we talking about potentially criminal penalties against

individuals or some of those companies that you mentioned if they breach this new act, which presumably will come into effect next year? Please.

PAUL FLETCHER: Well, thanks, Steve, for that question. I'd make a few points. Firstly, under the existing arrangements, there are mechanisms in the Act to deal with a failure by companies to respond to notices, and so we'll be maintaining those mechanisms.

STEVE LEWIS: But you will be toughening those up, presumably [indistinct]?

PAUL FLETCHER: Well, what we'll also be doing is setting out the basic online safety expectations and imposing reporting requirements, and certainly, a failure to meet those reporting requirements will attract penalties. I might say also that if don't see sufficient performance in meeting those basic online safety expectations, we certainly reserve the right to engage in more detailed regulatory enforcement action.

But the other point I'd make is this: that an important part of the philosophy underpinning the way the eSafety Commissioner has worked to date is to provide a quick, practical remedy for those who are victims of online abuse through the sharing, the publication online of material, cyber bullying material, intimate images and so on, where overwhelmingly, what people want is to get that material down quickly. And so, that is- a big part of what we're doing here is expanding the scope of where there will be that capacity for the eSafety Commissioner to issue take-down notices, to get such content down quickly. The scheme has worked effectively in the areas that it presently covers, and that's why we want to expand it, and certainly, of course, where appropriate, it's backed up with appropriate penalties.

STEVE LEWIS: Thank you. A question from Andrew Tillett.

QUESTION: Andrew Tillett from the *Australian Financial Review*. Thanks for your speech today, Minister. As well as dealing with the tech titans, you've got it look after the media moguls as well as part of your portfolio duties. We've currently got a situation where Kerry Stokes' Channel 7 is trying to buy Prime, the regional broadcaster, and being blocked by Bruce Gordon, the owner of WIN, and Anthony Catalano, the new owner of Australian Community Media, the regional newspapers. They both separately want to buy Prime, but they're currently blocked by the media ownership rules – the one to the market rule and the voices test in the case of Mr Catalano.

Are you open at all to changing any of those media ownership rules, in particularly, maybe, around perhaps countering social media companies like Facebook as a publisher under the

voices test? Is there any room to revisit at all these media ownership rules or is that off the agenda?

PAUL FLETCHER: Well, the point I'd make is that my predecessor, ex-Communications Minister Mitch Fifield, introduced some very significant changes to the Broadcasting Services Act under which it is now possible for a transaction of the kind that's proposed, namely the Seven-Prime merger to proceed. That would not have been possible without the changes that we made in 2017. So we have made very significant changes in response to the way that the media sector has changed and the competitive landscape has changed very significantly.

So, clearly, there was- the rationale for the transaction is to take advantage of those changes to the law, which would allow greater scale. Of course, how the particular transaction plays out and what individual shareholders do is a matter for them and not something that I would comment on. But in the broad, the point I'd make is we have made very significant changes to the Broadcasting Services Act. Those have already produced some significant changes in the Australian media landscape, such as the Nine acquisition of the former Fairfax newspapers, and we've just seen an example of another significant transaction being proposed to take advantage of those very changes.

STEVE LEWIS: Fergus Hunter.

QUESTION: Fergus Hunter from *The Sydney Morning Herald* and *The Age*. Thank you for your speech, Minister. User privacy is clearly at the heart of a lot of what you've talked about today and it's also a big part of the digital platforms inquiry. It's interesting to contrast that with this battle over encryption. These tech companies are warning that the Australian Government's demands, and the demands of other governments, to have backdoor access to encrypted services will break the entire system, will break the security for billions of users and undermine their privacy and threaten their wellbeing.

Is there a contradiction there between your emphasis here and the emphasis on privacy and this pursuit of backdoors and encrypted services? And how are you going to navigate that law enforcement incentive with the incentive to protect people from harm?

PAUL FLETCHER: Well, I'd make a couple of comments. The first is that the way that the powers of the eSafety Commissioner operate is, in the main, that a complaint is made by somebody who's been the victim of material being disseminated online, that is abusive or is the sharing of intimate images – other things that the complainant, for good reason, does not want posted and available on the internet. Now, by definition, that's content that is

seen by the complainant and by others. More broadly, though, what I'd say is, as I've been seeking to articulate in my remarks today, our government has a set of expectations of the major internet players. Indeed, all participants in the internet industry. If you are operating in the Australian market, serving Australians, serving the community, we have a set of expectations. I focused today on those expectations as they apply to online safety. But we also have a set of expectations about how you operate with law enforcement agencies.

And I may say from my own background in the telecommunications sector, there's always been a set of extensive expectations and legal requirements on the telco sector as to what they need to do to comply with the requirements of the law enforcement agencies, as part of keeping Australians safe, and we've similarly got a clear set of expectations of the internet platforms and indeed, all participants in the industry. My colleague Mr Dutton, of course, leads the work on that front. But again, it goes to the principle that I spoke about – that 20 years ago, 25 years ago, there were some arguing that the internet should, in some way, be beyond the reach of the law. That is not a sustainable position. Whether you're operating online or off line, you need to comply with the law.

STEVE LEWIS: Tim Shaw.

QUESTION: Minister, Tim Shaw, director of National Press Club board. Keeping Australians safe online, I know that's your theme, but today, firefighters around the country are trying to keep Australians safe. You, Minister McCormack, and certainly Minister Littleproud must have had discussions or intend to have discussions about the reconstruction of damaged communications infrastructure, particularly in these bushfire-affected areas. You've acknowledged your background in telecommunications. What can you do or do you intend to do to get those individual companies to assist in the reconstruction of that damaged infrastructure? It's one thing to talk about cyber safety, but communication in those regional communities is critical. What's your intention, and will you use Australia Post as part of that delivery of services?

PAUL FLETCHER: Can I make the point, first of all, that in terms of direct responsibility for emergency response issues, that does sit with my colleague, Minister Littleproud. He and I work together. We met with all of the major carriers some weeks ago for a briefing on their disaster preparedness. And certainly, the telecommunications industry has a very important role to play in Australia's response to disaster, both in preparing and also in getting back up and running as quickly as possible after, be it a bushfire or a flood. I certainly get regular updates on network status through NBN and through the other operators. To date, in the main, certainly, there have been instances of both fixed-line and

mobile network facilities being knocked out by fires. They've been able to come back online pretty quickly.

And I would make the point that because of the NBN's satellite coverage all across Australia, we have a degree of, in the telco jargon, redundancy. That's to say even if the terrestrial network has been
destroyed in an area, NBN has 10 satellite-equipped trucks that are able to go into any part of Australia and provide immediate connectivity. So, they've got their onboard power. The dish on the back of the truck connects up to the satellite and so that can be a very useful resource, particularly in a
disaster response scenario. Now of course, those trucks only go in when requested by emergency services and when the advice is clear that it's safe to go in. But for example, in the Townsville floods earlier this year, that was an important service that NBN was able to provide in one of the evacuation centres, meaning that people who were very anxious about contacting their insurance company, contacting friends and family to let them know they are safe, they had the capacity to do that. And so, it is actually an important piece of additional redundancy in our national telecommunications architecture, which we did not have until a few years ago.

STEVE LEWIS: The next question is from Sarah Ison.

QUESTION: Sarah Ison from *The West Australian*. Thank you for your speech, Minister. You spoke about age restrictions in terms of pornography and under-18s having access to that, but how concerned are you about age restrictions more generally? It's pretty well-known that it's pretty easy for someone who's under the set age restriction for a certain site, particularly social media, to still get access. That's something a lot of countries are struggling with.

How big a concern is it? How big is the impact? And what are we going to do about it?

PAUL FLETCHER: I think it falls into very much the category of things that we're wanting to go to with this notion of basic online safety expectations. What are the age verification mechanisms and what do you need to do to establish an account? It links to a range of other issues that have arisen in the context of abhorrent violent material, the capacity to- how quickly can new accounts be established, automated account establishment processes by criminals or terrorists. So, yes, there's certainly a significant set of issues there, and absolutely, that question of how- what age verification requirements exist are the kinds of things that we see as potentially falling within the basic online safety expectations.

STEVE LEWIS: Minister, in a fortnight's time, we're going to be celebrating Christmas. A lot of kids, excited kids, are going to be opening presents. A lot of those presents, more and more, are going to be linked to the internet. There's a lot of concerns about the fact that kids are basically exposed to the internet through these toys.

What's your concern and what is your message to parents to- how concerned are you that they could fall prey to some of these online trolls, et cetera, through everyday toys and that? Is that something we should be concerned about?

PAUL FLETCHER: There certainly are risks and dangers for children online, as at the same time there are enormous educational and social benefits for children and for all of us. The important thing is for parents to be aware of those risks and have resources available to them so they can help keep their children safe while also allowing them to have the education and other benefits [indistinct]…

STEVE LEWIS: [Interrupts] What's the best way to find out? If they've got a concern about a particular toy that's linked to the internet?

PAUL FLETCHER: Well, one thing I'd recommend you do is go to the e-safety.gov.au. And as I mentioned in my speech, one of the things that we are seeking to do is make information about parental control tools available at all stages of the sales process, so that that information is readily available to parents. The first thing I would say to parents is if you're getting your child a new phone for Christmas, don't get it out of the box and hand it to them and get them to set it up, because what you need to do is make sure you have identified where the parental control tools are and set those up, gone through and said: okay, what level of content do I want my child to be able to see? And so if you give the device straight to the child and they set it up, then you've missed that opportunity. So be aware that there are parental control tools on smart phones and on most devices. Find out how to use them. They are good tools, and it's part of modern parenting.

STEVE LEWIS: You are making a brave assumption that most parents know how to set up smart phones. [Laughter] And looking around this room, I'm not all that confident. Our next question is from Zoe Samios.

QUESTION: Thank you, Minister. Zoe Samios from *The Australian*. You mentioned the ACCC's Digital Platform Report and that the Government would have a response before the end of the year. Christian Porter has spoken previously about a level playing field between traditional media and the technology platforms. And I'm just wondering whether that would be reflected in your response and whether defamation law changes are at play at all.

PAUL FLETCHER: Well, there are a couple of separate process wrapped up in there. So Christian Porter, as Attorney-General, is working with his state and territory counterparts on the question of defamation law as it applies to online material, with the New South Wales Government taking the lead in the work there. And separately, in terms of the Digital Platforms Review, there's 23, recommendations as you know, across a range of areas. There's privacy issues, consumer protection issues, competition issue, a lot of media policy issues, and so we are obviously working through our response on that, and that response will come out before the end of the year.

STEVE LEWIS: Our next question from Jackson Snape.

QUESTION: Minister, Jack Snape from ABC. Thank you for the address, and good luck with the Online Safety Act, sounds like a big job. But I'm keen to ask you about the NBN. We are on the cusp of 2020, sounds futuristic, we're still faced by many challenges, and the same challenges then; telecommunications. The NBN was set up originally to bridge the digital divide between metro and regional Australia. The rollout is finishing next year. We are seeing dribs and drabs of funding for regional NBN, regional home broadband services. I think in 2023 there is the last bit of CAPEX for NBN on the fixed wireless network. There is also a move to funding under the regional broadband levy. I just want to take you into the detail about what your plans are with regional Australians' internet access. At the moment, they are stuck, many on 6 megabit per second busy-hour speeds. That's pretty much the threshold the NBN Co seems to be pursuing. Beyond 2023, how is the Government going to address this digital divide? And in the meantime, would you encourage Australians struggling with the NBN to pursue 4G or 5G solutions for their home broadband?

PAUL FLETCHER: Thanks, Jackson. I would say a couple of things. Firstly, I looked up the numbers the other day for a speech I was giving about having spent 10 years in Parliament. And 10 years ago, 5 per cent of Australians had access to internet services with a speed of 25 megabits per second or more; 5 per cent. It's now 85 per cent. So we have made a very substantial amount of progress. There's over - about 10.3 million Australians or premises now able to connect. About 6.2 million premises are connected, 35,000 premises connecting a week. Bear in mind that it took the previous Labor Government six years to get 50,000 premises connected to the fixed-line network. We are doing 35,000 a week. Now, in terms of where services are for regional and remote Australians, for those on the satellite, they've got access to the peak speed of 25 megabits per second. For those on fixed wireless, a peak speed of 50 megabits per second. So that is a very significant step up from what was available even a few years ago. And we are seeing very extensive use of both of those networks. NBN certainly plans continued CAPEX. In their most recent

corporate plan through to 2023, they are talking about $4 billion of CAPEX over the next few years, as we continue to improve the network. And of course, we are in the middle of spending $800 million to improve the experience of people on fixed wireless. And in the main, it has been a consequence of where we've had areas of rapid take-up, we've needed to go back and allocate additional capacity to divide the base stations into more sectors, also increase the back haul. All of those things are happening. That particular number you quoted is a jargon term for the busy-hour speed. It is a piece of network measurement, really. People will get much more than that, almost all of the time, but the key point is, it's double what the network was designed with. When we came to Government, we found it had been under provisioned. We redesigned it with nearly 1,000 additional base stations. So we've moved it a long way. But of course, this is a continuing story. People's expectations naturally continue to increase, and the amount that we are all using the broadband network continues to increase. In June of this year, the average customer across the fixed-line and fixed-wireless networks was downloading over 250 gigabytes a month. By contrast in 2010, that number was 11 gigabytes. So we've seen a massive, massive increase in our use of data, much of it driven by video streaming, not just for entertainment, but also for education, health and so on. So the NBN has made a very big difference in the lives of people in regional and rural Australia. Of course, there's always more we can do, and it is a continuing journey. But if we look at how things have changed over the last few years, it has been a big change.

QUESTION: Just on the second part of the question, would you encourage regional Australians to pursue mobile broadband solutions?

PAUL FLETCHER: Look, what I encourage is competition. I certainly, and I have spoken about this in the past, I certainly believe that NBN is and should be subject to competition, including from wireless, 4G and increasingly 5G. And I encourage Australians to go out and find the provider who gives them what they need. Now, there is a lot of choice over the NBN, different price points, different download limits and so on from the different retail service providers. And there is also continuing product innovation to better meet the needs of people in regional and rural Australia. So we recently introduced the Sky Muster plus product over the satellite. The way that works is that certain content is not included in your download limit. So if you have teenage kids in the house and they go crazy on video streaming and use up your download limit, that does not affect your capacity to do your banking, a whole lot of web-based content, and that has been very well received. That was developed after a lot of engagement with regional and remote customers, and it means that people can have the certainty that the essential services for the business, because a farm is obviously both a business and home, that the essential business services are there all through the month even if you've hit your download cap on video. So there is a whole

range of way we're working to better tailor the NBN product offerings to meet the needs of regional and remote Australians.

Another example is, we recently introduced a business-grade satellite service, and one of the elements of the business-grade product is very low band width service, only 10 kilobits per second, same speed up and down. Why would you possibly want that? For internet of things applications such as soil moisture monitoring. If you've got monitors across a lot of your fields, you need to get that data back into the network. To be able to do that over the satellite, that is an ideal application, and so we're at a point now with the rollout is almost complete, what our focus can be on much more is how do we leverage this massive public investment, peak funding of $49 billion, how do we best leverage for social and economic advantage for people in regional and remote Australia and people in metropolitan Australia? And those couple of examples I've given, in my view, show the way that we're now able to devote more mind share to using the network as we get to the end of the challenge of getting it rolled out as quickly as possible.

STEVE LEWIS: You mentioned $49 billion of public investment; wouldn't the NBN be more efficient in private hands?

PAUL FLETCHER: Well, our policy on that is no different from what our predecessors established for the NBN, namely the Act sets out the series of things that need to happen before it can be privatised, but it contemplates it being privatised.

STEVE LEWIS: [Interrupts] What's your time-frame?

PAUL FLETCHER: Well, I've been clear that won't happen any time soon. We need to focus on-

STEVE LEWIS: [Interrupts] Is it this term, I mean, over the next several years?

PAUL FLETCHER: It's not going to happen anytime soon.

STEVE LEWIS: So the investment bankers shouldn't get excited.

PAUL FLETCHER: It is premature to be talking about NBN privatisation. We've got to complete the rollout and then make sure that we are fully leveraging it for economic and social advantage. That is my-

STEVE LEWIS: I'm mindful it's nearly Christmas and I just wondered whether there's an early present. Our next question from Katie Burgess from *The Canberra Times*.

QUESTION: Katie Burgess from *The Canberra Times*. Thank you so much for your speech. Were you consulted about the massive machinery of government change we saw last week, where your department, the Department of the Arts was folded into the Infrastructure Department? And what do you think it says that Australia no longer has a dedicated, or an in name at least, a Federal Department of the Arts?

PAUL FLETCHER: Yes, I was consulted and I'd say a few things. Firstly, there's been no change to my ministerial responsibility for the Arts. The Arts are still represented by a Minister in Cabinet. There's been no change to the number of people working on arts policy issues. They will now form part of a merged department, but no change to the number of people. This is- there have been two periods in the last 10 years where the Arts has sat within departments that do not have arts in the title - one under Labor, one under the Coalition. In Queensland, arts officials sit within a department that does not have arts in its title; ditto in New South Wales. So this is not unusual or unprecedented. There's no change in the resources committed to the Arts. $749 million is what the Commonwealth is committing to the Arts in 2019-20. There's no change to the Australian Council or to Screen Australia or to all of the other agencies within my portfolio which deliver arts outcomes.

STEVE LEWIS: So your message to the arts community is absolutely no change? Because that decision has copped a lot of flack from the arts community, a lot of very senior film producers and others have really hit out at that particular decision.

PAUL FLETCHER: My message is it's business as usual. We're strongly committed to the arts and I think there are interesting ideas for cross-pollination. You know, one of the things that arts people say to me often is that they don't want to be just put into a bucket that's only about arts. It's a sector that
is full of very creative, innovative, thoughtful people, and they want their expertise to be available more broadly. This is a good opportunity to do that and certainly I think the arts focus and capability is really interesting going into a department which also has responsibility for regional development. The more we can make the arts available to people in regional Australia - and there's great arts activity - the HotHouse Theatre in Albury Wodonga, is one place I've had a chance to go and see a show, or the Araluen Gallery in Alice Springs where I had the chance to see Desert Mob, a wonderful show drawing on the works of about 30 Indigenous [indistinct] communities in central desert region. So there's a huge amount of artistic activity happening in regional Australia. I'm excited this is one way that we might even be able to boost it.

STEVE LEWIS: So what about an arts statement? I mean, why don't you come back to the National Press Club next year, we'd have you back anytime Minister to deliver an arts statement.

PAUL FLETCHER: That is a very generous invitation to which I will give proper and appropriate consideration.

[Laughter]

STEVE LEWIS: Morris, can we get a date, please? Thank you very much. Our next question from Simon Grose.

QUESTION: Simon Grose from *Canberra IQ*. Going back to online security. A few years ago, then-Minister Dan Tehan, he was the junior minister responsible for that part of the portfolio. I remember him saying here that if you- that the problem then was mainly hacking into corporate and government systems and he said that the long arm of the law would get you if you did it. And I pointed out to him that there'd been a lot of hacking but no one had ever got busted, and these perpetrators are usually somewhere in Eastern Europe or Russia or China. You said in your speech that the eSafe- you sketched out an idea the eSafety Commissioner would have some powers to close down or put sanctions on overseas sources of bad online stuff. What are the mechanisms to do that, that you would foresee?

PAUL FLETCHER: So can I start by drawing a distinction between cyber safety which I have responsibility for and cyber security which is primarily the responsibility of my colleague Peter Dutton, and it's that area which in earlier times sat with Dan Tehan and then Angus Taylor. And so that goes to issues like hacking of networks, the physical infrastructure. Cyber safety goes to the content delivered over the network and how we regulate that. And the point I'm making is that at the moment, there are within our own legislation, specific limitations on what the eSafety Commissioner can do. When she engages with global internet companies, she does so saying - I speak on behalf of the Australian Government. I have responsibility for these areas. I'm backed by Australian law. But in a number of areas she's essentially seeking cooperation on a voluntary basis. And I might say she's had significant success in getting that cooperation on a voluntary basis, but nevertheless, there are also ways we can change the law to give her clearer, stronger powers, and this is very much based upon our practical day-to-day experience of how her office has operated over the last four years or so, both under Julie and under her predecessor, Alastair MacGibbon.

STEVE LEWIS: We have time for two more very short, sharp questions. The first one from Michael Keating.

QUESTION: Michael Keating from Keating Media. The rate of cyber fraud going on online has increased exponentially over the last few years against Australian businesses and governments. Working with your Five Eyes partners, what are you doing to reduce that risk, especially as you've mentioned a lot of the intrusions and other things originate overseas?

PAUL FLETCHER: Well, I might split that question into two. Again, the first point I make is that the cyber security policy sits with Minister Dutton. We are working or he's leading the work on a new cyber security strategy, and that work is well under way, and there's also a lot of resources devoted to supporting both business and government in responding to attacks. We also need to be protecting consumers against things like scams over the telecommunications network, and that's something I've been doing a lot of work on, getting the cooperation of the telecommunications industry, I'm pleased to say. So things like the Wangiri scam which is where you get a call from an overseas number, it rings once and then stops. The temptation is to call it back and you'll be calling back a premium-rate number and paying a lot of money for it. That's a well-known scam. Another scam involves the so-called overstamping of the number that a call appears to be coming from so that a number- a call that's actually coming from criminals overseas is overstamped with what looks like the number of the Tax Office. And so we're doing a lot of work to identify that and seek to stamp it out, working with the telecommunications industry, so we can better protect citizens against those kind of scams delivered over the telco network.

STEVE LEWIS: Our final question for the year, John Millard.

QUESTION: Thank you Steve and thank you, Minister for your address. John Millard, Freelance. You've quite rightly and to be applauded have reduced the time for take-down schemes. But just the same as the [indistinct] always [indistinct] ahead of the police, do you think we can ever [indistinct] particularly these international criminals who can strike in a very short time? If there is any more we can do, what do you think it should be?

PAUL FLETCHER: I think there's a couple of things we need to be doing. One of those things is probably the principal focus of this legislative framework is setting clearer expectations of lawful businesses, because the internet sector has come out of nowhere in less than 30 years, and it's grown so fast that there's a lot of pretty basic safety practices and requirements and expectations that are entrenched in much longer-established industries like the automotive sector, that are not yet sufficiently and adequately entrenched within

this sector. So certainly that is one focus, but the work of the eSafety Commissioner when it comes to illegal content, as I've mentioned, there's a large involvement of criminality in that, and the eSafety Commissioner certainly works with all of the other agencies of the Commonwealth such as the Australian Federal Police in terms of appropriate criminal enforcement action as well.

STEVE LEWIS: Let's conclude on that note.

[Applause]

Transcript produced for THE NATIONAL PRESS CLUB OF AUSTRALIA by ISENTIA.