Journal of Contemporary Criminal Justice

http://ccj.sagepub.com/

Protecting Children From Online Predators: The Use of Covert Investigation Techniques by Law Enforcement

Gregor Urbas

Journal of Contemporary Criminal Justice 2010 26: 410
DOI: 10.1177/1043986210377103

The online version of this article can be found at:
http://ccj.sagepub.com/content/26/4/410

Published by:
SAGE
http://www.sagepublications.com

Journal of Contemporary Criminal Justice
26(4) 410–425

DOI: 10.1177/1043986210377103
http://ccj.sagepub.com
SAGE

Protecting Children From Online Predators: The Use of Covert Investigation Techniques by Law Enforcement

Gregor Urbas[1]

Abstract

As the range of cybercrimes expands, law enforcement agencies develop new strategies for their investigation. One method being adopted by police in some countries is to exploit the same anonymity that criminals use to operate online and engage with actual or potential suspects using assumed identities. For example, police investigating online child grooming may assume the identity of a child or young person and engage in chats or email or SMS communication with a suspect. In some situations they may take over the identity of a real child who has been contacted by a suspected child groomer, for example, if contacted by a concerned parent, but in others they may invent an entirely fictitious identity. Where this investigative technique results in arrest and prosecution, arguments about entrapment, or illegal/improper obtaining of evidence may arise. It is therefore important to clarify the legal basis on which such covert investigations may be conducted and to ensure that the substantive and procedural law that apply enable proper and effective law enforcement while at the same time guarding against improper manipulation of persons using electronic communications technologies. This article explores situations in which cybercrimes such as online child grooming can be covertly investigated and seeks to identify best practice for effective online law enforcement.

Keywords

cybercrime, child grooming, covert investigation, fictitious identity

[1]Australian National University, Canberra

Corresponding Author:
Dr Gregor Urbas, Senior Lecturer in Law, Australian National University, Law Building, Canberra ACT 0200
Email: Gregor.Urbas@anu.edu.au

Introduction

A famous cartoon by Peter Steiner and first published in *The New Yorker* on July 5, 1993 has as its caption: *"On the Internet, nobody knows you're a dog."* This early observation encapsulated what has since become a truism—that online identity is easily manipulated, and that people communicating with each other via email, chat room conversations, SMS, or other electronic technologies can and often do pretend to be someone other than, or at least to have different characteristics from, their real selves. The malleability of online identity is demonstrated even further in the phenomenon of Second Life and similar cyber worlds, where people interact through "avatars," or constructed personas that can be of radically different appearance, age, and even gender than their real owners. Although it is impossible to quantify the degree of misrepresentation about identity and personal characteristics that takes place using the Internet, the potential of exploitation of this facility by criminals is obvious.

Few users of the Internet remain unaware of the phenomenon of fraudulent communications that flit around cyberspace, claiming to be from close relatives of Nigerian ministers desperately needing to transfer large sums of money, or lottery officials notifying winners of their unexpected good fortune, or investment brokers promising quick returns on exceptional share market opportunities, or banks requiring clients to verify their account details, or tax offices needing taxpayer details to process tax returns. For the most part, to the extent that spam filters and other technological protections fail to deal with these emails invisibly, we just delete them manually, resigned to the knowledge that there will be plenty more where they came from. The exercise is time wasting and annoying, but mostly harmless. However, for some more vulnerable victims, or where more sophisticated "social engineering" strategies such as "phishing" are used, the harm from Internet-based criminals can be far more serious. The number of Internet fraud victims, including many who arguably should have known better than to trust such communications at face value, is large.

A particularly concerning area of online offending relates not to financial crime, but to the sexual exploitation of children. A significant proportion of the work of police dealing with Internet crime involves investigating the exploitation of children and young people through child pornography or attempts to make contact for sexual purposes. The latter activity is variously known as child "predation," "grooming," or "luring." It may involve the use of adult or child pornography in the attempt to exploit a child's or teenager's sexual curiosity or to break down resistance or reluctance, but need not do so. Indeed, many examples of child grooming begin with quite innocuous contact, for example, through a chat room with a focus on sports or music that may be of interest to children and teenagers, but leading on to more intimate and sexually oriented communications. Importantly, to gain a child's trust and to establish a relationship that can be exploited toward later sexual contact, offenders often assume a different identity from their own. Most children have been taught about "stranger danger" and have some level of distrust of grown-ups but are far more trusting of others their own age or just slightly older. A very effective strategy, therefore, is for adult

predators to adopt the pseudoidentity of a child or young person when seeking out and grooming their targets.

However, as in the saying "two can play at that game," law enforcement officers have sometimes found it useful also to adopt such pseudo identities in the attempt to identify and catch online predators. That is, they may assume the identity of a child or young person and engage in online chats or email or SMS communication with a suspect. In some situations they may take over the identity of a real child who has been contacted by a suspected child groomer, for example, if police have been contacted by a concerned parent, but in others they may invent an entirely fictitious identity. Noteworthy examples include reported cases where police have used chatroom names such as "[boy's name]_14" or "[girl's name]_volleyball" in online conversations with grooming suspects, clearly suggesting that their users were underage youngsters, and proceeded to arrange physical meetings with suspects who made sexual advances at which the suspects were arrested.

As these examples demonstrate, the Steiner cartoon might equally read: *"On the Internet, nobody knows you're a cop."* Adopting a false or fictitious identity, as is commonplace in covert policing generally, is particularly easy to do online. Where there is a real risk of harm to children—and there are certainly cases in which online contact by a sexual predator has been followed by rape, kidnapping, torture, and even murder—the actions of law enforcement officers are justifiable in principle. However, there are various legal and operational limitations on the use of covert techniques that need to be considered in practical terms. Police have to conduct themselves within a regulatory framework that may limit the extent to which pretending to be a child online yields rewards, particularly if it results in evidence being inadmissible in subsequent criminal proceedings. In some jurisdictions, there may simply be no grooming offence committed unless an actual child is communicated with, so that obtaining evidence of communications with an undercover officer is of little or no evidentiary value. In some legal systems, a defence of entrapment can be raised by a defendant to such a charge, especially where it appears that the defendant was cajoled or coerced into a course of action to which he was not otherwise predisposed. This means that great care must be taken in the way online contact with suspected sexual predators is initiated and conducted, especially so as to avoid interfering with legitimate communication between citizens, including children and young adults.

This article explores these issues by focusing on two jurisdictions which have recently enacted child grooming laws: Australia and Singapore. These jurisdictions exemplify significantly different legislative approaches.

Policing the Internet: Detecting Child Groomers

There have been many cases involving the exploitation of Internet communication by adults with a sexual interest in children, but perhaps the most widely reported is that of former U.S. marine Toby Studabaker, who in 2004 was convicted of abducting and having sex with a 12-year-old girl he met in an online chatroom (BBC News, 2004).

Studabaker groomed the girl through subsequent online exchanges of an increasingly sexual nature and convinced her to meet with him. He traveled to Manchester in the United Kingdom for this purpose, and the two then flew to Paris, staying in a hotel and having sex, before traveling by train to Strasbourg. Studabaker was arrested by German authorities in Frankfurt and extradited to the United Kingdom to face charges of abduction and incitement to gross indecency. He pleaded guilty, and the judge sentencing him, Mr. Justice Leveson, remarked on the content of the online communications that police had found on Studabaker's computers:

> The nature and tone of some of your communications, including the so-called cyber sex, demonstrates that you, then 32 years old, were intent on sexual intimacy with a girl you knew to be 12 . . . Although the internet can be a force for very great good it is not always so and its abuse can slip under the guard of parents who are not aware what their children can get involved in while on the web.

Studabaker was sentenced to 4.5 years in prison. The case raised public concern about child grooming in the United Kingdom and eased the passage of the *Sexual Offences Act 2003* (UK), which added a new offence of child grooming (s15) with a maximum penalty of 10 years' imprisonment (Wall, 2007, p. 125). On his release, Studabaker was then deported to the United States where in 2008 he was convicted by a federal judge in relation to the same conduct on charges of possessing child pornography and transporting a child across an international border for the purposes of sexual exploitation, this time receiving a sentence of more than 11 years in prison (Bowcott, 2008).

More recently, in South Australia, a middle-aged offender was convicted in March 2010 of the murder of a teenage girl whom he groomed online using a false identity, posing as a fictitious young musician named "Brandon Kane," and sentenced to life imprisonment with a 29-year nonparole period. The judge's sentencing remarks make clear the grooming methodology so tragically exploited in this case (Kelly, 2010):

> I am satisfied beyond reasonable doubt that it was you who set up and maintained the fictitious websites used to communicate with Carly Ryan. I am also satisfied that you were the author of the vast majority of the SMS communications, the telephone calls, and email traffic with Carly Ryan referred to at the trial in the period of weeks leading up to her death. In particular I am satisfied that it was you and you alone who was responsible for the fictitious Brandon Kane persona and it was that vehicle you used to develop an online relationship with Carly Ryan.
>
> Later, by masquerading as the father of Brandon Kane you inveigled your way, albeit temporarily, into the confidence and trust of both Carly Ryan and her mother sufficiently well to enable you to actually stay in their home for several days in January 2007.
>
> It was a terribly cruel thing to do to this beautiful, impressionable 14-year-old child, I say "child" because that is what she was, in love with the idea of the

> handsome, musically inclined and rather exotic Brandon Kane who spent Christmas in the United States and was coming home via Paris to be with her. The real man instead was an overweight, balding middle-aged paedophile with sex and murder on his mind.

Media reports about the trial evidence suggest that there was a significant period of online interaction between the offender and the victim as well as previous grooming attempts involving other teenage girls in the United States and Singapore and that the offender had been enraged because one of these girls had not met with him in Singapore as had been arranged in their online communications (Fewster, 2010a). (This aspect is of particular interest given the discussion of Australia's and Singapore's grooming legislation below.) The verdict and sentence are reportedly being appealed (Fewster, 2010b). The victim's mother has established a Web site for the "The Carly Ryan Foundation Inc." dedicated to online safety for children, aiming "to create awareness and educate children and parents using the internet [and] to expose the thousands of multiple identities pedophiles use to lure young children" (Fewster, 2010c).

Clearly, cases such as this would have a better outcome if the child groomer could be detected and intercepted before any physical contact with the child victim is made. There are cases in which a vigilant parent or guardian has found out about online communications that a child has engaged in and police have been called and were able to intervene before the child was physically abused. There are also cases in which authorities have been able to detect child grooming in progress because of to suspicions about persons traveling between countries (Brown 2008). In some cases, early intervention has been assisted where a parent or a law enforcement officer, on discovering that a child is being groomed, has been able to "adopt" the child's identity and continue interacting with the groomer, using the child's identity to agree to a physical meeting. Of course, by the time such a meeting occurs, the child is safely out of danger and the groomer is instead met by police, who are able to identify the suspect and take possession of articles he has brought to the meeting, which sometimes provide important evidence of the suspect's real intentions (Karp 2002; Smith, Grabosky, & Urbas 2004, p. 77).

Alternatively, law enforcement officers may proactively create and use fictitious children's identities online, for example, in investigating suspected child groomers in Internet chat rooms. This methodology is now in widespread use in several countries. Increasingly inventive investigators are in some cases resorting to the use of assistance from young people with a sense of civic duty in helping them to master expressions typical of their generation (Towell, 2008). There are now numerous examples from Australian and overseas cases in which police have posed as a child in an online chat room to identify and gather evidence against child groomers (Choo 2009a; Krone 2005a, 2005b).

A problem that arises in many such cases is that prosecutors must prove that a defendant in fact had a particular state of mind at the time of an alleged offence, and the content and tone of the communications involved as well as additional circumstantial

evidence as discussed above can support an inference of intention or knowledge as charged. For example, a prosecutor will find it easier to argue that a defendant intended to meet a supposed child victim for sexual contact if any such proposal originated from the defendant rather than the child (or an adult posing as the child). However, there is a prior and more fundamental problem in prosecuting child groomers in the covert policing scenario in some jurisdictions—if the supposed "child" being communicated with does not really exist and is merely a fictitious identity assumed by a law enforcement officer, then has the offence of child grooming really been committed? This depends critically on the way in which the offence has been defined in legislation.

Cybercrime Legislation and "Child Grooming" Offences

Cybercrime legislation typically sets out a number of offences criminalizing specified, or sometimes quite broad, misuses of computers and telecommunications networks. What are commonly referred to as "hacking" offences are standardly framed in terms of unauthorized access, modification, or impairment in relation to computers, computer data, or computer functions (including electronic communications). In addition, it is not unusual to see broader offences of using computers or telecommunications services (such as the Internet) to commit or attempt to commit some other offence, such as an offence involving fraud or dishonesty, or an unspecified serious offence. In principle, such broad offences—which are in essence preparatory offences constructed on the basis of computer use or misuse—are capable of application to child grooming conduct. However, several legislatures have in recent times enacted specific child grooming or luring offences, rather than leaving police and prosecutors to rely on broader computer misuse offences. There have also been proposals for greater sex offender registration and monitoring (Choo 2009b; Griffith & Roth 2007).

The following analysis contrasts the legislative approach taken in Australia and Singapore, with particular focus on provisions allowing covert policing.

Australia

In Australia, child procuring and grooming offences have been enacted at the federal level with similar offences also found in State and Territory legislation (Choo 2009a; Urbas & Choo 2008). The key elements of the two main federal offences are set out below (Table 1).

For the "grooming" offence, which involves the communication of indecent material, this is defined as meaning "indecent according to the standards of ordinary people." Clearly, this includes both adult and child pornography, the latter also being covered by other specific offences in both Commonwealth and State/Territory law (Krone 2004). Interestingly in this context, it has been held in the recent case of *McEwen v. Simmons & Anor* [2008] NSWSC 1292 (December 8, 2008) that sexual cartoon imagery using animated figures drawn from *The Simpsons* constituted child pornography for

Table 1. Australian Federal Child Grooming Offences

Criminal Code offence	Main elements	Penalty
474.26 Using a carriage service to procure persons under 16 years of age	A person (the sender) uses a carriage service to transmit a communication to another person (the recipient); and the sender does this with the intention of procuring the recipient to engage in, or submit to, sexual activity with the sender (or another person, or in the presence of the sender or another person); and the recipient is someone who is, or who the sender believes to be, under 16 years of age; and the sender (or the other person) is at least 18 years of age	Imprisonment for 15 years
474.27 Using a carriage service to "groom" persons under 16 years of age	A person (the sender) uses a carriage service to transmit a communication to another person (the recipient); and the communication includes material that is indecent; and the sender does this with the intention of making it easier to procure the recipient to engage in, or submit to, sexual activity with the sender (or another person, or in the presence of the sender or another person); and the recipient is someone who is, or who the sender believes to be, under 16 years of age; and the sender (or the other person) is at least 18 years of age	Imprisonment for 12 years (15 years if the intention includes sexual activity with a person under 18 years as well as the recipient)

Source: Commonwealth of Australia Law (ComLaw): http://www.comlaw.gov.au/

the purpose of both Commonwealth and New South Wales (NSW) offences, where the representations were held to be of "persons" who were recognizably well below the age of 16. In light of s474.27 of the Commonwealth Criminal Code, it might be added that such cartoon pornography may be especially dangerous in the grooming of younger children for sexual purposes.

The two "procuring" and "grooming" offences are followed by further provisions clarifying legal and evidentiary issues with respect to the age or perceived age of senders and recipients, including the following in s474.28 (Provisions relating to offences against sections 474.26 and 474.27). These state that a person may be found guilty even if it is impossible for the sexual activity referred to in that section to take place, that it does not matter that the recipient to whom the sender believes the sender is transmitting the communication is a fictitious person represented to the sender as a real person, and that it is an offence to attempt to commit an offence against section 474.26 or 474.27.

The legislation here addresses the legal position where the defendant has been communicating with, and attempting to procure or groom, a person who is apparently but is not in fact a child under the age of 16 years. In line with the approach taken by the Queensland legislation on which it is based (Krone 2005a; Urbas & Choo 2008), the federal legislation deliberately allows that the offence may be committed even though the offender is communicating with a "fictitious recipient" who appears to be a child. It is not a barrier to guilt that it is therefore impossible for the intended sexual activity to take place. However, the legislation does exclude the prosecution of attempts for these particular offences, presumably in recognition that the offences are already preparatory in nature. This approach allows law enforcement officers, and possibly others, to conduct early investigation and intervention in protection of potential child victims of sexual assault. That this is a deliberate legislative strategy is clear from the Explanatory Memorandum to the Commonwealth Bill introducing these provisions (Australian Parliament 2004):

> Proposed sections 474.26 to 474.29 contain an offence regime targeting adult offenders who exploit the anonymity of telecommunications services (for example, the Internet) to win the trust of a child as a first step toward the future sexual abuse of that child. The practice is known as "online grooming."
>
> There are two steps routinely taken by adult offenders leading up to a real life meeting between adult and child victim that results in child sexual abuse:
>
> 1. The adult wins the trust of a child over a period of time. Adults often use "chat rooms" on the Internet to do this. They may pose as another child, or as a sympathetic "parent" figure. Pedophiles reportedly expose children to pornographic images as part of this "grooming" process. It is proposed to specifically criminalize this practice. Specific offences would remove any doubt about whether online "grooming" of a child before actual contact is "mere preparation" (i.e., not a criminal offence) or an unlawful attempt to commit child sexual abuse.
> 2. With the child's trust won, adults often use telecommunications services to set up a meeting with the child. Although this step is more likely to be characterized as an attempt to commit child sexual abuse than step (1), it is desirable to provide a firm justification for police action by enacting specific "procurement" or "solicitation" offences. This is consistent with the underlying rationale for the new offences: to allow law enforcement to intervene before a child is actually abused.

Note that the terminology adopted differs from the uses of "grooming" in some other countries' legislation and in some academic discussion of child luring or grooming (Akdeniz 2008). At times, the term is used for the activity identified as "procuring" under Australian legislation, or to describe some uses of child or adult pornography in communications with children. However, the legislative intent is clearly to target a form of preparatory predatory activity adopted by child groomers. Indeed, as noted

Table 2. Singapore's Child Grooming Offence

Penal Code offence	Main elements	Penalty
376E Sexual grooming of minor under 16	Any person of or above the age of 21 years (A) having met or communicated with another person (B); A intentionally meets B or travels with the intention of meeting B; and at the time A intends to do anything to or in respect of B, during or after the meeting, which if done will involve the commission by A of a relevant offence; and B is under 16 years of age; and A does not reasonably believe that B is of or above the age of 16 years	Imprisonment for 3 years and/or a fine

Source: Singapore Statutes Online: http://statutes.agc.gov.sg/

above, the drafting of the offences allows that the recipient of communications be a fictitious child.

Importantly, the legislation provides for specific defences where the defendant had a genuine belief that the person he was communicating with was above the age of 16 years (or that another person involved was above the age of 18) in s474.29 (Defences to offences against section 474.26 or 474.27). The defendant seeking to rely on such a defence bears an evidential burden, defined as "the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist" as per s13.3 (Evidential burden of proof—defence).

Singapore

Singapore's computer crime legislation is essentially based on the United Kingdom's *Computer Misuse Act 1990*, which was enacted partly in response to the inadequacy of traditional criminal offences such as "theft" and "criminal damage" to translate to instances of computer hacking (Smith, Grabosky, & Urbas, p. 41). Additional computer-related offences have since been added in United Kingdom statutes, and Singapore has continued to look to these in reforming its own laws (Urbas, 2008). In 2003, the United Kingdom enacted the *Sexual Offences Act 2003*, which includes a provision (s15) titled: "Meeting a child following sexual grooming etc." Singapore's version, found in s376E of the *Penal Code* (Cap. 224), was enacted in 2007, but somewhat differently titled as "Sexual grooming of minor under 16." The main elements of the offence are set out below (Table 2).

The "relevant offences" referred to in s376E are specified as the *Penal Code* (Cap.224) offences of s354 (Assault or use of criminal force to a person with intent to outrage modesty), s354A (Outraging modesty in certain circumstances), s375 (Rape), s376 (Sexual assault by penetration), s376A (Sexual penetration of minor under 16),

s376B (Commercial sex with minor under 18), s376F (Procurement of sexual activity with person with mental disability), s376G (Incest) and s377A (Outrages on Decency); as well as the *Children and Young Persons Act* (Cap.38) offence of s7 (Sexual exploitation of child or young person) and the *Women's Charter* (Cap.353) offence of s140(1) (Offences relating to prostitution) which includes carnal knowledge of a girl under 16.

Because the offence must be committed in Singapore for s376E to apply, subject to some provisions regarding extraterritorial operation of Singapore's laws (Amirthalingam, 2006), this in effect means that the meeting or traveling referred to must be in Singapore. However, subsection (3) of s376E is worded so as to capture conduct that begins outside the country, stating: "For the purposes of this section, it is immaterial whether the 2 or more previous occasions of A having met or communicated with B . . . took place in or outside Singapore." As the Second reading Speech introducing this provision in 2007 made clear, the intention was to capture conduct directed at children in Singapore (Ho Peng Kee, 2007; Urbas, 2008):

Interestingly, the grooming offence in s376E may only be committed by a person of or above the age of 21 years, whereas as the corresponding United Kingdom and Australian provisions apply to persons of or above the age of 18 years (Urbas 2008). Notwithstanding this difference, the intent behind the Singapore offence is, as with the United Kingdom and Australian legislation—to allow preventive action by law enforcement officers. However, like the United Kingdom offence, but unlike the corresponding Australian offences (discussed above), the Singapore offence clearly requires the actual existence of "another person (B)" who is under 16 years of age such that the defendant "A intentionally meets B or travels with the intention of meeting B" to commit the offence. How, then, can law enforcement officers in Singapore conduct an investigation in which they assume the identity of a child?

The question has a number of different routes to a positive answer. First, there is an argument based on the broad provision of computer access with intent to commit or facilitate commission of an offence, found in the *Computer Misuse Act* (Cap.50A), s4 (Access with intent to commit or facilitate commission of offence). This provision applies where a person "causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence," and is thus a broad preparatory computer offence provision. However, this offence is limited in its application by the reference to intended offences involving property, fraud, dishonesty, or causing "bodily harm" and punishable by 2 years or more. Although some crimes of sexual assault on children involve physical harm or injury that might accurately be described as "bodily harm," it is not clear that intended sexual intercourse with a child (as intended by a child groomer to whom this offence might apply) necessarily falls within this designation. Therefore, this would be an uncertain basis on which to prosecute an alleged child groomer who has been in communication with a law enforcement officer pretending to be a child. By contrast, the Australian version of this offence has no such limitation, apart from the requirement that the intended offence be a "serious offence" defined as one punishable by 5 years'

imprisonment, and thus arguably would apply, though the specific child procuring and grooming offences set out above apply more directly: see s474.14 (Using a telecommunications network with intention to commit a serious offence) of the *Criminal Code Act 1995* (Cth).

More promisingly, Singapore's computer offences are drafted so as to allow prosecution for attempts. Under s10 of the *Computer Misuse Act* (Cap. 50A), abetments and attempts are punishable as offences, and the similar provision in s511 of the *Penal Code* (Cap.224) illustrates with a number of examples such as attempting to steal jewels from a locked box which is in fact empty, or attempting to pick a person's pocket which in fact contains nothing. Translating this reasoning to the computer misuse scenario, a person who attempts to gain unauthorized access to, or modify the contents of, a computer, but is foiled by a protection mechanism or law enforcement intervention, may still be guilty of the attempted offence. In the case of child grooming, the suggested analogy is that *A* is attempting to groom a child *B* but *B* does not exist, or is in reality an adult officer. Such a reading of attempt in relation to grooming—which under s376E refers to "another person (B)"—would arguably be consistent with the legislative intent behind Singapore's enactment of the child grooming offence.

Entrapment Issues

In some countries, notably the United States and Canada, a defence of entrapment can be raised in response to a criminal prosecution in which police or others in positions of authority have engaged in "sting operations" of the kind discussed above (Krone, 2005b). In general, what is required for such a defence to succeed is more than the mere fact that officers engaged in deceptive conduct, but some finding by the court that this conduct induced the defendant to engage in criminal conduct of a kind which he would not otherwise have engaged in, and this in turn allows the defence to be rebutted by the prosecution if it can lead evidence of a "prior disposition" on the part of the defendant to engage in conduct of that kind. More broadly, such arguments can operate not only through a substantive defence, but as a basis for excluding police evidence, as a basis for granting a stay of proceedings, or as a basis for convicting on lesser charge and/or reducing sentence. In the United Kingdom, there is no common law defence of entrapment but a prosecution can be stayed as an abuse of process where police misconduct is found (Bronitt, 2002).

In Australia, there is similarly no common law defence of entrapment, but illegally or improperly obtained evidence may be excluded on a "public policy" basis as set out in cases such as *Ridgeway v. The Queen* (1995) 184 CLR 19 and embodied in s138 (Discretion to exclude improperly or illegally obtained evidence) of the *Evidence Act 1995* (Cth). Such evidence may be admitted, but the hurdle to be overcome is in showing to the court's satisfaction that the public interest in admitting the evidence outweighs the public interest in not legitimating the methods used, taking into account a range of factors including probative value, offence seriousness, gravity of the contravention, and whether the impropriety or contravention was contrary to or inconsistent

with a right of a person recognized by the International Covenant on Civil and Political Rights. The High Court has drawn a distinction between cases in which the commission of the crime was itself procured by the conduct of police or others in authority, and those where only evidence of the commission of a crime was thus obtained. There is greater latitude given with respect to covert policing in the second type of case, as illustrated by the recent "fake criminal gang" case of *Tofilau v. The Queen; Marks v. The Queen; Hill v. The Queen; Clarke v. the Queen* [2007] HCA 39 (30 August 2007).

These principles have only recently started to be been explored in the context of Australian child grooming investigations, as the ACT case of *R v. Murray Colin Stubbs* [2009] ACTSC 63 (26 May 2009) illustrates. In this case, the accused had communicated in online chats and by email with "missTufsey14, Roxanne Taylor," represented to be a 14-year-old girl, but who was in reality Detective Stephen Waugh of New Zealand Police based in Auckland. After the communications from the accused became more sexually suggestive and he suggested a meeting with "Roxanne" at the Jolimont Centre in Canberra, the Australian Federal Police (AFP) were informed and an arrest followed. At trial, the accused pleaded not guilty to two counts under ss 474.26 (Using a carriage service to procure persons under 16 years of age) and 474.17 (Using a carriage service to menace, harass or cause offence) of the *Criminal Code Act 1995* (Cth), and raised a number of interesting arguments in support of the proposition that the prosecution's evidence should be excluded as having been illegally or improperly obtained. The first was to the effect that by posing as a 14-year-old girl, the New Zealand detective had breached s 474.5(1)(b) of the Code by causing a "communication to be received by a person other than the person to whom it is directed." This argument was summarily dismissed by the trial judge, Higgins CJ, who held that

> [i]t is clear that the accused, assuming him to be the responder to "Roxanne," could be found to have intended to correspond with that person, in truth being Detective Waugh, but mistakenly believed by the accused to be a 14-year-old girl.

In other words, it is not a breach of s 474.5(1)(b) to assume a fictitious identity online and receive communications meant to be directed to that identity.

A more substantial argument was advanced to the effect that the detective's conduct was improper in the Ridgeway sense, in inducing the accused to develop a sexual interest in "Roxanne" and thereby to commit the crimes charged. In considering this argument, Higgins CJ noted (at [35]—[36]) that the New Zealand police trained officers including Detective Waugh to create Internet "decoy profiles" of children to "track and identify paedophiles who used the world-wide web to target and groom children for sexual exploitation." The police followed a policy and procedure document entitled "Principles of Practice for Investigating On-Line Grooming of Children Under 16," which is reproduced in full in the ACT Supreme Court judgment. This policy is deliberately designed to avoid allegations that police have induced child grooming crimes by adopting the fictitious identities of children and acting as "agent

provocateur." Higgins CJ approached the issue of discretionary exclusion by observing (at [45]) that "whether Detective Waugh counselled or procured the allegedly offending conduct of the accused can only be judged by the content of their interaction." Having regard to this, His Honor concluded (at [53] and [66]):

> In the present case, the police officer, Detective Waugh, did nothing unlawful in pretending to be a 14 year old girl. He did not represent "Roxanne" to be a young person wishing to engage in sexual activity with adult men . . . In my view, there is not demonstrated in this case any breach of Australian law or any impropriety in Detective Waugh's communications with the accused which should be regarded as enlivening the discretion provided for by s138 Evidence Act.

In reaching this conclusion, Higgins CJ raised an interesting issue in regard to the use of "controlled operations" certificates, a mechanism established in Part IAB of the *Crimes Act 1914* (Cth) following the *Ridgeway* case to legalize certain undercover operations and thus remove the illegality basis for discretionary exclusion under s 135 of the *Evidence Act 1995* (Cth). Because undercover investigations of child groomers do not involve obviously illegal actions (such as sending child pornography), it appears that controlled operations certificates are not routinely obtained in this area of policing. Nor, apparently, are assumed identity authorizations required under Part IAC of the *Crimes Act 1914* (Cth), as there are no criminal or civil liability issues involved in the adoption of fictitious online chat identities such as "missTufsey14, Roxanne Taylor." The issue was briefly considered in *R v. Stubbs* (at [62]—[63]), where Higgins CJ observed that in the absence of illegal or improper conduct by the police, such "shield" mechanisms are not required. Instructively, Higgins CJ made clear that even if impropriety on the part of the New Zealand detective could be shown, this would still not have justified exclusion of the police evidence using s 138 of the *Evidence Act 1995* (Cth).

In Singapore, following cases such as *How Poh Sun v. PP* [1991] SLR 220, there is also no common law defence of entrapment, but criminal prosecution is subject to constitutional limitations. In the case of *Mohamed Emran bin Mohamed Ali v. PP* [2008] SGHC 103, it was recognized that although entrapment is not a defence, nonetheless a court will countenance an argument on constitutional grounds that a defendant has been treated unfairly if he is prosecuted but others (covert police) who engaged in the same conduct are not, such as where both the accused and police are engaged in drug trafficking. It is unclear whether this type of argument would make much inroad in a child grooming scenario, where the covert investigators are not engaged in the same conduct (grooming) as the offender.

To date there are no cases reported in Singapore where either police have obtained a child grooming conviction using a fictitious child's identity, or where such a method has been challenged on constitutional grounds. Given the legislative intent behind the enactment of s376E of the Penal Code, it is not likely that this will be a significant area of challenge in relation to child grooming prosecutions in future.

Conclusion

On the Internet, nobody really knows who is a child and who is a cop. Law enforcement officers can exploit this anonymity, much in the same way as cyber criminals, to detect and investigate suspected child groomers. The way in which child grooming offences are drafted can have a critical bearing on how covert policing of this kind of offending can proceed. In Australia, and some other countries, grooming offences have been enacted that make it clear that no real child need be involved. In Singapore, by contrast, the offence requires a real child (under 16 years) to be contacted, but it is arguable that the offence of attempt may be available to allow police to pose as a child online to detect and investigate suspected groomers. Under either approach, it is important that police be able to conduct such investigations in order to prevent serious harm from being done to vulnerable victims. However, they also need to take care to ensure that their actions are not legally challengeable through the application of entrapment or similar defence.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

References

Akdeniz, Y. (2008). *Internet Child Pornography and the Law: National and International Responses*. Ashgate.

Amirthalingam,K. (2006). Protection of victims, particularly women and children, against domestic violence, sexual offences and human trafficking. *Asean Law Association Journal, 17*.

Australian Parliament. (2004). Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004 (Cth), Explanatory Memorandum: http://www.austlii.edu.au/au/legis/cth/bill_em/claoaomb22004739/

BBC News. (2004, April 2). *Ex-marine jailed for abduction*. http://news.bbc.co.uk/1/hi/england/manchester/3594235.stm

Bowcott, O. (2008, April 24). Ex-US marine gets 11 years for abducting girl. *The Guardian*: http://www.guardian.co.uk/uk/2008/apr/24/ukcrime.usa

Bronitt, S. (2002). Sang is Dead, Loosely Speaking—R v. Loosely. *Singapore Journal of Legal Studies, 374*.

Brown, D. (2008, Dec 1). Paedophile Rachata Burasite caught after grooming 13-year-old in virtual world. *Times Online*: http://www.timesonline.co.uk/tol/news/uk/crime/article5266661.ece

Choo, Kim-Kwang R. (2009a). *Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences* (Policy Series

no.103). Australian Institute of Criminology, Research and Public: http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf

Choo, K.-K. R. (2009b). *Responding to online child sexual; grooming: An industry perspective. Trends & Issues in Crime and Criminal Justice* (No. 379). Australian Institute of Criminology:: http://www.aic.gov.au/publications/current%20series/tandi/361-380/tandi379.aspx

Fewster, S. (2010a, April 1). Revealed—The face of Carly Ryan's killer. *The (Adelaide) Advertiser*. http://www.adelaidenow.com.au/revealed-the-face-of-carly-ryans-killer/story-e6frea6u-1225847825217

Fewster, S. (2010b, April 19). Carly Ryan's killer to appeal conviction. *The (Adelaide) Advertiser*. http://www.adelaidenow.com.au/carly-ryans-killer-to-appeal-murder-conviction/story-e6frea6u-1225852661006

Fewster, S. (2010c). Carly's mum is online and helping. *The (Adelaide) Advertiser* http://www.adelaidenow.com.au/news/south-australia/carlys-mum-is-online-and-helping/story-e6frea83-1225826887261

Griffith G., & Roth, L. (2007). *Protecting children from online sexual predators* (Briefing Paper no. 10/07). NSW Parliamentary Library Research Service http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/key/ProtectingChildrenFromOnlineSexual Predators

Ho Peng Kee, Senior Minister of State (2007, January 22). Second Reading Speech of The Penal Code (Amendment) Bill, Parliament of Singapore, 22 October.

Karp, J. (2002). *Imaginary crime yields real time: Man accused of using Net to entice fictitious boy into sex ends up serving a not-so-fictitious sentence*. Tech TV.

Kelly, The Hon. Justice P. (2010). Sentencing Remarks in R v. Garry Francis Newman, Supreme Court of South Australia, No. SCCRM-08-355, 31 March: http://www.courts.sa.gov.au/sent_remarks/sr/0331_newman_garry_francis.htm

Krone, T. (2004). *A typology of online child pornography offending. Trends & Issues in Crime and Criminal Justice* (No. 279). Australian Institute of Criminology: http://www.aic.gov.au/publications/current%20series/tandi/261-280/tandi279.aspx

Krone, T. (2005a). *Queensland police stings in online chat rooms*. Trends & Issues in Crime and Criminal Justice, no. 301, Australian Institute of Criminology: http://www.aic.gov.au/publications/current%20series/tandi/301-320/tandi301.aspx

Krone, T. (2005b). *International police operations against online child pornography*. Trends & Issues in Crime and Criminal Justice, no.296, Australian Institute of Criminology: http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi296.aspx

Smith, R. G, Grabosky P., & Urbas G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Towell, N. (2008, July 10). Youth join fight against online abuse. *The Canberra Times*.

Urbas, G. (2008). *An Overview of Cybercrime Legislation and Cases in Singapore*. Asian Law Institute (ASLI) Working Paper Series no.1, National University of Singapore: http://law.nus.edu.sg/asli/working_paper_d.aspx?sno=WPS001

Urbas, G. & Choo, Kim-Kwang R. (2008). Resource materials on technology-enabled crime, Technical and Background Paper, No. 28, Australian Institute of Criminology: http://www.aic.gov.au/publications/current%20series/tbp/21-40/tbp028.aspx

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Bio

Gregor Urbas is a senior lecturer in law at the Australian National University (ANU) where he teaches in criminal law and procedure, evidence, and intellectual property. His research interests include cybercrime, criminal justice, and victims' issues. Previously, he has been a research analyst at the Australian Institute of Criminology (AIC), most recently working with the Australian High Tech Crime Centre within the Australian Federal Police on cybercrime issues. His publications include the book *Cyber Criminals on Trial* (with Russell Smith and Peter Grabosky, published by Cambridge University Press, 2004), which was awarded Distinguished Foreign Book Prize by the American Society for Criminology, and journal articles on cyberterrorism, cyberstalking, Internet crimes, and online copyright piracy.