



COMMUNITY SUPPORT AND SERVICES COMMITTEE

Members present:

Ms CP McMillan MP—Chair
Mr SA Bennett MP (virtual)
Dr A MacMahon MP
Dr MA Robinson MP
Mr PS Russo MP
Mr RCJ Skelton MP (virtual)

Staff present:

Ms L Pretty—Committee Secretary
Ms R Mills—Assistant Committee Secretary

PUBLIC BRIEFING—INQUIRY INTO THE CHILD PROTECTION (OFFENDER REPORTING AND OFFENDER PROHIBITION ORDER) AND OTHER LEGISLATION AMENDMENT BILL 2022

TRANSCRIPT OF PROCEEDINGS

MONDAY, 14 NOVEMBER 2022

Brisbane

MONDAY, 14 NOVEMBER 2022

The committee met at 2.34 pm.

CHAIR: Good afternoon. I declare open this public briefing for the committee's consideration of the Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022. I would like to respectfully acknowledge the traditional custodians of the land on which we meet today and pay our respects to elders past, present and emerging. We are very fortunate to live in a country with two of the oldest continuing cultures in Aboriginal and Torres Strait Islander peoples, whose lands, winds and waters we are lucky to all share.

On 26 October 2022 the Hon. Mark Ryan MP, Minister for Police and Corrective Services and Minister for Fire and Emergency Services, introduced the bill into the Queensland parliament. On the same day, the bill was referred to the Community Support and Services Committee for detailed consideration. The purpose of today is to assist the committee with its examination and deliberation of the bill.

My name is Corrine McMillan. I am the member for Mansfield and chair of the committee. With me here today and online are: Mr Stephen Bennett MP, member for Burnett and deputy chair; Dr Amy MacMahon MP, member for South Brisbane, who is substituting for Mr Michael Berkman MP, member for Maiwar, who is unable to attend today; Mr Peter Russo MP, member for Toohey, who is substituting for Cynthia Lui MP, member for Cook, who is also unable to attend today; Mr Robert Skelton MP, member for Nicklin, who is attending via teleconference; and Dr Mark Robinson, member for Oodgeroo.

The committee's proceedings are proceedings of the Queensland parliament and are subject to the standing rules and orders of the parliament. The proceedings are being recorded by Hansard—thank you, Hansard—and broadcast live on the parliament's website. Media may be present and will be subject to the chair's direction at all times. The media rules endorsed by the committee are available from committee staff if required. All those present today should note that it is possible you might be filmed or photographed during the proceedings by media, and images may also appear on the parliament's website or social media pages. I ask everyone present to turn mobile phones off or to silent mode.

Only the committee and invited officers may participate in the proceedings. As parliamentary proceedings, under the standing orders any person may be excluded from the briefing at the discretion of the chair or by order of the committee. I also ask that any responses to questions taken on notice today are provided to the committee by 12 pm on Friday, 18 November 2022. The program for today has been published on the committee's webpage and there are hard copies available from committee staff.

AITKIN, Detective Senior Sergeant Sarah, State Registrar, Child Protection Offender Registry, Queensland Police Service

CLARK, Detective Acting Chief Superintendent Denzil, Child Abuse and Sexual Crime Group, Queensland Police Service

DONALDSON, Detective Acting Superintendent Glen, Child Abuse and Sexual Crime Group, Queensland Police Service

DUNCAN, Detective Inspector Julie, Officer in Charge, Child Protection Offender Registry, Queensland Police Service

REEVES, Senior Sergeant Andrea, Instructing Officer, Legislation Branch, Queensland Police Service

CHAIR: Good afternoon to each and every one of you. The committee thanks you for your time today. I invite you to make a brief opening statement, after which I am sure our committee members will have a number of questions.

Det. Chief Supt Clark: Thank you for the opportunity to brief the committee in relation to the Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022. The purpose of the bill is to ensure the legislation underpinning and supporting the child protection registry scheme continues to protect the lives of children and their sexual safety. I have four officers with me from the Queensland Police Service to assist the committee in its understanding of the bill. As the Acting Chief Superintendent of Crime at the Crime and Intelligence Command, I oversee the management, administration and operations of the Child Abuse and Sexual Crime Group, which includes the Child Protection Offender Register, Argos, the child trauma and sexual crimes unit and the youth justice unit. My substantive position is actually as the superintendent of the Child Abuse and Sexual Crime Group. The Child Protection Offender Registry primarily focuses on prevention, disruption and early intervention strategies to reduce the likelihood of reoffending by reportable offenders. It does so by engaging with reportable offenders and monitoring their activities while they reside in the community.

I understand the committee has been provided with a departmental written briefing for consideration. The written briefing complements the bill, explanatory notes and statement of compatibility. I intend to focus my statements today on the operational aspects of the bill and the benefits those amendments bring to my staff, the Queensland Police Service generally and, most importantly, the children in the community.

As at today, the Child Protection Offender Registry is responsible for the monitoring of 3,982 reportable offenders in the community. Of these, approximately 55 are considered higher risk offenders due to their status as a reportable offender who has previously been the subject of an order under division 3 of the Dangerous Prisoners (Sexual Offenders) Act 2003 and has been convicted of reportable offences under the Child Protection (Offender Reporting and Offender Prohibition Order) Act—these people are referred to as post-DPSO offenders—or because they are subject of an offender prohibition order.

The registry comprises 42 specialist detectives based regionally throughout Queensland; a forensic behavioural investigation specialist team who assess risk and high harm; a high-risk offenders team; a registry investigation team; and staff members who receive reports regarding changes in personal details from reportable offenders. Reportable offenders are required to report their personal details four times in each year and then on each occasion those details change. The details required to be reported are provided in schedule 2 of the act. There is capacity to increase or suspend reporting requirements based on risk.

Every reportable offender is personally given a notice of their reporting obligations. This is a written document setting out what is required to be reported and the consequences of failing to meet those requirements. A new notice is given each time those obligations change. This ensures every reportable offender is fully aware of their obligations at all times. In addition to giving each reportable offender a notice of their obligations, each reportable offender is assigned a police case officer who not only monitors compliance but can actively assist a reportable offender to meet their obligations under the act and, where appropriate, refer the reportable offender to an external agency for support.

The way in which child sex offenders engage, groom and offend against children has changed in recent years. This is due in part to the COVID-19 pandemic and enhancements in technology. Children are more present in an online environment at a younger age, and the increased use of online dating forums has created an environment where child sex offenders can groom parents as well as their children. These changes have significantly enhanced the opportunity for child sex offenders to gain access to vulnerable children. To illustrate this point, research conducted by the Australian Institute of Criminology into how online dating sites are being used to conduct child abuse and exploitation was published in October of this year. Of the 9,987 respondents who took part in the Australia-wide research, 12.4 per cent reported receiving requests to facilitate the sexual exploitation of their own children or children they had access to. This is concerning and highlights the diverse ways in which child sex offenders operate.

The bill addresses these changes in offending by providing police with the tools they need to monitor online activities and to inspect digital devices, with the aim of preventing and disrupting sexual offending against children. The new technology-based provisions contained in the bill will allow police to enter the residence of a reportable offender for the purpose of undertaking a digital device inspection. A device inspection applies generally to all reportable offenders in a three-month period after their release from custody or sentence to a supervision order and also where they have been convicted of a prescribed offence. Other reportable offenders may be subject to a digital device inspection if a court makes a digital device inspection order because the court is satisfied there is an increased risk of reoffending, particularly online.

The new entry provision is a simple but important change which operates in the same way as the current entry provision to verify personal information. It does not infer a search of the residence. It is, as it suggests, entry to inspect digital devices. The use of the power will be subject to the same parliamentary oversight as the current power to verify information. This entry provision is supported by a requirement for reportable offenders to report each digital device in their possession. Currently, offenders are only required to present a device, and this is being interpreted to mean one device. As a consequence, other devices that may be in the possession of the reportable offender are not presented and, in the absence of an entry provision, this impedes our ability to effectively monitor this cohort of offenders.

Working in concert with these changes is the new requirement for reportable offenders to report the media access control, MAC, address of each digital device they possess or use. Reporting the MAC address for each digital device will assist my team identify the number of digital devices each offender possesses or uses, for the purpose of undertaking a digital device inspection. There is a dual benefit in obtaining this information: for reportable offenders it simplifies the device inspection process and minimises disruption to their lives; for my team of specialists it provides an insight into how offenders are engaging in the online environment.

The bill also increases the number of offences that will trigger a digital device inspection. There is a cohort of reportable offenders who use digital technology to access, possess and produce child exploitation material or to groom and/or engage in sexual activity with children. These additional offences target those reportable offenders who have harmed children, either directly or indirectly, through the misuse of technology and have been assessed by my team as presenting the greatest risk to children. The new offence provisions operate retrospectively to capture existing reportable offenders. This is vital to risk reduction. We need to understand our offenders' online activity if we are going to prevent or disrupt the offending cycle.

The amendments move away from the generic monitoring model to focus on risk, presenting a new way of looking at how we engage with reportable offenders in the community to prevent reoffending. We are very fortunate to have a dedicated team of forensic behavioural specialists who are well trained to determine any increase or decrease in the risk that a particular reportable offender presents.

To assist with online risk assessment and reduction, we need reportable offenders to be visible at all times. The bill assists with this by requiring reportable offenders to report the details of any anonymising software or the details of applications that hide information on a digital device. Anonymising software includes virtual privacy networks, which are used to hide the IP address of the device and any activity used through the device. Anonymising software can be beneficial by providing the user with an additional layer of security when they are online; however, it is most often used by child sex offenders to engage with other child sex offenders on the dark web or to engage with and offend against children without detection.

Other applications which hide information on a device will also be required to be reported—for example, vault type applications which look like a normal desktop phone icon and secure sensitive information, and black hole applications which hide other applications such as vault applications from plain sight. I understand there is a need for sensitive online information to be protected; however, where an offender has been convicted of child sex offences using a digital device there need to be checks and balances in place to prevent reoffending and to maintain the safety of children.

Information is one of the greatest tools we have to determine the behaviour of our reportable offender cohort. The capacity to obtain information from agencies such as Queensland Corrective Services saves valuable time and resources when an offender cannot readily be located, so too information sharing and collaboration. In this regard, the bill improves our information-sharing capabilities so that our Commonwealth colleagues—the Department of Home Affairs, Australian Border Force and the Australian Federal Police—will be able to readily receive information held on the Child Protection Register about Queensland reportable offenders to assist in their operations targeting national and international child sex offenders and exploitation.

We will also be able to receive and share information with our overseas registrars about reportable offenders entering or leaving Queensland. While Australia can prevent a reportable offender travelling overseas, reportable offenders are able to enter from other countries. By recognising any jurisdiction that has a reportable offender scheme, my team can act preventively by serving a notice of reporting obligations and commence monitoring their activities while they remain in this state. As a result of this bill, the Child Protection Offender Registry will also be able to work

collaboratively with the department of immigration to ensure reportable offenders in immigration detention are given a notice of reporting obligations. This is particularly pertinent where an offender is later discharged into the Queensland community.

There is also an increase in offender reported information requiring reportable offenders to provide information that they have previously failed to report and to report additional information about their activities. This not only holds them accountable for the short period of time they are required to report; it also ensures the National Child Offender System has a complete repository of information and activities about each reportable offender.

The bill will require some reportable offenders to report a place where they stay or can be located that is not their general residence for three or more consecutive days and within 24 hours of a change happening. New section 19B focuses on offenders who have been assessed as presenting an increased risk of offending and who engage in short stays throughout Queensland because they are travelling or are not able to stay at their usual place of residence. This provision is not dissimilar to the requirement on our current post-DPSO reportable offenders, who must report a change of residence within 24 hours.

To offset the increase in reporting requirements, we are focusing on technology to drive reporting. In this day and age, most people have access to some form of technology. Reporting methods such as telephone and online secure platforms are available 24 hours a day, every day of the year. They also remove the impost associated with reporting at a police station in person. It is not our intention to penalise offenders who are not able to access or use the online platform. These offenders can still send their reports through the post to the officer in charge of the Child Protection Offender Registry. The postmark on the envelope will be considered the date the report was made.

There are also specific provisions under the act for remote reportable offenders. These provisions will continue to allow an agreement to be made with us about how reports can be made. The changes to how reports are made will be included in the notice of reporting obligations and does not remove the ability for the registry to require an offender to report in person or more frequently based on the risk an individual poses to the lives or sexual safety of children.

I have spoken previously regarding the benefits of information to determine how reportable offenders are monitored in the community. I have not fully addressed when information can have a converse effect. In particular, we are required to give reportable offenders a report of all the information reported as part of the obligations under the act. This includes personal information about reportable child contact. Some reportable contact with children may be due to prior employment or a previous relationship with a parent. That information may no longer be in the possession of the reportable offender. The bill removes this obligation to ensure that personal information about children is not given to a convicted child sex offender.

This bill will enhance the operation of the Child Protection Offender Registry and ensures the offender reporting framework remains contemporary to emerging offending behaviours. My colleagues and I are now happy to answer any questions the committee may have in relation to this bill.

CHAIR: Thank you, Detective Acting Chief Superintendent. That was a very thorough introduction. Thank you very much for all of that information. On behalf of the committee, I thank each and every one of you for the work that you do in keeping our children in Queensland safe. We all acknowledge the very tough job that you have, sometimes under quite horrific circumstances. We thank you.

Mr BENNETT: Good afternoon. I am sorry I cannot be with you in person. The thing that concerns me from the briefing and the legislation is that reportable offenders from overseas are even being allowed into Australia. You might be able to help the committee understand. There are crimes that prevent people coming into our country—for drink driving, as I understand it, you have to get some sort of special character assessment check. Why would we even allow these convicted people on a register into Australia?

Det. Chief Supt Clark: I suppose the issue for us is that that legislation rests with the Commonwealth. We have no influence at all in relation to who comes into the country, but once they are in the country our concern is that they may come into Queensland, and we do want to be able to identify them, capture them and then monitor them, as we do with reportable offenders already here.

Mr BENNETT: I think you said there were 38- or 40-odd people on the child offender register who you are actively working with. I am wondering about their access to the internet outside the basic parameters. The fact that they can get this software to protect their identity—it worries me that that is

even allowed to exist in our country. I know that you cannot be hard all the time, but, if they have been convicted, why are there not more stringent restrictions on what they are allowed to use on the internet or social media?

CHAIR: We might just need to confirm those numbers. It is very hard when members are on the phone, but I think the numbers might have been incorrect.

Det. Chief Supt Clark: As of today, we have 3,982 offenders on the register in total.

CHAIR: That is in Queensland?

Det. Chief Supt Clark: That is correct—that is the Queensland component of the national register. We have 55 post-DPSO offenders that we are currently monitoring. They are the higher risk offenders for us in the community.

Mr BENNETT: Maybe this is a policy question that is not fair to ask the panel. That is probably a question for the minister.

CHAIR: Deputy Chair, I think we are delving into a federal issue around networks and access. Do you have another question?

Mr BENNETT: In relation to the use of the software that is being talked about from the perspective of the police monitoring dark web or deep web information, how many different software packages do we know of that might be used to try to provide them the anonymity we are talking about in the bill?

Det. Chief Supt Clark: I will speak briefly to that and then I might go to Detective Inspector Donaldson on that. I would not have an answer on the number of pieces of software out there. In my view there are two parts to this: there is the anonymising software, which is hiding that person's identity from police so we cannot identify—we know something has happened or is happening but we do not know who is the person behind that; and then you have the vault or blackhole software. We do know who that person is because we are looking at their device, but they are using that to obfuscate and hide their activities from us. There are two groups of people we are looking at here: those who are hiding in plain sight and those we know about but who are hiding their activities on their devices. We have been very broad in our definition in relation to both the anonymising software and the types of devices because technology is changing so quickly we would not be able to list them all individually.

Det. Supt Donaldson: My substantive role is as the officer in charge of Argos. It is the online unit. In terms of the software that is available, there is a plethora of software. If you just google apps that hide apps, a list will come up of the top 10 apps that will hide apps. When we talk of the darknet, it is a phrase that encompasses any part of the internet you need special software to access. That can include TOR, or The Onion Router, which is what a lot of people know about. There are other types of darknet such as the Invisible Internet Protocol or Freenet. There are apps you can get through the Play store and Google or through the Apple Store. Anyone can get them.

In terms of some of the anonymising software or the virtual private networks that we speak of, there are lawful and legitimate reasons to have that technology. I have a VPN on my mobile phone. If you go to a public wi-fi or you want to use Westfield's wi-fi, I would not be using that without a VPN; otherwise, people who own those routers could read what you are doing. There are certainly lawful reasons to have that but also there are nefarious reasons. In terms of some of the darknets, The Onion Router and Freenet, obviously the legitimate reasons to hold that are very small for this cohort, definitely.

CHAIR: Deputy Chair, does that suffice?

Mr BENNETT: Yes, thank you.

CHAIR: Detective Chief Superintendent, during your opening statement you referred to a report written by the Institute of Criminology. I wondered whether you would be so kind as to share that report with the committee. It certainly would help with our deliberations.

Det. Chief Supt Clark: Absolutely.

Mr RUSSO: I am interested in why the retrospectivity is needed to look at the current, for example, 55 high-risk offenders. Would they not already be subject to this once the legislation is passed?

Det. Chief Supt Clark: The legislation would normally capture them as they are coming onto the register. The intent of the retrospectivity—

Mr RUSSO: It does not capture them if they are already on it?

Det. Chief Supt Clark: That is correct.

Dr ROBINSON: To what degree does the reportable offender scheme rely on the offender providing accurate and honest information at risk of penalties? To what degree are other police investigations conducted, for example, into the number of devices an offender may have?

Det. Chief Supt Clark: The reporting of the information is critical to the basis of the register. The accuracy of that information is important. That is the crux of the register. For the first part of that question, yes, the accurate reporting of information is critical to the purpose of the register itself. What was the second part of that question?

Dr ROBINSON: To what degree are police investigative tools used to determine whether there are other devices an offender is using—other than what they have self-reported or confessed to?

Det. Chief Supt Clark: Through the course of our duties we do obtain information which will identify a number of different devices an offender may be using. The purpose of requesting them to produce all of those devices is that if they are being honest, truthful and open we will be able to check those off against those that we know about. If they fail to produce devices that we are aware they have in their possession, that will heighten our concern as to why they have failed to produce that device. We would make further inquiries in relation to why that is the case. I will not disclose details of how we can come across that particular information, suffice it to say we have both covert and overt means to identify different devices.

Mr SKELTON: In regards to (inaudible) and anonymising, with a penalty for non-reporting, is it an offence for a reportable offender to possess or use those applications?

CHAIR: The signal is not very good for the member for Nicklin. He is asking: under the bill, offenders would have to report the possession or use of anonymising software and hidden applications with a penalty for non-reporting. Is it an offence for reportable offenders to possess or use those applications?

Det. Chief Supt Clark: No. My partners could correct me on this, but there is no offence for having those in your possession. We certainly would not want to restrict any member of the community protecting their own online identity or digital information; hence, there would be no offence for a reportable offender possessing it. However, as we know how it is used to commit offences, the obligation is that they will report that to us so we can then explore that further.

CHAIR: That alludes to remarks made by Detective Acting Superintendent Donaldson around the use of public wi-fi.

Det. Chief Supt Clark: That is correct.

Dr MacMAHON: Detective, you talked about a level of risk that would be triggered when people are moving around to lots of different locations. There are lots of reasons people might move around. Would you be asking people, 'Why have you been moving around to these different locations? Is it because your housing tenure is complicated?' Does that automatically trigger a level of risk?

Det. Chief Supt Clark: There are two parts to that. The first one is what the legislation obligates the offender to report, and that is what we would require them to provide to us. In terms of questions in relation to their welfare, their current living arrangements and support, we would do that by negotiation as part of our broader care towards that person in the community. Then it is up to them as to whether they would like to provide that information to us. If we can work with them, as I said, if we can assist them stabilise their environment and provide them supports, we will because we know that if they have a stable environment and are feeling secure there is less risk of them entering into their offending cycle.

CHAIR: Just out of interest, I want to pick up on the question of the deputy chair in relation to—and I know it is not your jurisdiction. In relation to those reportable offenders residing overseas, I assume they do not have their passport taken, which would allow them to travel internationally?

Det. Chief Supt Clark: I will speak in generalities because each jurisdiction is different. I will say that some do restrict the offenders from travelling, as does Australia; we are quite strict on that. We have some good legislation to stop that. Other countries perhaps do not have that same level of rigour and that broader sense of community to protect other countries' children.

Mr BENNETT: I might be getting a bit focused here. I refer to a person getting an offender reporting order and I note there have been some changes in new section 12D. What prompted the inclusion of this? Was there something that was happening previously that was not assisting you in your daily work issues?

Det. Chief Supt Clark: Thank you for the question. I will defer to Julie and then go to Sarah Aitkin.

Mr BENNETT: While you are looking, I am wondering how it happens now that people go from being an offender to being a reportable offender.

Det. Chief Supt Clark: I will answer that one. There is a list of reportable offences. If a person is convicted of a reportable offence they are automatically included on our register. We also recognise corresponding acts across the country. If they are placed on a register in another state or territory, they will automatically be placed onto our register when they enter our state for more than seven days. Then for those offences that sit outside of the reportable offences list where the court believes that person poses a significant risk to the life or sexual safety of a child, the court may order that person be placed on the register for us to monitor.

Det. Snr Sgt Aitkin: I will add to that. The inclusion of proposed section 12D has provided some clarity and guidance to the courts about some considerations for those scheduled offences that sit outside of the act as it stands now about what is to be considered when an offender or reporting order is being made.

Mr BENNETT: Those changes—and you might be able to tell us what they are; I do not think that is the issue. We have broadened the definitions and added some offences to section 12D for the judges to consider?

Det. Snr Sgt Aitkin: No, it just gives some clarity. Even though the offences in themselves stand as a conviction, and given there are so many complexities involving hypothetically the age of the respondent, their relationship with the victim and the differences between their ages as well, there are a lot of complexities that need to be considered before an offender reporting order is made. The courts had provided some feedback in our consultation phase that the act in itself was silent on what considerations need to be made.

Mr RUSSO: The new section will allow the court guidance in relation to the interpretation of when a reportable offence—there are two ways it happens now. One, if you are in the schedule, it is automatic. This will just cover a cohort of offenders who were not being captured by the automatic reporting?

Det. Chief Supt Clark: That is correct.

Mr RUSSO: This came about from consultation with the judiciary?

Det. Snr Sgt Aitkin: That is correct.

CHAIR: Member for Burnett, does that clarify your thoughts?

Mr BENNETT: Absolutely. Thank you, Chair.

Dr ROBINSON: In terms of inspections of devices, are they always scheduled inspections or are they sometimes conducted randomly or by surprise?

Det. Chief Supt Clark: I will defer to Sarah on that one.

Det. Snr Sgt Aitkin: In the high percentage of it, it is a random inspection—unannounced arrival by either the high-risk offenders team or the case manager for each district.

Mr SKELTON: How would you verify that the MAC address is that of the reportable offender and that they have provided the correct one?

CHAIR: So how would police verify that the MAC address the reportable offender provides is the correct one?

Det. Supt Donaldson: That would basically be through the settings. It is a physical examination of the device itself.

Dr MacMAHON: Is the research that you mentioned around online dating platforms publicly available?

Det. Chief Supt Clark: Yes, it is.

Dr MacMAHON: Are you able to make that public at all or just direct me to where I can find that?

Det. Chief Supt Clark: Yes. I believe we have already agreed that we will provide that to you.

Dr MacMAHON: Great. Also, you mentioned that people will be referred to external agencies if they need support. What agencies are they?

Det. Chief Supt Clark: There are multiple agencies in the community that we can refer to, depending on the location of the reportable offender. As we know, not all services are available across all locations in the state. I will again go to Sarah, who has a lot more of the intricate operational knowledge.

Det. Snr Sgt Aitkin: As the chief indicated, it depends on the geographic location of the offender. It could be assistance with housing, Centrelink applications or obtaining a GP or a treatment program in their area. We are also piloting a program at the moment—Stop It Now!—which is an online telephone centre they can call and talk about if they think there are offending urges or anything. It is really specific to the individual and the individual circumstances that are surrounding both them and their families or whatever connections they have in the community.

CHAIR: The bill would introduce a new reporting obligation requiring a reportable offender to report the details of every premise or location they stay or can be located for a maximum of three consecutive days within 24 hours of that change happening. I am interested to know why three days. It is obviously an evidence-based decision. That obligation would be enlivened only in certain circumstances. Why does it not apply to every reportable offender?

Det. Chief Supt Clark: Making reports does place an onus on every reportable offender. This is not meant to be a punishment, that they make reports to us. There is a balance between the information being provided to us in a timely fashion and the demands we are placing on reportable offenders. We do not want to set them up to fail. These time frames are nationally consistent regarding the seven days et cetera. For those we are asking for the three days, we have greater concern around those particular offenders and their movements—for whatever reason—and we have decided that, because of the risk around that person, we are going to increase the demand we are making on them regarding reporting. It is not for everybody; it is only for those we feel create the greatest concern.

CHAIR: Could you explain the three days? It is nationally consistent. Why is it not less than three?

Det. Chief Supt Clark: Again, it comes down to reporting obligations. People having to report every single day creates a burden on the police as well as on the offender. Three days has been deemed a reasonable time to allow somebody to transition to a new location and then report it to us. Obviously an offender could offend within minutes of attending to a certain location but, managing risk and all the other considerations, three days is the time that we have decided is appropriate.

Det. Insp. Duncan: I suppose it goes both ways with regard to making sure the reportable offender can obtain suitable accommodation as well. There are people in our community, unfortunately, due to their circumstances, who need assistance. The member for South Brisbane asked about the welfare and looking after the community via supporting reportable offenders. The three days is an opportunity to have them placed. These are the restrictions on specific circumstances based off risk.

Mr BENNETT: In your introduction you provided information about the media access control, the MAC. So that is a unique code that allows you to find and monitor that device? I am sorry, I am putting words in your mouth. Can you explain the media access control? Is that on all 3,982 offenders or just the 55 offenders?

Det. Supt Donaldson: A MAC address is a serial number for a device. I guess that is the best way to describe it. Your house has an IP address, but in your house you could have 15 or 20 internet connected devices. Say you go to couriermail.com. When the information comes back, your router needs to know which device is requesting this information. That is via a MAC address, which is hard stamped into the network interface card of your device, whether it is a phone, an Xbox, a laptop or a PC.

Det. Chief Supt Clark: In relation to your second query, it is not just in relation to the 55; it is in relation to all those people who have qualified for a device inspection. That is not the entirety of those on the register; it is only a cohort.

Mr BENNETT: Picking up on an earlier comment about setting people up to fail, why would certain locations on the web not be banned? We can do it for kids under 15 in terms of parental control. Is that being overly paternalistic to these offenders?

Det. Supt Donaldson: Again, I think it is balancing everyone's human rights to access information. There are legitimate reasons to access any of these sites. Some of them—for example, the Freenet or the invisible internet protocol—have a much higher illegal usage rate. So does the darknet. That is not to say that someone does not have a lawful reason. They could even be studying at university or at TAFE and be accessing it. I think it would be very difficult to totally prevent access. As I said, certainly for software like a virtual private network, that is something that people have lawful reasons to utilise.

CHAIR: Detective Acting Chief Superintendent, do you want to add something?

Det. Chief Supt Clark: Yes. I just want to correct a statement I made before. I said that the requirement to report a MAC address was for only the cohort who are subject to device inspections. That was incorrect. All reportable offenders are required to report their MAC addresses to us, but there is only a cohort of offenders for which we would be doing device inspections. I am sorry about that.

CHAIR: I understand the confusion.

Mr BENNETT: With the 55 reportable offenders that we are talking about, do we know right now where those 55 are living? They can be quite transient and it is sometimes difficult to keep up with that. I understand the reporting, but do we have any outside the reporting regime of the three days that we do not know where they are?

Det. Chief Supt Clark: No. All of them are present and accounted for. We do have a status called 'whereabouts unknown'. We have none who are currently whereabouts unknown.

CHAIR: Thank you, Deputy Chair. That can alleviate any of your concerns.

Mr RUSSO: In relation to the darknet, that brings to mind that if you are using the darknet you cannot be using it for any good purpose. Is that too simplistic?

Det. Supt Donaldson: Look, it is. Think of people's concerns about big data, companies like Facebook and how much Facebook knows about you. You can actually access Facebook via the darknet so it will significantly limit what Facebook will know about you. Again, depending on your level of privacy concerns, I know some people who will access Facebook through the darknet. It will be a lot slower, given the way that it routes your data through different servers. It is something that is almost impossible to police anyway, to ban access to the darknet.

Mr RUSSO: The name 'darknet' is probably—

Det. Supt Donaldson: It is a parenthood term for part of the internet that can only be accessed by certain software. There are basically three types of internet. The image they commonly see—you might have seen it online—is an iceberg. The tip of the iceberg is called the clear net, which any of us can access. There are no passwords and there is no user ID. It is the tip of the iceberg. The majority of the internet is what they call the deep web, which I am sure your parliamentary email and the Police Service system use. It gives access the internet but it is locked away. You need user ID and a password. Then there is very bottom of the iceberg image which is the dark web, and that is only accessible via certain software. It is not indexed by Google or by Safari. You need specific software. You cannot hop on and type in 'Courier-Mail'; you need to know the specific address to access those sites.

Mr RUSSO: That is why it facilitates the illegal access to sites? For example, if you are using Google to try and find those sites, it would not be possible?

Det. Supt Donaldson: No. Google will not know where they are. It is like a table of contents, I guess, at the back of a book. Google indexes the entire internet. When you type in a search, it uses a DNS, or domain name server, to find out where is couriermail.com. All of these sites in the darknet are not indexed. It is not in the table of contents of Google, so you need specific software.

It is also the way that the data is accessed. If I want to hop on the *Courier-Mail's* website, I will go to, say, Google as my web browser. It will reach off and then it will come back with the *Courier-Mail's* data or website. That is almost a direct connection. Anyone—Google, Telstra—can see what I am doing. The way the dark web works is that it routes your traffic. For example, I might use The Onion Router. They call it an onion router because at each level it is unwrapped, basically. If we go back to writing letters—no-one writes letters anymore—I may write a letter to you, but it is wrapped in a letter to Sarah that is wrapped in a letter to Denzil that is wrapped in a letter to Julie. At each stage of the process, you only know the next stage. No-one knows whether they are the end where it is going. That is why it is extremely difficult. Other than the entry and exit nodes, when it goes in and goes out, no-one knows where it comes from. It is very difficult to trace back.

Mr RUSSO: There is a possibility that someone who is on the register who has access to the darknet could be using it for illegal purposes?

Det. Supt Donaldson: That is correct, yes.

Dr MacMAHON: This is a technical question, but can you direct the use of apps on your phone through the dark web?

Det. Supt Donaldson: If you go to the app store you can type in 'TOR' and the TOR browser will be there. That will enable you to access the dark web. I believe there is also the I2P, the Invisible Internet Protocol. That is another app you can get. I am an Android person, so I am assuming it is also on Apple.

Dr MacMAHON: You could access a dating app, for example, through the dark web?

Det. Supt Donaldson: It would depend. Not every website in the clear net is available through the darknet. Certain companies like Facebook or other websites allow access via the darknet, but generally the locations are specific to the darknet.

Dr MacMAHON: For someone on a dating app, is that something you would look at when you go and inspect someone's phone? You would see that they are using this platform, who they are talking to and so on?

Det. Supt Donaldson: It depends on the nature of the app. Some apps like Snapchat will obviously delete those messages as soon as they are read. It depends on the actual application they are using.

CHAIR: Thank you, member for South Brisbane. That concludes our session this afternoon. I do not believe any questions were taken on notice. I thank each and every one of you again for the work that you do in keeping our children safe. We know that you work at a level far beyond our understanding, but we have absolute confidence in the work that you do. We thank you again for all that you do to keep Queensland children as safe as we can. That concludes this briefing. On behalf of the committee, I thank you for your attendance today. Thank you to our Hansard reporter. A transcript of these proceedings will be available on the committee's parliamentary webpage in due course. I now declare this public briefing closed.

The committee adjourned at 3.30 pm.