Crime Interrupted
An AFP and Casefile Presents podcast.
Episode 4, Operation Ascalon transcript.

Host – introduction
The Australian Federal Police – or AFP for short – is Australia's national policing agency. Its aim? To outsmart serious crime with intelligent action. Officers from the AFP work with local, national, and international agencies to combat serious criminal threats. Their work includes counter terrorism, serious organised crime, human trafficking, cybercrime, fraud, and child exploitation. The AFP exists to disrupt major criminal operations. In 2020-21, they did that over 400 times. They seized 38 tonnes of illicit drugs and precursors, and assisted overseas police services in seizing 19 tonnes of drugs. The AFP charged 235 people with child exploitation, and charged 25 people following terrorism investigations.

We've got exclusive access to the AFP case vault and personnel to provide you with in-depth insight into how they investigated and interrupted the most serious of crimes to stay a step ahead.

[theme music]

Host (1.48)
Some crimes are so disturbing, our natural instinct is to look away – especially crimes against children. But the truth is, these are the very crimes we need to know about, because if we know how offenders target children, then we can use that knowledge to protect them. We need to know the signs to look out for. Having said that, this is an AFP operation where an offender targets children online, so we wanted to include a trigger warning.

The AFP's Operation Ascalon investigated a 23-year-old offender who was able to manipulate teenage boys online, and once they were caught in his snare, he used blackmail and threats to keep them there. At least he did, until his activities were reported to the AFP. From that moment on, his days as an online offender were numbered.

We are going to call the offender Michael. This is not to protect his identity, but rather to protect the identify of his young victims.

Michael's methodology was consistent and simple. Going online, pretending to be a 16-year-old girl, he connected with pubescent boys, at first, requesting pictures of them, but soon specifically asking for naked photos. In return, Michael would send various clothed and naked images of a teenage girl to groom his victims into sending more graphic pictures of themselves. Increasingly, he would ask the boys for more images and then sexualised videos. When the boys declined to send further videos, because they grew suspicious, or the requests became too invasive, the offender would threaten to distribute the material he'd already received from the boys and send it to their friends and families. Sometimes, he followed through on the threats.

You can only imagine the terror the young victims went through. Their exciting online chats with a girl, suddenly became filled with coercion and threats, and no way out unless they told an adult what they had done, which for most young people would be far too embarrassing and humiliating to contemplate.

It all began a couple of years ago, when a father reported that his 13-year-old son had been the victim of online sexual abuse.

Detective Acting Inspector Jarryd Dunbar was the Team Leader of Child Protection Operations in the AFP when the case came through.

Jarryd Dunbar (4.36)
These children thought that they were talking to someone who was their own age, that they could share these intimate moments with, only to find out that it was an adult male that they were talking to. The father of the child victim contacted our assessment centre, which they're essentially responsible for receiving all incoming referrals into the AFP. So the father advised them of what had occurred in relation to his son, and provided additional information regarding the account that was used by the offender to contact his son. From that information, they were able to put in checks to the social media company, which in this particular instance was Instagram, and that identified an IP address that they were then able to link to the family's internet connection, and his premises here in New South Wales.

Host
When Jarryd's team first heard of the complaint by the father of the young victim, it was easy enough to trace the offender – a 23-year-old man called Michael. The investigation was named Operation Ascalon. Jarryd's team tracked Michael down. It turned out, he wasn't in the country, but he was due back soon.

Jarryd Dunbar (5.45)
When we received the referral from our assessment centre, we actually found out that he was offshore. He was actually enjoying a ski trip overseas at the time that the referral initially landed with our team. So it gave us a little bit of lead in time to identify exactly where he was and where the evidence was likely to be stored, whether it be at his house or on his person as well. What it also allowed us to do was essentially stop him once he returned to the country. So, it would have been about a week after we received the referral, he returned into the country. We were able to stop him at the border, with the assistance of the Australian Border Force, and at that point in time, he was arrested.

Host
Michael arrived back from his overseas ski trip with no idea that he was about to be taken into police custody. All electronic devices he had with him as he entered the country were seized.

Jarryd Dunbar (6.33)
Anything that he bought back with him, so there's a couple of mobile phones he had with him, a laptop, computer, and a tablet computer. And at the same time, we executed a search warrant at his house as well in New South Wales where a number of other electronic devices; so there was some hard drives, some more computer equipment as well that were seized. Once we gather up all those items, we look at a lot of those electronic items in the field. And the reason that we do that is because it allows us to identify offences that have occurred that we can then charge with at the time. The last thing we want is for someone like this, to be able to be released

without a charge, which is the worst-case scenario, or potentially released on bail. So the more charges we can identify at that time when we arrest them, the greater prospects we have of having them remanded in custody.

Host
The on-the-spot check of Michael's electronic devices at the airport, showed enough evidence of child abuse materials, for charges to be laid.

Jarryd Dunbar (7.26)
So what we're able to do was locate the evidence that was important in this particular matter, primarily in relation to the first victim, whose father had contacted the AFP only about a week earlier, and we were able to recover that evidence from those devices in the field, which then resulted in him being charged with those offences at that time.

Host
When the AFP investigators interviewed Michael, he seemed to have no understanding of what he put his young victims through.

Jarryd Dunbar (7.52)
When he was arrested upon his return to Australia, he made no admissions in relation to any of what had been uncovered on his devices. He denied any involvement in any of the offending, and it didn't really seem that he really cared too much about the impact that it was having on those people that he targeted.

Host
When Michael was identified, the AFP had no idea that their investigation would uncover so many victims. The recorded interactions they found on his devices dated from as far back as when Michael was 18, and continued more or less uninterrupted over the five years until his arrest at 23.

Jarryd Dunbar (8.39)
The number of victims that he targeted, it wasn't just one child or two children, it was hundreds of children across the world. We were able to identify 54 of those children, we identified about 110 social media accounts that he'd had contact with. Around 330 instances of anonymous chat on different platforms with different children over the space of a number of years.

Host
The images and videos Michael coerced children into producing and sending him were mostly boys aged 10 to 14, but some of the victims were younger than that. Federal Agent Brendan Hayler had just joined the Child Protection Operations team and Operation Ascalon would be the first investigation he ran.

Brendan Hayler (9.27)
After coming to Child Protection Operations in the AFP, I was allocated this operation, this job. So I took it on, and it was the first one they'd given me to run myself. And it turned out to be quite a big one in the end. So it was a really good case to learn a lot, a lot on, and yeah, really get a good grounding in child protection.

Host
When the team examined the contents of his electronic devices, it became clear how Michael had targeted the boys.

Brendan Hayler (9.55)
When the job came to us, it was a referral from a young person and um, he'd gone to his father and told him what had happened. And his father was pretty cluey and they captured the whole conversation from the first introduction straight through to when they reported it to police.

Host
When Brendan's team examined the script, they could see how it had been refined and used over many victims.

Brendan Hayler (10.17)
Once we'd gone through some of his devices and found all these other conversations that had carried on previously using that first script as a bit of a roadmap or a guide, I guess, sections of conversation that we were able to find that he'd saved or captured inadvertently, you could match them up pretty closely almost to this script that we had. It was a really good roadmap to show where they were up to in the conversation with these other victims. And it was consistent across so many different conversations that he'd had, that we started to realise that he'd really developed quite a sophisticated method. He had his procedure for how he went about collecting this kind of material.

Host
The members of Operation Ascalon began examining all the material that Michael had saved onto his computer. There were 110 different boys and aside from the first victim who had come forward, the AFP didn't know who the others were. They began the huge task to try and identify all the victims. As the Team Leader of Child Protection Operations, Jarryd Dunbar had other AFP experts he could call on.

Jarryd Dunbar (11.28)
From that point on, we then need to look at those devices more holistically, which can take weeks, months, or potentially years, depending on how much material there is. In this circumstance, after the examination was completed, which the initial examination is conducted by our digital forensics experts to look through electronic evidence and draw out electronic evidence for us to review. And then it then falls to the case officer and the investigators to look through all the files that are located on these devices to identify any child abuse material, and then to look at that child abuse material to determine what its relevance is to this particular investigation, but then also whether or not there's any other victims that need to be identified.

Host
One of the experts called in by Operation Ascalon was Jimmy Aitken. Jimmy is a Criminal Intelligence Analyst in Child Protection Operations. His team was tasked with examining Michael's electronic devices and analysing the crime type.

Jimmy Aitken (12.22)
Following the arrest of the offender, the team reviewed the offender's electronic devices, and it was only then that the true extent of these crimes became apparent.

Host
In the analysis of the child abuse materials, Jimmy sensed an element of 'gamification' about the way Michael approached his victims.

Jimmy Aitken (12.41)
The criminology of it all is extremely fascinating, but we can't get inside the head of an offender, so all we have to go on is what the offender tells us after they're arrested, or by the actions that they've taken, their modus operandi. So, it's possible that what started as the offender's pursuit of sexual gratification, gradually morphed into somewhat of a game for the offender. His ability to pursue and influence victims, gain leverage over them, and then exert his power and control; all these elements seem to be gamified, achievements to be unlocked. It's not clear whether the offender perceived his actions for what they actually were, which was child abuse, or whether in his mind he perceived the victims to be a commodity, something to be won and collected like a sick game of Pokémon Go. In real life, the offender was someone you would pass on the street without even noticing, but on the internet, he felt powerful and important, and in control, despite the fact that he was exerting power over the powerless, taking full advantage of sexuality, shame, and the vulnerability of children.

Host
It became clear to the investigators as they unravelled the extent of Michael's offending, that he was much more than just a sex offender, preying on young teenage boys. He was also sadistic in the way he treated his victims. Jarryd explains how Michael wielded that power.

Jarryd Dunbar (14.17)
In child sexual abuse matters, there has to be some kind of sexual attraction to children. There's other elements that go into it as well, and there was a certain attraction to the power that he was able to exert over these children. Essentially at any point in time, he could contact a child and say, you need to go and do this. And if they didn't do it, there was going to be a consequence for it. So that ability to be able to control a child's life remotely from somewhere else, anywhere in the world, the power of having that control over the child, I think was a significant motivating factor for him. It elevates him into a different type of offender, in the sense that it makes them more dangerous. It essentially allows him to control their lives and he's almost a puppet master. He has full control over what they do, when they do it, and how they do it, and if they don't do it, then there's consequences.

Host
It was also part of Jimmy's brief to use his tradecraft in the identification of the child victims.

Jimmy Aitken (15.17)
Brendan and the team reviewed hundreds of dreadful images and messages, noting down information that could be used to identify or locate these child victims. But for the majority, the information was pretty sparse and all we had to go on was a social media username. So as the criminal intelligence analyst assigned to this case, it was my job to leverage my intelligence tradecraft, pretty much exhaust every opportunity in an effort to identify and locate these victims.

Host
Part of the analysis that Jimmy did was look at ways to identify the boys featured in the 1600 images and videos that Michael had on his computer.

Jimmy Aitken (15.58)
For most victims, we only had a single piece of information to go on to identify or locate them, which is a social media handle. Some were much easier to find than others using parts of their real name or their initials or year of birth or their town in their username, making it quite easy to find them, relatively. Others were much more difficult to find so, many had locked down profiles, closed friends lists, or use nicknames or pseudonyms when they were online. So locating these children was really essential to figuring out a real world identity for these kids.

Host
Also working on the task of identifying the victims was the AFP's Victim Identification Team. It is their job to closely examine images and videos to identify clues to try and find each victim. AFP member, Kirsty Clarke is a Victim Identification Case Officer.

Kirsty Clarke (16.58)
The Victim Identification Team focuses on identifying victims depicted in child abuse material. So that includes videos or images. It includes the physical and sexual abuse by hands-on offenders or material where the victim has been groomed into producing the sexually explicit material.

Host
And this is what Michael did. He was very good at getting his victims to produce sexually explicit material and send it to him. The Victim Identification Team set about looking for clues in the images. Kirsty explains how the team goes about the identification process.

Kirsty Clarke (17.41)
We use a specialised software designed for victim identification specialists to start viewing the images and the videos to start looking for clues. At this point in time, it's really about putting all of the pieces of the puzzle back together. To find these kids, we would start viewing the videos, looking for languages or accents, names, or background noises like radio programs, to try and find what country that child is in; looking for things like clocks or power points to try and indicate a country. And we also start mapping the children in the rooms as well, say, looking for objects, such as bedspreads toys, pyjamas, clothing, and these start giving us an opportunity to try and find out where those objects are sold. In this particular case, the Victim Identification Team looked at a t-shirt a victim was seen in. We did some research on that particular shirt and saw it was sold at Target, but it was only sold at Target in the US so we were able to refer that victim over to the United States, to their Victim Identification Team, to find that victim within their country.

Host
Part of the challenge was linking images over a number of Michael's devices.

Kirsty Clarke (18.58)
Before we start connecting the social media accounts, it's about building that intelligence around the victims, to see where they're located, and we did start seeing those connections between the social media accounts. So, whilst all of this analysis is happening, we start to group the victims together to make sure we have all the abuse imagery of the child. So, for example, we might find the abuse imagery on the offender's USB, but then we might find the image of the child in the school uniform on his phone. And it's actually up to the team to try and find these linkages to be able to match this material together. Whilst we have this software to try and help us look at the multiple devices, it really does come down to the manual work of the

team that makes the difference as to whether that child is found. So, we can spend hours comparing moles or freckles or bodily features and other objects, seen in the background.-And it's about the actual experience of that victim identification specialist to make the links between the child and the surroundings. And that will ultimately determine whether that child is actually found or not.

Host
What was unusual about what the AFP investigators found on Michael's computer was he had categorised his victims, storing images of each victim in a separate folder.

Jarryd Dunbar (20.26)
The way he organised his material suggested to us that there was more of a interest in the power that it gave him over the victims, that he was able to store that material in such a way that he could use it if he needed to later on down the path.

Host
As the evidence was examined, it was the job of investigators to find out how Michael had targeted his victims.

Jarryd Dunbar (20.47)
He took on the persona of a 16-year-old female that was based in the UK, and he had images of a person who was roughly around 16 years of age to try and legitimise his online presence. And what he would do is he would contact the child through Facebook or Instagram, and would send them a friend request. So like most people do, send through a friend request to people that you know, in this particular circumstance, a lot of those children obviously never met this 16 year old girl before, but the curiosity factor was enough for a lot of these boys to accept those friend requests and immediately he would engage the child in just general conversation before sending images of himself being the 16-year-old girl, that he had a bank of images of this 16-year-old girl that he would then send. So they would start with a facial picture and then it might be a picture in the mirror of wearing just underwear, but enough for the child to believe that he was who he said he was. And that he was willing to produce and provide images to that child that were sexualised, that would encourage the child to then produce those images themselves and send them back thinking that they were sending the images of themselves back to a 16-year-old girl, not a 23-year-old man.

Host
To connect with his victims, Michael would research them through their social media profiles. The unsuspecting teenaged boys were quick to engage with the personable teenaged girl who seemed to be connected to other people they knew.

Jarryd Dunbar (22.18)
He'd also do a fair bit of research into the victims that he was targeting. So, through social media, as we know, once you're accepted as a friend on Facebook or you're accepted as a follower on Instagram, you're able to see that person's profile. You're able to see who they're communicating with, potentially where they went to school, and their family circles and their friendship circles and things like that. So he was able to legitimise his connections with these children, which I guess broke down that initial suspicion that a child may have regarding this individual that had contacted them on Instagram, and allowed them to feel more comfortable in talking to him and providing him the material that he was asking for. I think there's a perception out there that grooming occurs over days and weeks and months, and yes, that does

in some circumstances, but in this particular circumstance, because of the persona that he had built, and the manner in which he engaged with these children, he was able to build that confidence in the child within a matter of minutes and hours, to the point where that child felt comfortable to send naked images of themselves, or later on images of themselves involved in sex acts to him.

Host
The mutual exchange of images happened, and then in his guise as a teenaged girl, Michael would quickly become more demanding. He wanted more pictures, then videos of the boys. If they refused or grew suspicious of what they were being asked to do, Michael threw aside any gentle coercion and instead, threatened the young victims. And if in the beginning, the boys felt comfortable sending images on platforms where the image could be viewed once and then disappear, they soon found out that Michael was saving and storing those images.

Jarryd Dunbar (24.05)
What he was doing was using screen capture software as well, to then capture those images as they were being displayed on the screen. He'd then save those images and then use those images to blackmail the child later on, to produce more images. So it wasn't that he pretended to be this 16-year-old girl the entire time, to get to a point where either the child became suspicious they weren't talking to a 16-year-old, or became suspicious they were actually talking to a male as opposed to a female and would try to cut off the conversation or try and back out of the private conversation they were having. It was at that point, that he would reveal himself as a male, and then threaten the child to produce more material. And the threats involve things such as disseminating those images and videos the child had already produced to friends and family and other social media contacts, which essentially motivated the child to produce more material.

Host
In going through the child abuse materials on Michael's devices, Criminal Intelligence Analyst Jimmy Aitken could see the threat the victims faced, every time they went to their computer.

Jimmy Aitken (25.13)
For these child victims, the threat of their intimate images being released and the demand from the offender for more compromising images, it didn't go away. The threat was always there, always present like a dark cloud hanging over their heads, a cloud that only they could see. So herein lies the problem. Social media is everywhere and it's nowhere at the same time. It's not a physical place, but it exists everywhere that you go, wherever you go. So it transcends not only geography, but also time. Even when you're fast asleep, networks are always buzzing with millions of people interacting at full volume. There's no pause button for the internet. It simply does not sleep. So for these victims, no matter where they were or what time of day it was, they had those threats, that dark cloud hanging over them. Nowhere felt safe, not even their own homes or their school. So when your worst fears could be realised on the internet at any time, where on earth could you hide?

Host
In the beginning, Michael put more effort into building fake profiles. After a while, he realised he didn't need to do that. Case officer Brendan Hayler could see the refinement in his grooming techniques.

Brendan Hayler (26.29)
In the beginning, his Facebook profiles would have a profile picture and then like a real name. And then there'd be some posts and some, some images in the gallery to make it look like this person was legitimate. And maybe even friend a few different people, that kind of thing. By the time it got to us, the username of the account he'd used to speak to this young boy was basically just a few letters jumbled together. No profile picture and no posts or anything like that. It was really just a blank set up Instagram post and a couple of ones he must've used before that work was similar. So he went from trying to set up these really convincing, fake profiles to lure these young boys into talking to him, to the point where he realised that as long as he had a functioning account, he could reach out to whoever he wanted and then try and entrap them.

Host
In the first instance, Michael would ask for a picture of the boy's face which seemed like an innocent enough request to the boys. But there was a sinister reason behind this.

Brendan Hayler (27.30)
He had his method; he had his little script that he'd use, and he'd give the boys compliments to make them feel, I guess, safe or to encourage them, and he'd get a picture of their face if he could, cause that's something that, again, in the cyber safety it's, don't show your body that kind of thing, but a picture of your face, it seems quite normal and quite innocuous. But then once he had a picture of their face, he could identify them to their friends.

Host
Brendan and his team pieced together the web Michael would weave as he friended people connected to the victims on social media.

Brendan Hayler (28.06)
We understood pretty clearly how he would interact with individual victims. I would often see when there was one victim, he'd either be chatting to friends of that victim or there would be other victims, being chatted to at the same time. So, there were kind of in loose friendship groups, but at the same time, he carried on chats with people around Australia and also overseas in like New Zealand and the US and Europe. He'd friend one kid who might accept him and then use that to try and hit up other kids and he'd build a bit of a network and then he'd go through their profile and see who they're friends with and then maybe start matching with them. And then just slowly like work his way through people's friend groups and social networks to move from essentially school to school, from family to family and around the state. When I spoke to a couple of victims, they would commonly say that, 'I saw that my friends were friends with him already, or my cousin or whatever, so I thought it was okay to accept that person's request.'

Host
With the propensity for online offenders to arrange to meet their victims in person, Brendan and the Operation Ascalon team searched for evidence to see if Michael had done this.

Brendan Hayler (29.11)
One of our concerns was whether these conversations had occurred online only, or whether he'd moved into the realm of meeting up with kids and trying to offend against them in person. From looking through all the evidence and reviewing everything and speaking to the children themselves, it didn't ever seem like that was something he was planning to do at least through

this method that we detected. His persona would be this 16-year-old girl, and he would say he either lived in Perth or that he lived in the UK. It was a way of saying, 'Oh, we can't meet up.' Nothing that I saw ever looked like he was trying to pivot it into a real-world interaction.

Host
In one way, Operation Ascalon was the reverse of what usually happens in an investigation. Usually, the child victim makes a disclosure, has a conversation with their family, then the police are alerted. With Ascalon, the AFP was approaching parents with the news that their child was a victim.

Brendan Hayler (30.11)
Sometimes it's more common that there'll be a disclosure by a child, and then the police will investigate that. So, they're working, kind of, with a family who is aware of disclosure, or the child's come forward to somebody about it. So especially with this job is that we are going to people who, where this conversation hasn't necessarily happened, and we're telling them what's happened to their child. And then speaking to the child about something that they haven't themselves necessarily spoken to somebody before about.

Host
Because of this, Brendan had an unenviable task.

Brendan Hayler (30.42)
I would go and knock on the door, speak to parents and say, 'Look, I'm from the AFP. A very delicate situation saying that your child has been essentially abused online. The other tricky part of it is, you want them to speak to their child about it, and ask them if they want to be interviewed or participate with police in trying to you know, do an interview and collect some more evidence. So you can't say too much to the parents about what you know, because you don't want the child's memory to be tainted and you're kind of thinking of it from that aspect. And I think a lot of parents weren't really interested in the details either. They were just concerned about, you know, the welfare of the child and the fact that they had been exploited online. It was a difficult conversation to have on people's front doorstep. It's the last thing they were expecting.

Host
How did the victims feel when Brendan spoke to them?

Brendan Hayler (31.26)
They felt embarrassed about being tricked. They were also very open, honest with us and we'd ask them how they felt once they were starting to be exploited in the conversations and, you know, they would honestly tell me that they were feeling scared, embarrassed, frightened, all that kind of stuff, so.

Host
Brendan spoke to 21 families around Australia, resulting in 11 children agreeing to provide a formal interview to police. While technically, the law sees self-generated material created by people under the age of 18, as child sexual abuse material or illegal content, the boys coerced and blackmailed by Michael were victims of online child exploitation. In cases such as this, victims may be manipulated into believing they have done something wrong and will be punished by their parents or carers, or even prosecuted by law enforcement.

Brendan Hayler (32.24)
The first thing in their mind was that they were speaking with a police officer. They were speaking about something they'd done online, that they um, were tricked into doing, but they felt shameful and embarrassed about. We were there to charge someone with child abuse material and sending it. And in these talks that they, you hear about sending pictures of yourself over the internet as a child is the wrong thing to do. So when the police come to speak to you about you doing it, I think in the back of their minds, they were always worried that they were in trouble. So that was something that me and the other officers reassured them about that they weren't in trouble for what they'd done and that it wasn't their fault.

Host
Getting these interviews right would forever give the boys the message that the police are there to help them, no matter what the circumstances.

Brendan Hayler (33.08)
In speaking with them, you need to bring a level of humanity and personality to speak with them and make them feel comfortable and supported. We don't wear uniforms when speaking to young people, but they are always aware that they're speaking to a police officer. And it's bringing your own experiences and your, yourself, your personality into the job like this, so you can make an impact on these kids in the short time that you have with them to try and reassure them, make them feel safer, make the police somewhere that they had as a good an experience, I guess, given the circumstances so that in future, when anything happens, that they can feel safer approaching police and speaking about it, knowing that they'll be valued, treated with respect, and understood.

Host
A lot of online offenders try and establish a connection with their child victims. What made Michael's offending so unusual was that he dropped all pretence very quickly.

Brendan Hayler (34.03)
They're also, I guess, trying to be their friend in some way, to get them onside. It's part of the grooming. Whereas in this matter, really once the offender got one or two pictures of the child, it just went just straight into the extortion and the threats to get more out of them. It just became about eliciting the material, rather than trying to pretend that they were this person any longer than they really needed to be.

Host
If they didn't send more images, Michael threatened to share the images they'd already sent with their friends and family. And on occasion, he made good on that threat.

Brendan Hayler (34.41)
Yeah, once he got something that he could basically blackmail them with, then he didn't need to keep up this charade. He didn't need to keep up this, 'Oh, you know, I think you're really attractive.' He would stop saying things like that. And just go into the, 'Do this. Send me this video or else I'll share what you've already sent me with your friends and your family.' And he did. I've got statements from family members where images of their son or their brother or whatever was sent to them. He sent one video to a nine-year-old girl who was the sister of one of the boys. And that formed one of the charges. Luckily, she didn't see it. Her parents monitor her social media, so they saw it before it went to the young person, but the offender sent it to that Instagram profile knowing it was that the nine-year-old sister of one of the boys.

Host
Michael was so confident he would never be caught, he boasted about it to his victims.

Brendan Hayler (35.33)
In one of the um conversations as well, he kind of mocks one of the boys where he says, 'You think I'll be caught? The police don't know how to catch people like me.' And said basically that he was untouchable and that the police would never be able to find him.

Host
But all it took was one phone call from a concerned father to bring Michael down. Like all the members working on Operation Ascalon, it wasn't lost on Kirsty Clarke that when the first victim's dad came forward to the AFP, the abuse of many children stopped.

Kirsty Clarke (36.06)
As a result of the original victim speaking up, he's really directly contributed to saving many more children from further online abuse. The victim's dad did everything when his son came to him about the abuse that he was enduring. They first preserved the data; so they took screen captures of the blackmailing, and they didn't alert the offender at this stage. He quickly reported the matter to the AFP. And most importantly, he kept calm and he openly communicated, and this allowed his son to tell him exactly what was taking place. So, there's the clear and open communication between a parent and a child, allowed the victim to have the courage to come forward. And it not only stopped his extorting, but it also stopped the extortion of so many more other children around the world.

Host
Once that first victim came forward, Michael's boasting that he couldn't be caught, was quickly proven false. Even though he had made fake profiles on social media in order to target his victims, the AFP have ways to trace offenders like him, then track them down and arrest them. And when victims are located outside of Australia, the AFP can call on other law enforcement organisations like the FBI for assistance. Case officer Brendan explains how the police rely on the cooperation of social media operators to assist them.

Brendan Hayler (37.38)
We definitely have ways of identifying people online on these social media platforms. The bigger ones are pretty cooperative with police, and they have the information that we need, the subscriber details, that kind of thing. We were fortunate in this investigation, we had some um liaison with some US law enforcement officers who helped us collect that information in a faster manner, which allowed us to identify a lot more of the victims. The internet community is open or aware of these issues and they are doing things to prevent it. The social media giants have avenues and they have processes for dealing with this material when it becomes known to them. If you're on the internet, you're not invisible. We can find you.

Host
The harsh reality is that child abuse material is shared around the world. Images and videos are swapped and traded online. When an offender's computer is forensically examined, typically, police find images they've seen before. Jarryd explains how the material is stored centrally so international law enforcement can access it in investigations.

Jarryd Dunbar (38.47)
All the material that's collected by law enforcement around the world goes onto an international database, which is managed by Interpol. So if the material is first-generation material, it hasn't appeared on that database before.

Host
Michael was producing that first-generation material. All of the child abuse material he possessed, he had generated himself. As case officer, Brendan needed to classify the images as he prepared the case for court. For the AFP investigators, new material means there are new victims to identify and try and locate.

Brendan Hayler (39.25)
A lot of the material that we get has been around for a while and is collected and shared and sent. We're always on the lookout for original material and we have some programs and other ways of detecting what might be new material. And this instance, it looked to me pretty quickly like it was, so then the investigation shifted a little bit, from just classifying the material and producing a brief into kind of investigating what this offender had been up to and the extent of it.

Host
With the work of the Victim Identification Team, the investigators from Operation Ascalon were able to identify a large number of the victims which meant they could take a really strong case to court.

Brendan Hayler (40.08)
In a lot of these cases in child abuse material, you'll often get a plea pretty early on. It's really important when we do our brief of evidence, when we put something towards the court, that it encompasses all the offending that we've identified to give the court a really clear understanding of what this matter is about, so that the court has the best information to deal with them as they should. To come out with 54 charges that he pled guilty to and was sentenced on was a good outcome. That's all down to the work that our intelligence did, victim identification and everyone who worked on the job. You know, you apply yourself and you can get really good outcomes like this.

Host
For Criminal Intelligence Analyst Jimmy Aitken, Michael exploited the two things teenagers feel especially vulnerable about: sexuality and shame.

Jimmy Aitken (41.01)
Think back to when you're a teenager, when we were all teenagers; times were tough, right? It's a period of life where you're super awkward. You're coming to terms with your own identity. You're unsure of yourself and everyone around you. Sadly, for these kids on top of all of this growing pains of teenage-dom, they were subjected to some abhorrent manipulation. So, for most of us as humans, the most powerful emotion that we can feel is shame. And typically, the most vulnerable part of our personal identities is our sexuality. The offender deliberately exploited these most vulnerable parts of the human psyche, the parts associated with sexuality and the parts associated with shame. Sexuality and shame aren't topics that adults rarely talk about, let alone young people. So, it's the shame that led most victims to keep their abuse a secret from their loved ones, meaning that they were processing the trauma of these experiences all alone and trying to figure out a way out of this situation all alone as well.

Host
The online abuse left the victims to try and deal with a sadistic sex offender on their own.

Jimmy Aitken (42.10)
It's hard to imagine the stress that these kids were under. Without someone to talk to, they were really just talking to themselves in their own heads. I would imagine them bargaining with themselves and weighing up their options. They might ask: how can I stop this? Maybe if I do what they want, they'll finally leave me alone. Can I tell my parents? How will my parents react? Maybe I'll get in trouble. Again, it's very hard to imagine what these kids were going through.

Host
Jimmy had some insight into the distress the boys felt in keeping their secret.

Jimmy Aitken (42.45)
On a personal level, I can somewhat relate to the distress that comes from keeping secrets from those that you love the most. I'm now a member of, a proud member of the LGBTQI community, but once I was an awkward closeted gay teen coming to terms with my own identity. And it was the feelings of secret shame that made my teen years much harder than they needed to be. When you're keeping a secret from your family, everything good in life kind of has a bittersweet tone to it. For example, even a warm hug from your mother, a warm embrace from your loving parent, instead of you feeling loved, like you should, there's a seed of doubt in your mind. And that internal voice saying, *they say they love me, but if only they knew*. It's a terribly lonely place to be. We want kids to feel safe, to talk, to have their story heard without judgment, um, because every child really deserves to be loved and to feel safe, especially in their home.

Host
While he was offending, Michael kept up a regular job, and had friends and family. None had any idea of what he was doing in his online life. Offenders like Michael become expert at hiding what they do.

Jarryd Dunbar (44.02)
He had a job. He had relationships. He had friendships. He had a very loving family. He was very much engaged in his life. He certainly didn't come from any level of disadvantage. His age and his upbringing and, and his level of social interaction with other people, was quite unusual.

Host
Some children had an ongoing fear of Michael. Not all victims felt comfortable speaking to police or reliving what had happened to them. They were not required to participate in an interview.

Jarryd Dunbar (44.38)
He had been able to identify enough information about their personal circumstance, about their life, about their family, about their friends, where they went to school, who they hung out with, where they went to on weekends, holidays they'd had, enough personal information that a child felt genuinely scared that he knew where they lived. And that was that fear factor that he instilled in these children that silenced them.

Host
It took months to build the case against Michael. Every chat had to be documented, every interaction had to be transcribed to build the case for court.

Jarryd Dunbar (45.12)
For a case like this, even though there was not a huge amount of material, there's only 1600 images and videos, that's probably the part of the case that takes the longest, going through all the material. So we had to go through each of those chats and transcribe them, identify where images and videos had been produced, how many of them had been produced for each child and what offences he had committed against each child. So in online offending there's a variety of different offences that can occur. Anything from indecent communications with a child, through to grooming, through to procurement a child for sexual activity, and then your straight child abuse, possession, transmission, access offences. So, we have to go through all that material and identify where those specific offences lie.

Host
Even in the face of their obvious distress, Michael showed no mercy for his victims. This was most obvious as the case came together.

Jarryd Dunbar (46.11)
There was never anything within any of these communications with these children that suggest that there was any kind of concern for how these children may react. There was children that were begging him to stop, that were crying when they were performing the acts that he was asking them to do and trying to find any way that they could do something else that would mean that they didn't have to do what he was asking them to do, and it didn't matter to him. He just wanted what he wanted, and he just wanted them to perform the acts that he wanted them to do. There was never any hint that he really cared what impact that was having on the child.

Host
Once the case got to court, Michael pleaded guilty to all charges. He was sentenced to almost ten years in jail for what the judge described as his 'cruel and relentless' manipulation of children and teenage boys. Every case where children are targeted online, teaches AFP investigators something more about the way offenders find their victims. What lessons did the AFP learn from Michael? For Jarryd Dunbar, it was that offenders can be anybody.

Jarryd Dunbar (47.26)
For me personally, and when this case came about, I'd only been in the area for about six months, and it's an area where I say anyone that comes into this area, it takes at least a year, if not a year and a half to two years to get a firm understanding of how this environment works and how these offences are committed, and where the vulnerabilities are for children online. So for me, I came in with that naive perception that a lot of these offenders were older offenders, and this is what I expected, and then along came a 23-year-old, who at that point in time, since I'd been in the team, was probably one of our most prolific offenders, that had victimised such a large number of children. But it's not something that I would expect to have, have experienced, for someone of his age and his upbringing as well. So I think what this case teaches us as is that that the offender can be anybody, and it might be the person you least expect.

Host
There is a perception that crimes that occur online, don't have the same impact as physical based crimes. But for the boys who were targeted by Michael, they experienced a huge breach of trust. They trusted their interaction with the girl, only to find out that all their online communications had in fact been with a 23-year-old man. They knew images of them were in cyberspace and there was no telling when they could resurface – Michael made sure they knew that. Not only did the boys lose trust in the online community, but they also perhaps came to doubt their ability to protect themselves.

Jarryd Dunbar (49.12)
They go through the same range of emotions that somebody who has been the subject of physical offence does, so they become withdrawn. It may lead to substance, alcohol issues, mental health issues. It's all the same reactions that somebody who has been physically contacted offended against.

Host
This means seeking help and counselling is really important for victims. What message does Jarryd want to send to anyone thinking of offending online?

Jarryd Dunbar (49.41)
In this crime type, every law enforcement officer I've dealt with has the same level of dedication. So, there are law enforcement officers everywhere in the world right now, looking for you. And one day they will find you.

Host
Parents are at the frontline of child protection. What can they do? What can they look out for? Kate Laidler is one of the most experienced AFP officers from the Victim Identification Team. She has some advice to offer parents to help protect their kids online.

Kate Laidler (50.17)
My one piece of advice is education is the key to keeping your kids safe. And those lessons and conversations need to start early on. The youngest child we've identified who produced material of themselves and uploaded it to the internet was four years old, so we need to be having those conversations about staying safe online, and at that age, preschool, sort of early primary school age, really simple, and only a few amount of rules, but it needs to start that early. So as soon as they're given access to the internet via a device, they need to be taught about being safe online. You need to develop that family environment where they're going to come forward and they're going to trust you so when something big happens, they know that they can count on you to listen, to believe them. And the final piece of advice I would give is don't threaten or actually take a device away. If you take a phone away from a teenager, that's their life. This is how they live. They make social connections. They organise plans with their friends. And if they think that by coming forward and admitting to an issue online, that you are going to take the device or the access away, they won't come forward. We just need to reassure them that no matter what, we're here, we'll support and help you, but don't threaten to take those devices away because that may make them reluctant to come forward.

Host
Jimmy Aitken feels that diversity is integral within the AFP, especially in Operation Ascalon.

Jimmy Aitken (51.48)
Everyone in the AFP's travelled their own journey and has their own story. And the strength of the team comes from the diversity of each of our experiences and backgrounds and what we bring to the job. For example, I come from a culturally diverse family; both my parents being migrants, and I never would have thought that one day I'd be using my deep knowledge of Filipino culture to solve crimes and save children a world away. I'm lucky enough to be currently steering the government's strategic direction in tackling live online child sexual abuse here in Australia and overseas in the Philippines. And my tiny Filipino mother could not be prouder. I am a member of the LGBTI community. Those of us in the community have had to reconcile our identities against the expectations of wider society. We truly know ourselves and have gone through some adversity, so just by existing, we really show how resilient we are as a people. I never thought that I would be in a police force as a, as a LGBTI member, but I am, and I'm not only surviving, but I'm thriving. Through my journey to coming out, I've developed a mental fortitude, which has really served me well in the police force.

Host
Victim Identification Case Officer, Kirsty Clarke describes her job as the worst job, but the best job. They know that when they examine images of shocking child abuse, they have a chance to stop it. Kirsty says sometimes, the AFP is the only one looking for the children featured in the images.

Kirsty Clarke (53.31)
One of the main things that motivates us is that we know that we might be the only opportunity for that child to be found. For some victims, they may not feel like they have a voice. And for us, we may be the only person that witnesses that abuse and we can do something about it. That's what motivates me to keep looking for clues within the actual imagery that we're looking at.

Host
In the past, offenders with a sexual interest in children had to move among the community, find jobs that would give them access to children, and groom their victims in person. Cyberspace has changed this completely.

Jarryd Dunbar (54.12)
The online child sex offender is basically a chameleon. They adapt to the environment; they change their appearance. They try to anonymise themselves in such a way that it becomes easy for them to target as many children as they can. And all it takes is for somebody who has a smartphone, they don't need a particular type of computer. They've got a smartphone, they've got a knowledge of how social media works. It can give them access to any child anywhere in the world. It gives them access to a child in their bedroom, which is supposed to be the safest place for a child in their own home, under the supervision of their parents. They are vulnerable in their own home. And that's what makes the online child sex offender a very dangerous individual.

Host
Thanks to the AFP's network of teams dedicated to the protection of children and the identification of both victims and those who prey on them, offenders like Michael can be brought to justice.

Serious crime is getting seriously complex. To stay a step ahead, the AFP is recruiting those with diverse skillsets and backgrounds. Just like AFP personnel Jarryd, Brendan, Jimmy, Kirsty and Kate, and the roles they played in interrupting online sexual child exploitation as part of Operation Ascalon.

After all, it takes all kinds to solve crime. With more than 200 roles across the organisation, in Australia and across the globe, you could help the AFP stay a step ahead too. Consider a career with the AFP.