COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON INFRASTRUCTURE AND COMMUNICATIONS

Section 313 of the Telecommunications Act 1997

WEDNESDAY, 4 MARCH 2015

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

INTERNET

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

To search the parliamentary database, go to:

http://parlinfo.aph.gov.au

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON INFRASTRUCTURE AND COMMUNICATIONS

Wednesday, 4 March 2015

Members in attendance: Mr Giles, Ms Marino, Mr Pitt, Mrs Prentice, Ms Price, Ms Rowland, Mr Thistlethwaite, Mr Van Manen, Mrs Wicks.

Terms of Reference for the Inquiry:

To inquire into and report on:

Government agency use of section 313 for the purpose of disrupting illegal online services.

The Committee is to consider:

(a) which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians

(b) what level of authority should such agencies have in order to make such a request

(c) the characteristics of illegal or potentially illegal online services which should be subject to such requests, and

(d) what are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:

a. Legislation

b. Regulations, or

c. Government policy.

WITNESSES

CLARKE, Dr Roger, Immediate Past Chair, Australian Privacy Foundation

LAWRENCE, Mr Jon, Executive Officer, Electronic Frontiers Australia Inc.

Committee met at 08:09

CHAIR (Mrs Prentice): I declare open the committee's public hearing for the inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services. I welcome Mr Jon Lawrence and Dr Roger Clarke to provide evidence today. Do you have any additional information about the capacity in which you appear?

Mr Lawrence: I am a non-executive director of the Internet Society of Australia, from whom I believe you are receiving testimony later this week in Sydney.

Dr Clarke: I am an e-business consultant, a visiting professor in computer science at ANU and a visiting professor in law at UNSW. I appear in my capacity as immediate past chair of the Australian Privacy Foundation. I need to declare that I am a life member of Electronic Frontiers Australia. I was a director of Electronic Frontiers Australia. I am also company secretary of the Internet Society of Australia, who are appearing before you on Friday. It is a close linkage in civil society.

CHAIR: I love all this energy. That is great. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the House. Would you like to start by making some opening statements?

Mr Lawrence: Thank you. I will make a brief opening statement and then pass over to Dr Clarke. Electronic Frontiers Australia, for those who are not aware of us, has been fighting for digital rights since 1994. We are a national membership based non-profit association. Turning to the subject of the inquiry, section 313 is a source of significant concern to us and our members. We believe its vague wording and broad scope have far-reaching potential for misuse and abuse. We believe it represents a potentially dangerous impediment to internet freedoms. We believe it is largely superfluous in achieving its stated outcomes in terms of law enforcement.

We believe it is largely, therefore, against the public interest and we recommend that it should be struck out in its entirety. Should the parliament choose not to do this, we then recommend that its scope and applicability need to be significantly restricted. Specifically, we would like to see the agencies able to utilise section 313 limited, as we have seen the government propose with the data retention legislation; we would like to see clear thresholds set for the type and seriousness of offences and civil penalties that can be used to trigger this section implemented; and we would like to see a form of independent authorisation for actions involving the disruption of online services such as the blocking of websites.

I have a couple of final points. As we have seen in the recent past, there are significant issues relating to technical competence with implementation of certain actions under this section. We believe it is probably appropriate that a centralised agency such as, for example, the ACMA should play a role in managing requests for any disruption of online services to ensure that these are done in the most appropriate technical manner. Clearly, there needs to be some meaningful reporting of actions taken under this section, and we would like to see some form of appeal provisions for people affected by it.

CHAIR: Thank you.

Dr Clarke: What I would like to do is go into somewhat more detail on some of the points that Jon has raised. The points I am intending to make reflect APF's submission from last August, which was prepared by one of the lawyers on our board. It also reflects the submissions of EFA, of ISOC-AU and of ACCAN in particular, because I have had the opportunity to see those.

CHAIR: Do you want to make a full statement or do you want to invite questions after each issue you raise?

Dr Clarke: I suspect they are cumulative so I suspect it might be better—though I am entirely in your hands.

CHAIR: That is fine. Go for it.

Dr Clarke: Thank you. We have a primary submission, in effect, and a secondary submission. The primary submission is about section 313 as a whole. Our statement is that it is not clear that the section fulfils any justifiable need that is not addressed by other much better defined and controlled mechanisms. It is completely unacceptable in a democracy for the parliament to grant the executive powers that are convenient to the executive but that drive a truck through the careful balances that have been achieved over centuries of development of the law.

Of course it is possible that section 313 does fill one or more gaps—if so, it is up to the affected agencies to publicly demonstrate that this is the case and to sustain their argument in the face of counterarguments. If a need

is demonstrated, then the appropriate course of action is for the executive to bring forward appropriate amendments to existing mechanisms. Under no circumstances should parliament grant carte blanche to agencies as section 313 does. So our submission on this point is that the committee should recommend that section 313 be rescinded and that the executive be requested to bring forward arguments for specific and suitably constrained and controlled powers that address any gap that may arise from its rescission.

Reflecting Realpolitik, we have a secondary submission, which is: in the event that the committee does not recommend that section 313 be rescinded, the provisions require wholesale reworking in order to overcome a long list of serious problems. The following comments summarise the key things that are wrong with it and the necessary characteristics of a replacement for it.

The first small bracket relates to the scope of the powers. The first one that is worth dealing with is 'purposes'. The categories of 'purpose' are listed in section 313(3)(c)-(e) and all five of the purposes defined are seriously problematical. The first is at (c), 'enforcing the criminal law'; that encompasses the whole vast array of laws rather than limiting the scope to serious criminal laws. The second is 'enforcing laws imposing pecuniary penalties', also at (c); that is a desperately broad category and is entirely inappropriate to such an extreme power as this.

Similarly, (d), 'protecting the public revenue', is an entirely inappropriate category. It lacks clear meaning and it includes a host of very minor matters and yet it is subject to extreme and inadequately controlled powers. The fourth of the purposes in the act is (ca), 'assisting the enforcement of the criminal laws enforced in a foreign country'; that encompasses acts that are not a crime in Australia and even acts whose prohibition would be repugnant in Australia. The fifth and last is (e), 'safeguarding national security'; the term 'national security' is completely lacking in a reliable and reasonable definition; it is subject to continual invocation by law enforcement agencies whenever they seek uncontrolled powers.

Our submission on that aspect of scope is that the committee should recommend that the purpose of any such law be expressly limited to serious criminal laws, defined—we suggest—as those that have penalties of five or more years in jail.

The second of the scope issues is in relation to the organisations that are empowered by section 313. The relevant expression there in section 3131(3) is: 'officers and authorities of the Commonwealth and of the States and Territories'—without any apparent clarification or qualification. This represents hundreds of thousands of individuals, in thousands of agencies—which is quite extraordinary. We submit that the committee should recommend that a list of agencies be defined, and that the list include only those agencies that enforce serious criminal laws, as discussed above.

The third scope aspect is organisations that are subject to section 313 requests. Under section 313(1) and (2) a moderate number of large carriers, as defined in the TA, at least 200 to 300 carriage service providers, in common parlance ISPs, and some hundreds of carriage services intermediaries, as unclearly defined in the act—which we presume is intended to capture resellers and agents and internet-cafe-style providers—are all subject to those requests. That is something like 500 to 1,000 organisations; they are mostly small companies; they have neither the competence nor the resources to evaluate the reasonableness of requests that are addressed to them, and, accordingly, those requests are effectively demands.

We submit that the committee should recommend that the executive provide an analysis of the categories of organisation on which requests are to be made and an assessment of alternative approaches to the definitions of those categories.

The fourth and last scope aspect is: it is entirely unclear to the public—and indeed to those 500 to 1,000 companies—what they can be requested to do. We submit that the committee should recommend that the actions that can be imposed on organisations be expressly stated and clearly defined.

The second small bracket is concerned with the exercise of the power. The fifth point that we make is that the grounds are unclear. There is no definition of the basis on which a request is justifiable—things such as the degree of gravity of a matter, the extent to which reasonable grounds for suspicion exist or the extent to which compliance with a request may assist the agency. None of those is clear, so we submit that the committee should recommend that the executive propose the specific grounds that can be used to justify exercise of the power. The second aspect of the exercise of power is thresholds. There appears to be no definition of the threshold tests that need to be applied in order to determine whether a proposed exercise of the power is justified. In effect, here we are discussing the proportionality test. So we submit that the committee should recommend that the executive propose in respect of each ground the specific threshold conditions that must be satisfied and that the thresholds apply standard regulatory principles, particularly those of justification and of proportionality.

The last bracket has to do with safeguards. Transparency is the first. There is no meaningful information published about agencies' invocation of section 313, what they use it for, how often or what value it delivers. Specifically, in respect of blocks arising from the Interpol child abuse list, the committee's website states, 'When a user seeks to access one of these sites they are provided a block page that provides certain information, including reasons for the block and contact details for the dispute'—which we are very supportive of. Unfortunately, it is far from clear whether agencies in Australia apply such techniques, so we submit that the committee should recommend that in respect of every exercise of the power an appropriate form of disclosure must be made. For example, in the case of the blocking of a web page, which is only one of the possible actions, an agency must be subject to a legal obligation to communicate the facts and the nature of the dispute process.

Point 8 is about independent evaluation. There currently appears to be no process whereby any independent party tests whether the basis on which an officer proposes to issue a request reaches whatever threshold tests are applicable. In particular, the process does not include judicial warrants. Such an absence of controls is a gross breach of regulatory norms. In all circumstances it is essential that the exercise of a power be subject to a precondition that a competent, resourced and independent party receive and consider the agency's justification, deny unreasonable proposals and authorise reasonable ones. So, we submit that the committee should recommend that the scheme involve an independent party that has the responsibility and the authority to test whether the basis on which a requesting agency proposes exercise of the power satisfies the defined criteria and reaches the applicable thresholds, failing which the agency cannot use the power.

Point 9 is about technical competence. Despite the almost complete absence of transparency, several instances of technical incompetence have come to light, which have caused considerable collateral damage. I am sure I do not need to rehearse those before this committee. It is unacceptable for the parliament to countenance amateurism in the application of such broad powers, so we submit that the committee should recommend that the independent body that we have proposed must have sufficient technical, as well as legal, competence.

The 10th and last point is to do with contestability and sanctions. Beyond just transparency, demands by agencies must be able to be objected to, both by the organisation that is subject to the demand and by parties who are or who would be affected by the action. So, we recommend that the committee should recommend that the executive propose specific mechanisms whereby the exercise of the power can be contested by any affected party. Further, we believe that the committee should recommend that wrongful or unjustifiably harmful exercise of the power should be subject to sanctions.

We believe that the current section 313 is an embarrassment to the original legislative drafters, to the Australian public and to the previous parliament which passed it, unaware of what its actual meaning was. We were not aware of its meaning, either; otherwise, we would have objected like this before. We believe that the committee needs to recommend its rescission or, alternatively, to drastically overhaul its provisions. I have a few words here which relate what I have been saying to the terms of reference of the committee as a cross-check to ensure that I am not trying to push the committee outside its brief, and I have a copy to provide to the secretary.

CHAIR: Thank you very much. That is my first question: have you ever raised any objections before?

Dr Clarke: I have not researched the many submissions that the Privacy Foundation has made over the last 15 years or more in relation to the Telecommunications Act and the Telecommunications (Interception and Access) Act. There is a large number of them, they are quite deep, and I did not write any of them. I cannot recall section 313 ever being perceived as an issue, and I have been involved since 1987 with the foundation.

CHAIR: Until the ASIC activity?

Dr Clarke: Until ASIC came to light because of an error, yes.

CHAIR: That has gone under the radar until then hasn't it?

Dr Clarke: We believe so.

Mr Lawrence: If you will indulge me, I think it is worth pointing out that uncovering the activities of ASIC actually involved a large group of people over many weeks doing some very forensic analysis of what was going on. It was very unclear for some time exactly what was happening. Clearly, there was collateral damage, as you are well aware, and that alerted certain people that something weird was happening—that certain websites were just disappearing as it were. It is important to realise that that the whole issue, which of course gave rise to this entire inquiry, encapsulates in it many of the issues that we are dealing with here today.

Mr THISTLETHWAITE: Mr Lawrence, you said that you believed that the operation of the power should be limited to certain agencies. Can you elaborate on that? Have you got an idea of which agencies they should be?

Mr Lawrence: Yes, so we would assert that, as has been foreshadowed in the data retention legislation, that should be restricted to those agencies which are able to, for example, request surveillance warrants, so the police, the ICAC, the Crime Commission and so forth. We accept that there may be circumstances where civil agencies such as ASIC and the ACCC—or ASIC at least—may have a role here. As we have said, there needs to be clear thresholds around what sort of actions they can take and on what justification.

Mr THISTLETHWAITE: Dr Clarke, are you aware of similar systems that operate in other jurisdictions throughout the world? And are there jurisdictions that you think get the balance right that we could have a look at?

Dr Clarke: No. My background is electronic business. I trip into the law far too frequently but not sufficiently deeply. I am not aware. My strong impression is that Australia is not the only country that has gone too far since 2001. Quite a few of the excesses in Europe, in particular, are being hauled back by the courts as finally test cases reach the courts. I am sure that there are plenty of unfree countries around the world that have got provisions of the nature that is in section 313. In terms of a democratically appropriate process; no, I am not aware of a country that has got that kind of balance right.

Bear in mind that our stand point is that we have real doubts about whether there is anything that, considered in isolation, we would as a nation consider ought to be done. We are not clear that there is anything that cannot be done with other laws. If there are things that cannot be done that should be done then we would be the first people at the table supporting appropriate processes. We do not believe that anything of this shape should ever be permitted because it breaches not just one or two but a whole sheaf of norms.

Mr THISTLETHWAITE: Do you want to add anything, Mr Lawrence?

Mr Lawrence: I was going to say that I would be happy to reach out to our colleagues in other countries to get some feedback from them as to what the situation is there and report back if there is any useful information. If that would be helpful?

CHAIR: Yes, please. Thank you very much.

Mr THISTLETHWAITE: One final question, Dr Clarke. You proposed warrants. Which jurisdictions should the warrants come from?

Dr Clarke: I very carefully phrased the wording to avoid formally recommending warrants. Our normal standpoint is judicial warrants is the appropriate mechanism. We certainly have accepted in a range of circumstances that a suitably designed process that does not include a judicial officer is entirely appropriate. Clearly, I have in mind ACMA as the kind of agency that you would have in mind. The technical competence question being one of them. If they have not quite got sufficient technical competence in that branch at the time then I am sure they will be pleased to get it. I suspect in these circumstances, because of the technical content, it may actually be an occasion when a suitably designed process would not include a judicial officer.

Mr THISTLETHWAITE: Independent being the key concept.

Dr Clarke: Independent is the key word that we are trying to underline.

CHAIR: And you agree that ACMA would be classified as independent?

Dr Clarke: The independence then depends upon the manner of the drafting of the legislation. In the event that the function is independent, then the agency is as independent as agencies typically are within government. Although we do not believe ACMA is an absolutely wonderful champion of freedom, we believe ACMA does, by and large, the job that it is asked to do by the parliament.

Mr Lawrence: And it does sit outside the Attorney-General's portfolio.

Dr Clarke: That certainly helps.

Mr Lawrence: As opposed to, for example, putting this within the Attorney-General's portfolio. I think that does give it a degree of potentially genuine independence to the extent that you can get that within government.

Dr Clarke: Both the question of independence in reality and the appearance and credibility of independence.

CHAIR: Perception.

Mr PITT: Your submission says:

… the technologically savvy evade clumsy laws administered by amateurs …

Firstly, what sort of skillset would you expect enforcement agents to have? And, secondly, could you give those of us with a non-technological background a rough explanation of how VPN and Tor are used to evade all the things we are trying to do.

Mr Lawrence: In terms of evading these sorts of things, our general principle, particularly in relation to blocking websites, is that—and I think this became pretty clear during the debate about the Rudd government's proposals for a broad, mandatory internet filter—these things are fairly trivial to circumvent—ask any 14-year-old. The reality is that even what, for example, ASIC was doing is fairly easy to get around. The reality is—and Dr Clarke touched on this—there are actually many hundreds of different providers in this country, and getting full coverage of that in terms of actually preventing anyone in the country to access a certain site offshore is next to impossible.

In terms of VPNs specifically, this is one easy way around it. A VPN, or virtual private network—and pretty much everything I am saying here, by the way, is also applicable to the data retention context—essentially allows you to create what in the parlance is called a secure tunnel through the internet. It creates essentially a dedicated pipe through which you can send secure communications. It is routinely used in the corporate and government contexts for absolutely legitimate purposes in terms of securing external access to networks and so forth. It is also, as the committee would probably be aware, useful and often used by consumers in terms of getting around geographic blocking—Netflix being the obvious example. A VPN allows you to appear to be coming from a location where you are not actually at, so it does obfuscate your location in that sense. It obfuscates potentially your source internet protocol address as well—your IP address.

Tor is essentially an anonymisation tool that would tend to be used in conjunction with a VPN. What Tor does is essentially bounce your requests and your traffic around a number of random sites across the internet to essentially anonymise who you are and not just where you are coming from. It is, like any technology, value-neutral. It is a very powerful tool for people in non-democratic countries to express dissent and to communicate with others. It is also of course, as the committee would probably be well aware, used by criminals to do all sorts of nasty things. That is the context here. Those tools do not necessarily require any particularly significant technical skill to use. But they do provide the ability for people that wish to get around the sorts of actions that might be taken under section 313 or, as I mentioned, under the data retention legislation, to essentially circumvent those actions pretty easily.

Mr PITT: Is there a way to stop that?

Mr Lawrence: Well, you could ban the use of VPNs, which was suggested by the CEO of one of the cable companies in Canada this week. It would be a pretty extreme—

CHAIR: Courageous decision.

Mr Lawrence: Yes, a courageous decision that would essentially bring a lot of corporate communications to a grinding halt. But, as I say, the issue with technologies is that they are essentially value neutral. They are used for good and bad. The problem when you try to address a lot of these things on a technological basis is that you end up throwing the baby out with the bath water, and potentially doing more harm than good. By trying to address one issue you are actually losing the benefits as well, which, in our long experience, tends to massively outweigh the downsides.

Mr PITT: Is there an alternate to VPN?

Mr Lawrence: An alternate?

Mr PITT: Is there another way to do the same thing?

Dr Clarke: VPN, in a number of respects, is a set of principles, and it is capable of many different kinds of implementation. There are many approaches.

Mr Lawrence: Yes. You can use proxy servers and so forth. I think I will stop there, because we are reaching the limits of my technical competence.

Dr Clarke: If I can just add a couple of points to what Jon was saying: as regards the technical competence, the AFP has a high-tech crime centre. They cycle people through on training schemes and the private sector then takes advantage of them a few years later. They just cannot hang on for very long to the highly competent people that they generate. State police forces have an even bigger challenge in that regard.

It does require a moderate amount of competence. I have been struck by it when I have given expert evidence before courts in relation to some of these sorts of matters. The care with which you have to build up an explanation of simple concepts in order to convey even to the prosecution, let alone to the judge, what the real issues are on things like child pornography accusations and so forth and, indeed, on internet defamation issues is extraordinary. This is because the general lay population only has an understanding of IT in use because that is what they have in the hands and their minds reflect what their hands do and what they see on screens. So it is quite a big jump to move to the levels of technical competence needed to deal with this. So we use nasty strong

words like 'incompetence' of ASIC. ASIC was a surprise, because they do have a solid IT section. They did not apply their internal IT expertise to the job at hand. They needed to get out there and employ the right kinds of people.

A couple of further aspects, just following on to Jon's points. One of the mistakes that is often made with the example in focus, which is, of course, the blocking of highly undesirable websites, is that people tend to assume that the web is the internet. The web is one protocol out of 100 that runs over the top of internet. It is only one element of a thin layer at the top. It happens to be responsible for a significant volume of what goes on, but no more than, at a rough guess, 30 or 40 per cent at the moment. I would have to go back and check the statistics, but it is not that huge. You have to actually get on top of a whole range of other protocols and services in order to be able to form reliable sentences. So, if you are trying to attack child pornography being hidden, the web is probably the least likely place to go looking at the moment. That is not understood by enough people, unfortunately, and it is sometimes hard to convey the argument.

The last quick point I would make is that Malcolm Turnbull did not invent the internet, despite some rumours, but he does know how to achieve the sorts of things that we are discussing. He is not the only person in parliament who understands that. I suspect Kate Lundy might as well, and probably one or two others—but not many people. But it is definitely knowable and understandable partly by being on the right services and partly by having a clue about what those services do. The critical point is not Malcolm Turnbull.

The critical point is that anybody who has a real reason to dig in and find out can do so. The first people who are going to be doing that are organised crime. The second people are going to be semi-organised crime. Disorganised crime will probably never get there. But the idea that we can tackle the most serious levels of crime in Australia on the basis that we ban one or more of these things or that we block the most obvious place where we find some content is, I am afraid, amateurish. It is not the way that the technology works. So the competence question is a big heading.

Mr PITT: Just to confirm, the training that is provided through the AFP and their crime centre is more than adequate, obviously, if they are being poached by the private sector?

Dr Clarke: At any given time there are good people in there, though not enough of them, and obviously they have to focus on their particular priorities. I was using them as an example of how it takes time to train them up, and then they lose them because they are valuable people. Of course they can be hired back in—I am a consultant, after all. They can be hired back in from wherever they went to.

Ms MARINO: Can I just thank you. I do a lot of cybersafety presentations into schools and into the community, and you talk about how this is not the answer. Well, what is?

Mr Lawrence: Education.

Dr Clarke: Education at various levels.

Ms MARINO: Hey, come on. When we as a government talk about the technology and the capabilities and you with your experience and knowledge talk about the various parts of the internet, what is the answer? Given our commitment to dealing with the huge challenges faced online, particularly by young people, and what they are exposed to, I want to know from you what the potential answers are across all of the availabilities on the internet.

Dr Clarke: The first thing that has to be confronted is that there is no ultimate safety and no absolute security. That is the argument that is always put, because there will always be countermeasures that will breach that security. So we have to face the fact that technological solutions are part of the exercise but they are never going to be the whole answer. There never will be a whole answer. There will be children on occasions who find things that disturb them—we will never be able to defeat that. We can reduce it and we can provide protective mechanisms to filter it—and I am sorry; you may shake your head all you like—but the simple fact from a technological perspective is that there will always be ways in which people who are so minded will be able to beat safeguards that have been built up, which is the reason why we immediately turned to education, not only of children but of parents and of society as a whole—and, of course, going back to the question of technical capabilities in the various agencies, including in schools. The IT people within schools need to have access to the kinds of training they need to build filters as effectively as they can and to have response mechanisms in place. So there is a big educational layer, together with a bunch of technological things.

I do not want to sound as if it is impossible to ever block anything—that would obviously be a hopeless overstatement. Quite a lot of blocking is effective within schools, for example. Unfortunately, there is overblocking, because you have to overblock in order to achieve a reasonable degree of confidence that you are

blocking the right things, but there is effectiveness subject to that measure. So: education, education, education, and then technological insight and application in order to provide assistance to people.

Ms MARINO: Dr Clarke, I shake my head because I work with the people. It concerns me most greatly—not what you are saying but the risk that they are exposed to and our capacity to assist in managing that. That is why I shake my head.

Dr Clarke: I see. I agree that it is problematic, but it is also something that I believe is capable of being overdramatised. As a parent and grandparent, I believe that it is important that we bring our children up understanding that there is a big, wide, nasty physical world out there so that they are aware of how to protect themselves; and that there is a big, nasty parallel electronic world out there which is also capable of doing them damage unless they are well educated and can cope with these things. If that is what you were shaking your head at then, yes, I agree with you. It is a head-shaking area, but it is not a desperate situation. We have to do what we can with education and technological features.

Mr Lawrence: Can I add to that that I have had a fair bit of exposure to a number of the school-based cybersafety programs that are currently around, particularly the Alannah and Madeline Foundation's eSmart program—or eSmart framework, as they call it. I have noticed in my time in this role, and talking to various people looking at those sorts of things and so forth, that in many ways young people coming through the education system now are better prepared to deal with some of the dangers and so forth that are out there in the digital world than perhaps people who are now in their late 20s and early 30s are, because those programs were not as well developed within the school space when they were there. I agree that there are genuine threats out there. I would concur with Dr Clarke in the sense that this is a space where it can be quite difficult to have objective discussions, because it is obviously very emotionally loaded.

We do lack empirical evidence. As an example, I think it would be useful to look at the number of times people from Australia are trying to access the sites that are blocked on the Interpol list. I certainly have no concept—the AFP may have some stats around this—of whether this is happening once a week or fifty times a day. I think it is important to remember that this really, at base, is not a technological issue. There are, as Dr Clarke has said, some technological mechanisms that can be used to alleviate it. As long as those are not top-down mandatory processes they can be really pretty effective.

As I said, due to the work of a lot of very committed and talented people, in some ways young people today are probably slightly better prepared than the generation above them. That is just to say that perhaps we are heading in the right direction. We will never achieve a total solution to this issue but I think there are positive elements to the story.

Dr Clarke: Can I just add one thing to that, which is some evidence that I got hold of a few days ago. I was in front of an Australian Press Council roundtable last week and a lady who is the chief executive of Ipsos—a social research organisation in Sydney—made the point, independently of any discussion that I had raised, that young people's understanding and perceptions of privacy is clearly on the rise. It shows up in their focus groups in particular; they have not done survey studies of this. I have been arguing the case for five years that the current generation of young people will be far more privacy sensitised in 30 years' time than your cohort or my cohort, because they have gone through, and seen others go through, much more in the way of self-exposure and harm arising from the self-exposure.

That was the first time that I heard it from an Australian social science researcher, I had just made it up as systemic reasoning. She has actually got some numbers. That, to me, was a very positive development because once they have got that perception they may think, 'Hey, perhaps I should be careful.' Then they would be motivated to start looking at, 'Hang on a tick, I did hear there were some techniques here; how do I do that?' I think there is real progress being made—amongst young people more so than the 20- to 30-year-olds.

Ms ROWLAND: Your first best outcome is the serious reworking/repeal of these provisions. At the time when the Australian Law Reform Commission did its detailed privacy review a few years ago, are you aware of what recommendations came up on part 13 of the Telecommunications Act and related provisions, and whether there is any guidance in there that might assist the committee in this inquiry?

Dr Clarke: I would be quite happy to take that as a question on notice because I did not think to look at that 2006 to 2008 study and report before I came in. They certainly looked at aspects of TA and T(IA)A but I cannot recall whether they directly addressed 313—

Mr Lawrence: It is well before my time.

Dr Clarke: I am on the move for the next few days but I will look that up or ask some of my colleagues to look that up.

Ms ROWLAND: That would be really useful, thank you.

CHAIR: Gentleman, you indicate that wrongful use of the process should be subject to sanctions. What would you envisage those sanctions to look like?

Dr Clarke: That biggest issue which is addressed in the AFP submission—I am casting my mind back—has to do with adjustment back to the state that existed before and compensation in the event of harm. Clearly, because there are many different actions that could be taken we must not focus solely on inappropriate blockage of websites; there are other actions. Those sorts of things are the first line.

The second line then is that, to the extent that organisations are cavalier in their behaviours and cause problems continually, there should be a ramping-up of sanctions. We do not think that people should be going to jail because they wrongly issued a request under a future section 313; we are saying there should be processes that haul them back in and get them under control.

Mr Lawrence: I think it is pretty clear that an action to disrupt a service could, in certain circumstances, drive a business into bankruptcy. And that needs, obviously, to be catered for if it is done inappropriately.

CHAIR: Just to clear, you were talking before about ASIC. Are you saying that if it was not for people like your members identifying what they have done, they would not have come out and confessed to it?

Mr Lawrence: Essentially, yes. I have heard testimony from ASIC where they have said, 'Oh, we have done press releases about what we'd done.' That may be true, but I have certainly not been able to ever find them and I certainly went looking for them at the time. Just dealing with the particular issue that they were trying to address, which of course was sort of consumer fraud, in many ways I would have thought that the more publicity they generated about that the better. I can see there are certain circumstances, let us say, where there may be some particularly egregious jihadi website where perhaps promoting its existence is not ideal, but I think, particularly in those sort of consumer issues, the more publicity the better. As I say, I have heard claims that they had publicised what they were doing, but I have not ever been able to find that information.

CHAIR: Until people like your members—

Mr Lawrence: Yes, and it literally did take some weeks. I must admit I was one of the most sceptical at the start—I said, 'Oh, this is just some incompetent person at an ISP doing something wrong'—but there were others that kept at it and determined that this was actually something that was happening. There were certain conversations with certain administrators at certain ISPs, and of course part of what happened was that ASIC had only sent their request to a small number of ISPs anyway, so some websites were working through one ISP and they were not through another. It was really quite an involved, technical, forensic operation involving a number of people to get to the point where it became clear that this was an act of government.

Dr Clarke: One of the points that were made by the particular educational company that was at the centre of this was that, had they not had sufficient technical expertise to be able to come up with a sensible question and address it to some people who had a clue, it would still not have been understood and solved. There were 2,000 organisations, I understand—I did not study this, but it was reported that there were 2,000 organisation affected.

Mr Lawrence: In the first one; there were 250,000 in the later one.

Dr Clarke: Yes. That is quite significant, because it came to Jon's attention and my attention on the day that it occurred—through separate channels—and we both went searching. With reasonable technological competence in these areas, I could get through the first few rounds and establish a couple of things that it was not, but nailing it down to what it was required a lot more technical competence than I could bring to the table. But fortunately, from there, once you have an insoluble problem you turn to your own reference points, and the problem rippled out until a couple of people said, 'Hang on a minute,' and actually did the appropriate studies. That is quite significant, because it means that it was so buried. What ASIC had previously very probably issued media releases on was the fact that they had warned against scamming websites, which obviously we pay them to do and we are very thankful to them for doing it. Their motivation was entirely appropriate in line with their remit; it was their action that did not work.

CHAIR: The adjective 'incompetent' popped in there.

Mr Lawrence: Yes. The level of knowledge that would be required to avoid the mistakes that ASIC made is the sort of thing that one would learn in the first five minutes of a course about the structure of the internet. I mean, we are talking absolutely fundamental, basic information. I had another point, but it has gone.

CHAIR: Are there any further comments at this point? Mr Lawrence and Dr Clarke, thank you for attending the public hearing today. We appreciate you taking some requests and also offering further information on a few issues. The secretariat will liaise with you on that, and we look forward to receiving those. Thank you very much.

We appreciate you being here today. We will send you a draft transcript of the proceedings so requests can be made to correct any errors in transcription.

Resolved that these proceedings be published.

Committee adjourned at 08:54