CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19/0006

DAY 9 - FRIDAY 22 NOVEMBER 2019
(DURATION: 47MINS)

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KIMBERLEY SAUNDERS
W Witness – GERALDINE MACKENZIE
LR Legal Representative – N/A

HRO All stand. This hearing has resumed.

PO Good morning.

CA Good morning, Chair. I call Professor Geraldine MACKENZIE.

PO Good morning, Professor.

W Good morning.

PO Would you prefer to take an oath or affirmation?

W Oath is fine.

PO Thank you.

HRO Can you stand for me.

W Sure.

HRO Take the Bible and repeat after me. The evidence which I shall give.

W The evidence which I shall give.

HRO In these proceedings.

W In these proceedings.

HRO Shall be the truth.

W Shall be the truth

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

HRO So help me God.

W So help me God.

HRO Thank you.

W Thank you.

CA Good morning, Professor MACKENZIE.

W Good morning.

CA You were provided a notice to attend this morning?

W I was.

CA Yes. I'll just show you a copy of the notice.

W That is the notice I was given.

CA I tender that document.

PO Exhibit 157.

ADMITTED AND MARKED EXHIBIT 157

CA Professor MACKENZIE, you are the Vice-Chancellor at the University of Southern Queensland and have held that position since 2017?

W That's correct.

CA Your areas of expertise are criminal law and sentencing?

W That's correct.

CA Prior to your current appointment you were the Deputy Vice-Chancellor in Research at the Southern Cross University?

W That's correct.

CA And you returned to the University of Southern Queensland having been the foundation head of the university School of Law in 2007 and 2008?

W That's right.

CA And you then took up senior executive positions at Bond University?

W Correct.

CA Where you were the Pro-Vice-Chancellor?

W That's correct. I held two Pro-Vice-Chancellor positions. That's right.

CA Yes. The first one being in Business and Community Engagement.

W Mmm hmm.

CA And the second in research and you were also the Executive Dean of the Faculty of Law.

W That's correct.

CA And then prior to joining the University of Southern Queensland in 2007 you held various senior roles at the Queensland University of Technology, having lectured there in criminal law for 19 years.

W That's correct.

CA And you were on the Queensland University of Technology Council for 9 years?

W That's correct.

CA You are an expert in criminal law with a PhD in sentencing law from the University of New South Wales.

W That's correct.

CA Your research interests are law and public policy?

W Correct.

CA Over your 35-year career in law, having been admitted as a barrister-in-law in 1985, you have published widely in the area of criminal law and also in sentencing.

W That's correct.

CA Having published in many journal articles and also conference papers and in particular the following four following publications: the Principles of Sentencing; How Judges Sentence; the Queensland Sentencing Manual; and the Summary Offences Law and Practice Queensland.

W That's correct.

CA Professor, could you please detail the legislative history with respect to section 408E of the Criminal Code?

W Sure. So section 408E commenced as 408D in 1997. It was introduced by the Criminal Law Amendment Act as amendment to the Criminal Code as part of a large suite of amendments made at that time. The principal purpose of that legislation was with regard to the introduction of viruses into computer systems and computer hacking. That particular provision was then amended by

renumbering only in 2007 by the Criminal Code and Civil Liability Amendment Act and there were no other changes made to it other than renumbering to 408E.

CA And, in your view, was the aim, with respect to computer hacking, pertained to pulling information – to go into the computer rather than pulling information out?

W So at the time that it was introduced which was fairly early on in the days comparatively of using computers, it was about the concept of going into a computer system and introducing harm by viruses or by hacking, again, the introduction of harm. So it was more going into the computer system. It had three different offences in it. The offence simpliciter, which was about using the restricted computer without the consent of the computer's controller. So it really envisaged going into the computer and doing something that somebody wasn't supposed to do and then causing or intending to cause detriment, or damage or gain or intends to gain a benefit was one of the aggravating factors.

And another one was also about the benefit aspects and we can go into that later, if you wish. But it was for that purpose that it was introduced. I don't think at the time any of us considered the situation that's currently the purpose apparently currently the subject of the reference.

CA And I'll just show you section 408E for completeness. That's Exhibit 11. And there on the screen there is a definition of benefit: includes a benefit obtained or delivered to any person. And then I'll just show you section 108, which further defines benefit – Exhibit 108, sorry, section 1, which further defines benefit.

W So that's section 1 of the Criminal Code?

CA Yes. So that's on the screen now. It should be on the screen shortly. Yes? Is that on your screen?

W I've got it now and I do have a copy of it as well. Thanks.

CA So there would you just like to talk to the definition of benefit there for how wide it is?

W Sure. So benefit comes in because in the section 408E(3) it is one of the aggravating factors. If a person causes a detriment or damage or obtains a benefit for any person to the value of more than $5,000 or intends to commit an indictable offence the person who commits a crime is liable to imprisonment for 10 years. So it is the most serious form of computer hacking and misuse in 408E.

Benefit is defined in the provision itself as including a benefit obtained by or delivered to any person. And also there's an additional definition in section 1 of the Criminal Code. And you don't have the right page up for me there but I have got it in front of me. You've got the previous page on the screen there.

No, I have got it at the bottom. Sorry, it is there. Includes property, advantage, service, entertainment, the use of or access to property or facilities and anything of benefit to a person whether or not it has had an inherent or tangible value, purpose or attribute. It is useful having that bigger definition in the Criminal Code that applies more generally but it has been difficult in some of the cases fitting benefit in there.

CA We'll just go to one of them. But just going to 408E(2) includes the benefit as the aggravating factor as well, just to cover off on that?

W Correct. You're absolutely right.

CA So I'll just show you The Queen v Neiland which was a decision on 26th August 2019. And that was with respect to prosecution under section 92A of the Criminal Code but the same issue of the definition of benefit arose there. I tender that document.

PO Exhibit 158.

ADMITTED AND MARKED EXHIBIT 158

CA So that was in the District Court at Brisbane. Would you just like to speak to the issue there for why it was considered benefit wasn't encompassing the action, the offence at that time, which was accessing the computer without the consent of the controller; namely the QPRIME Queensland Police Service computer information system for an unrelated work purpose?

W Sorry, did you want me to speak to that?

CA Yes. So it was discovered that – well, it was found that on page 3, line 25 that the conviction for drink driving is made in open court. So this is the situation where the police officer was accessing QPRIME for an unrelated work purpose to look up a drink driving offence. And that it was considered not a benefit because the information is publicly available at the time of the hearing and on request through the open courts?

W I think there are a couple of problems that this case brings up and some of the other things that I've read as well that where the information is publicly available, and that has become a problem, that is an issue for the provision, because I think it has to be somewhere explicitly stated because I think that should be included within the provision. And also the fact that knowledge itself should amount to a benefit. That there doesn't have to be any pecuniary benefit, for example, that the knowledge itself is the critical thing here.

CA And I'll just show you section 10.1 of the Police Service Administration Act 1990 Queensland. We've got seven subject agencies that are subject to the scrutiny under Operation Impala, and the police are one of them, and they've all

got their respective Acts with their prohibitions on disclosure. And this is the police one. I'll just show it to you because of 10.1(1)(b). I tender that document.

PO Exhibit 159.

ADMITTED AND MARKED EXHIBIT 159

CA Because here it captures all of the information that's on their system by the wording "has come to the knowledge of the officer or staff member or person because of employment in the service." So that's more encompassing than we currently have under section 408E.

And then there has been a – the number of prosecutions has been low. And, in part, throughout the public hearings, we've heard from the agencies and there appears to be some confusion and difficulties with the definition of benefit. And the penalties handed down, especially when having regard to the penalties that can occur in a disciplinary environment, are relatively low. I'll just show you a table of a sample of the matters that have come before the court to date.

W Thank you. It's certainly been my opinion through reviewing some of the these cases, and looking at the legislation, that section 408E is difficult to use in these situations and has a number of problems, benefit being one, but a number of others as well.

CA So with the penalties being handed down – given that the range of maximum sentence is from two years up to 10 years – we have Banks. And I tender that document.

PO Exhibit 160.

ADMITTED AND MARKED EXHIBIT 160.

CA We have BANKS which included 23 counts ranging over two years under section 408E(2) for benefit, the benefit being knowledge on that occasion. That was access only. And there was a $4,000 fine. No conviction recorded.

And then BETTS. There was access and disclosure, 51 counts under 408E(2). There was a slightly larger fine of $8,000. Again no conviction recorded.

And then BINNEY was prosecuted both under section 408E for the access and then section 10.1 for the disclosure of the Police Service Administration Act and had one combined penalty there of $1,200 for access and disclosure. Conviction recorded.

And then McANANY, and again another low fine. And PRYCZEK.

So we do have one where there was a suspended sentence of two months for a period of 18 months, Neil PUNCHARD. That sentence was handed down

relating to access and disclosure and that was on 14th October this year, but that is subject to appeal.

So could you please, Professor MACKENZIE, discuss some of the issues with respect to the purpose of sentencing and how it works with respect to this provision?

W Sure. So section 9(1) of the Penalties and Sentences Act-

CA -I'll just put that up on the screen-

W Sure.

CA -if that's okay.

W Thank you.

CA I tender that document.

PO Exhibit 161.

ADMITTED AND MARKED EXHIBIT 161

CA Yes, please continue, Professor.

W So in terms of the punishment that's been handed out at the moment there are a number of different possible purposes for sentencing. And the Penalties and Sentences Act sets these out in section 9(1). In my view one of the most critical ones is to punish the offender to an extent or in a way that is just in all of the circumstances. And that's subsection (a), and that's about punishing in relation to the severity of the crime. That also brings in that element of public expectations and looks at all of the circumstances of the case.

Subsection (b) is about rehabilitation which may not be as applicable in these cases; (c) is important to deter the offender or other persons from committing the same or a similar offence; (d) is about the community denouncing that type of conduct. Again, really important here. (e) is about protecting the Queensland community, and arguably that's important here as well, by punishing for these types of offences. The courts are saying both with denunciation and protection that these offences should not be occurring to protect the Queensland community or a combination of two or more.

Depending on the severity of the matter and the fact that imprisonment hasn't yet been handed down, except a suspended sentence, this is under appeal, it does tend to send a message of lesser importance of these types of cases.

The consequences of unlawful access and disclosure can be devastating, depending what happens, and therefore it's important, not just in sentencing, but

relevant to this reference, to have the right provision that sends a very clear message that this is completely inappropriate behaviour and will be punished accordingly given the maximum penalties.

So the most critical thing here is to have the right provision and the right sentence maximum there available. The most critical thing in these cases is always that the offender needs to think that they're going to be caught. And that is probably one of the issues here that people take it too lightly. But there also has to be a very clear message by that provision. And that's part of the problem in 408E because it doesn't have direct application in these cases, it has been retrofitted, if you like, but has been able to be successful in some cases.

CA So with "important to show that it's taken seriously", if Parliament were to enact, say, another provision – and we'll talk about that shortly – with a larger minimum – or maximum sentence then would that show that Parliament is taking the offence seriously.

W So the most important way of being able to do that is to set the maximum penalties.

CA And with respect to the maximum penalty, the judicial officers have to have regard to that when sentencing.

W They do have to have regard to that.

CA Which in your view may lead to harsher penalties being handed down?

W So that will always depend on the nature of the case.

CA Yes.

W But the most critical thing is detection and prosecution where appropriate and for Parliament setting the maximum as an indication of the seriousness of the offence. And that's always critical so that not only the courts have to look at that, but in terms of generally saying to the community, "This behaviour is wrong. There is a serious maximum penalty there and it must be taken seriously." But alongside that, and we've touched on that already, they have to believe that they're caught and they have to believe that what they're doing is actually a criminal offence and, therefore, the clarity of the provision becomes critical.

CA Now, with respect to looking to, sort of, tweak and amend 408E to ameliorate it with respect to this specific purpose of employees misusing confidential information that they obtain through work purposes, in particular on the computer – their databases, that may cause some interference with prosecuting under – for hackers if it's amended too much. In your view would it be better to have a whole new section?

W In looking at this in preparing for coming along today I came to the very clear view that a new provision was needed for a number of reasons: one I've already touched on, being clear what the offending behaviour is. But in changing this too much, 408E, you may inadvertently have the provision then become less useful in that hacking/viruses-type situation. It may be possible to do both, to do some clarifications in 408E.

But my submission would be having thought carefully about this that it would be much more productive to have a new provision, mainly for the fact of sending that very clear message about the type of offending, that this is criminal behaviour and that you may not do – you may not access confidential information.

I think a public officer who looks at 408E may not even understand it applies in their situation. The wording is not directed towards this type of offending behaviour. It has been able to be, if I can use the word, and I don't mean it in a pejorative sense, but it has been retrofitted to fit that 22 years after it was brought in. Perhaps it's time not to change that radically because it might, as you suggest, harm the intended purpose of it with respect to viruses and hacking and other types of misuse of a computer but look more generally at the problem. And the problem as I see it is misuse of confidential information.

CA So if we could just go through 408E and look to where if there were to be a new section there could be some adjustments and then translated over into the new section. In your view, should it be an aggravating factor that the offence is committed by a public officer?

W Yes. And I think that's one of the major problems in that provision. There are other ancillary provisions in the Criminal Code where that is the case.

CA Yes, we'll just go to one of those. I'll just show you section 398 with respect to stealing. I tender that document.

PO Exhibit 162.

ADMITTED AND MARKED EXHIBIT 162

CA So we'll just go to 398(5). That's one of the provisions you're talking about, stealing by persons in public service as being a punishment in special cases.

W That's correct.

CA And there is great trust and confidence put by the public in public sector employees and so you see an importance there for deterrence to add to that aggravating factor?

W I wouldn't necessarily phrase it around deterrence. I would phrase it around the duty of confidentiality of a public officer and emphasise what duties and what obligations that public officer has.

CA And then with public officer; that's already defined in the Code under section 1. We'll just get that up.

W Thank you.

CA I tender that document. So there the definition, that's fine for the purpose of the aggravating factor in your view?

W That's correct.

CA Yes, thank you.

PO Exhibit 163.

ADMITTED AND MARKED EXHIBIT 163

CA And another aggravating factor would be, as you've said, there can be some real harm, as we have seen with Neil PUNCHARD as an example in more recent times, where there was disclosure of contact details for a domestic violence victim to the ex where she was concealing her address. Some real risk of physical and emotional harm can be one of the types of harm. So, in your view, another aggravating factor should be disclosure?

W Yes. And I think that is one of the major problems with 408E as it currently stands, that disclosure isn't explicitly in that provision.

CA And then-

W -Although, can I just add to that?

CA Yes.

W Quantifying the harm though becomes I think a problem and it is better just to have disclosure. Because if you start quantifying that there has to be a particular type of harm caused it restricts the ability to use the provision, because how do you define what harm might come from that disclosure. The person themselves might, who, you know, who's information has been disclosed, might feel extremely violated even though nothing's been done with that. So I think, after careful thought about it, I think just straight disclosure is the best way to go.

CA Thank you. And then amalgamating, although it wouldn't work for hacking per se, but for our purposes amalgamating 408E(1) and (2)?

W I probably don't have a view on that one and that would have to be very carefully looked at so as not to lose the straight use of a restricted computer which may well harm the hacking-

CA -No but if we're not talking about – we're not talking about hacking, we're talking about setting up a new section.

W Sure. But I'm going to suggest something quite different.

CA Yes.

W I think if you were to amalgamate those two, you do get into the realm of changing what's there now and having unattended effect. So whilst I think on a new provision you may well want to have something as an amalgam like that I probably wouldn't want to do it from 408E itself because you want-

CA -Yes but for a new – yes, sorry, go on.

W So for a new provision I'm going to suggest something quite different.

CA So with (1) and (2); (1) is access, and then (2) is benefit. But just accessing is obtaining the benefit when there's the knowledge that you obtain from accessing. So in relation to increasing penalty, I'll just show you section 92A of the Code.

W Thank you.

CA I tender that document. So that's misconduct in relation to public office. And we've got the maximum penalty there; seven years.

PO That's Exhibit 164.

ADMITTED AND MARKED EXHIBIT 164

W Correct.

CA And then we've seen 398 with the aggravating circumstance of being in public office and that was 10 years. And then under section 340, I'll just show you that section relating to serious assault. I tender that document.

PO Exhibit 165.

ADMITTED AND MARKED EXHIBIT 165

CA So just while we're getting that up on the screen, section 340 relates to serious assault where there's some extra protection given for the police and the like services. So would it be tables turned if that public officer is breaching a

member of the public's privacy then they should be having some extra punishment?

W I believe that's the case.

CA So with the new provision; seven years being the maximum penalty would be in line with other provisions, in your view?

W Given – using computer hacking and misuse in section 340 perhaps as comparatives, I think it's around five to seven years as the initial one. And there's not a lot of difference between five and seven. We have the seven, 14 years and life because of the original transportation provisions. But anything around that five to seven I think sets the right message. But I am going to suggest an offence simpliciter that perhaps has a lower penalty.

CA Before we get to that if we just could go through a couple of other-

W Sure-

CA -sort of parts of 408. So with the definition of benefit; at the moment in the section it says "includes a benefit obtained by or delivered to any person." So we've had some problems where there's looking up, checking for information, for example, quite serious matters, say, where there's a police officer involved in some illegal drug activity, checking to see that there isn't any checking up, surveillance of him. And then another one where checking, as we talked in NEILAND, where checking and obtaining information that is also available publicly. And then you've got checking your own record. We've noticed one of the agencies in particular there's quite a lot of that going on and it seemed to be okay. And so, with respect to benefit, adding and firming up that that includes knowledge. What would be your proposal for that, if any?

W I think that would have to be added. And I can't see any problem adding that to that section, in any event, whether or not there's another provision.

CA And also that could include satisfying personal curiosity, that also type of-

W -I think somehow that could be brought in. It would also need to somehow include where there's been no information found. So checking somebody's record, discovering there wasn't one and acting accordingly. And also your own information. But, again, that starts to not work with 408E. That gets difficult. But certainly including knowledge there would not have any effect on the original intent of computer hacking and misuse.

CA And then with the consent of the controller, just tightening that up to specify that anything outside of being authorised directly for the "during the course of employment for the purpose of carrying out a task associated with employment" is the only time that there's the consent. What are your views on that?

W Sure. I have no problem with that.

CA And so your proposal is to – well would you like to explain your proposal?

W So in thinking about this there's a number of limitations of section 408E. So I might just start with that.

CA Yes.

W It's based on the misuse of a computer and a restricted computer. It's not information more generally. So it doesn't apply if I pick up a piece of paper that I shouldn't have and act accordingly. It doesn't apply where I am told information in confidence and then use that information. So it's, as we've already discussed, it's to do with adding viruses and hacking and those type of activities, not where you're actually just using the information.

It has to be restricted. The whole pass code and other device. Many of the people who have been accessing the records in these cases have done so when they've had permission to be in that database. And I'm sure a lot of the cases that haven't been prosecuted have turned on that point, they have to have been, because the officer had permission to be in where they did. They didn't have permission to do what they did, but that then depends on the agency having a very, very clear statement in relation to those activities. Some I know do, and some may not, but that can be why some of these cases wouldn't be able to be prosecuted. And that comes to the point of using the restricted computer without the consent. Many people do have that lawful access.

And then it turns on some quite difficult points which as we've already discussed prevent the prosecution because then you have to prove all of those things. It is constructed about elements and concepts of damage to a computer system or information. Not necessarily taking out information, which is what we're talking about here. So somebody who goes in and takes it out. And, as I said, information comes in many forms, not just on a computer.

The type of concept we're really talking about here is breaching their duty of confidentiality and it is where it crosses the line between a breach of privacy under the legislation and becomes criminal behaviour. I think any provision that's suggested does need to apply more generally, not just to public officers, although public officers should be an aggravating factor. The key of a provision needs to be about the misuse of information, not just something on a computer, and allowing flexibility in what form that information takes.

I'd suggest taking away any requirement for restricted computer restricted data and so on and confidential information becomes the main point. So, for example, an officer looks up information on a database, it may be their own information that needs to be included. It may be, as I said earlier, searching for information that's not there and then they discover that, for example, somebody doesn't have a criminal record – or it might be health records or something else

– and also needs to apply in other cases where they're getting information verbally or in hard copy.

I think the offence itself needs to be something like a person who without proper authorisation obtains or accesses confidential information. That's probably the offence simpliciter. And that's consistent with 408E, but much simpler and applicable to this situation. So they're obtaining or accessing that confidential information.

The UK provision, which I might come to in a moment, also has added "retaining". And retaining could be a useful element to add into the offence simpliciter as well. So you go in and you find information and you then keep it rather than – I think which goes to the criminality of that behaviour rather than, "Oh I've discovered that, I shouldn't have had that, I'm putting it back." You actually retain it.

Aggravating factors: disclosing the information to a third party. As I said earlier, and I did really grapple with whether that damage should be specified. Perhaps that needs further thought. But I don't know that you can ever quantify the damage of disclosure from somebody's confidential information. And people feel very, very strongly about that. And the public officer definitely should be an aggravating factor.

It does need to include accessing your own record. It needs to include information available publicly. And it needs to include where there was no information found.

There are other elements in there I think need to be there. When you look at some of the cases, for example, where that was necessary for the purpose of preventing or detecting crime. And you do see that element in other pieces of legislation. So there needs to be some safeguards on this because sometimes there's a good reason why that information was accessed even though on the face of it it might have been a breach of the Act or a breach of that provision.

CA Thank you. And there have been some issues with prosecutions where there's the time constraints under the current section, particularly if, as we've seen, often the corrupt conduct of a more serious nature is also involved, and there may be times where there's an investigation in relation to that, and it would be compromised to then charge under the section 408E before that's finalised. And just otherwise the time taken to pursue the investigation. So have you got any thoughts on trying to overcome the issues with time constraints?

W Do you mean in terms of a misdemeanour versus a crime?

CA Yes.

W That has to be really carefully thought out because there will inevitably be cases where that offending behaviour is detected quite some time afterwards by

checking those computer records or by some other method. So I think that does need to be carefully thought out in any new provision. And, indeed, in relation to 408E perhaps that's something that needs to be changed in there as well with subsection 1.

CA Thank you. Thank you, professor. Chair I don't have any further questions for professor.

PO Professor, just one matter. The question of attempting to quantify the damage, I suppose if the provision was simply left at disclosure being an aggravating factor, it could then be up to the sentencing court to make a rough determination of the seriousness by the nature of the damage caused, but the disclosure itself of any sort being an aggravating factor on sentence.

W I think that's right and that could be a further aggravating provision again but it's certainly nothing prevents the sentencing court from looking at the effect of the offending behaviour, what happened after that disclosure and what were the effects of that. It may well be that something was disclosed that identified a witness in a case. And that witness may have been harmed or, even worse, killed as a result. There could be and will be devastating effects of this type of disclosure. But I think just disclosure itself is enough to be an aggravating factor.

PO And I think you said in your evidence that the provision, the new provision that you proposed would have a lesser penalty. Did you have a figure in mind for that?

W Well, with respect to the offence simpliciter, if somebody's just going into a database or some other types of confidential information, they go out again, it's detected by a routine search or for some other reason, they knew something they shouldn't have known, perhaps that is a two-year penalty. I think it would be difficult. Even though we have the crime misdemeanour issue, that would be difficult I think to specify anything higher. It's when it is disclosed becomes the serious aspect. And when it's a public officer. Because of, again, the duty of confidentiality with respect to public officers. But any provision, even though that's outside this inquiry, does need to apply more broadly because you've got banks, you've got private hospitals, you've got the whole gamut.

And I might just add, I didn't mention it earlier, if I could, just so that it is in play here, section 170 of the UK Data Protection Act is something that's quite similar. So I just wanted to mention that.

CA I will just check. Yes, we have that as an exhibit.

W Okay.

CA So we'll exhibit that.

W I think it's just relevant so that becomes-

CA -Yes. I tender that document.

W Thank you. This was the only provision I could find, although there may well be others, when attempting to draft this type of provision, but this was one that I found in the UK. It is an amendment of an earlier Act. It is still very similar, and this is about obtaining or disclosing personal data. So similar to what I've talked about. I think though the way I've phrased is probably better because it is about without proper authorisation, obtaining or accessing. This one though has got in it, as I said earlier, in subsection (c), the retention of the data.

So I think in drafting any new provision this one would be very useful to look at; section 170. I think a lot of jurisdictions are grappling with this problem now that it is so easy to go in and access data of your own or somebody else's and with social media and other ways of disseminating, there is so much more potential for harm than we could ever have envisaged. And that harm can be devastating.

PO This one also has the advantage of outlining with some particularity the available defences.

W Correct. And this one I think is the most – is the most useful and that's got the prevention or detecting crime one as well. In fact that might have been where I saw it originally. And the defences I do think have to be in there as well.

PO I'll make that Exhibit 166.

ADMITTED AND MARKED EXHIBIT 166

W And just one final thing there with respect to this and also with others, you'll note that there's no fault element there; intention or – I think reckless comes in, knowingly or recklessly. But once you start introducing them there can be a real problem. In this case you either access it or you don't and then there's defences available.

PO Thank you. Anything else?

CA Thank you very much. Very helpful.

PO Thank you, Professor, for coming. Thank you. You're excused.

W Thank you very much.

CA Thank you, Chair.

PO Thank you.

END OF SESSION