Copyright © 2019 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2019. Vol. 13(1): 38–54. DOI: 10.5281/zenodo.3383885
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Online Undercover Investigations and the Role of Private Third Parties

Peter Grabosky[1] **& Gregor Urbas**[2]
Australian National University, Australia

Abstract

This article explores the use of covert online investigative methods by state agencies, and by individuals and institutions in civil society. Our focus is primarily on active investigations of online child exploitation. In particular, we are concerned with two types of investigative activity-- a) an investigator's active deceptive impersonation of a child or of a facilitator of child exploitation, online; and b) techniques of accessing and compromising information systems used for the purpose of child exploitation. While these investigative methods may have a legitimate place in contemporary crime control, they do pose problems. We look first at their potential for abuse by state agencies, and the remedies available to the targets of illegal or otherwise questionable state practices. We then turn to non-state investigators, and note that the targets of private investigation have even less protection. We conclude by articulating some standards by which the propriety of state and non-state covert online investigative activity may be evaluated.

Keywords: Vigilantes, Undercover Investigations, Child Exploitation, Entrapment, Outrageous Government Conduct.

Introduction

Over the past quarter century, a great deal of crime has migrated from physical space to cyberspace. What was formerly achieved with a can of spray paint can now be engineered with SQL injections and file transfer protocols (Balduzzi et al., 2018). Extortion demands, once made face to face, by letter, or through a telephone call, can now be made on line. Extortion payments, previously delivered in a paper bag or briefcase, can now be accomplished by electronic funds transfer (Grabosky, Smith & Dempsey, 2001, Chapter 3). Sexually explicit images of children, once circulated by hand or purchased in seedy bookstores, are now reproduced and disseminated instantaneously, in real time. Adults no longer need lurk near schoolyards to arrange illicit assignations,

[1] Professor Emeritus, School of Regulation and Global Governance (RegNet), ANU College of Asia and the Pacific, H.C. Coombs Extension Building #8, Canberra ACT 2601 Australia. (Corresponding author) E-mail: Peter.Grabosky@anu.edu.au
[2] School of Regulation and Global Governance (RegNet), ANU College of Asia and the Pacific, H.C. Coombs Extension Building #8, Canberra ACT 2601 Australia. GregorUrbas@anu.edu.au

preferring less obtrusive encounters in chatrooms frequented by young people (Davidson & Gottschalk, 2011).

Predictably, a great deal of criminal investigation has also migrated to cyberspace. Cyber forensics, once an esoteric specialty on the margins of detective work, is becoming increasingly central to crime control. Law enforcement agencies around the world are scrambling to keep abreast of their criminal adversaries. Accompanying the activities of state agencies are those of private citizens. Just as police in recent years have invited a degree of citizen "co-production" in conventional crime control through such organizational auspices as Neighbourhood Watch and Crimestoppers, contemporary law enforcement agencies have established online reporting protocols and hotlines. The FBI's Internet Crime Complaints Center (IC3) and the Australian Cybercrime Reporting Network (ACORN) are but two examples (Federal Bureau of Investigation, 2018; Australian Cybercrime Online Reporting Network, 2018; Chang, Zhong & Grabosky, 2018; Cheong & Gomng, 2010).

Throughout history, state police have used covert or undercover methods to complement more visible, transparent investigative techniques. The reasons for this are pragmatic: Certain types of activity, such as serious organized crime and complex criminal conspiracies, are less amenable to interdiction by means of overt, conventional police practices.

Undercover policing has been described as a "necessary evil" because of its potential for misuse. By their very nature, covert methods are subject to abuse and to the avoidance of accountability. One needs look no further than totalitarian states of the 20th century for grim illustrations. But even in democratic states that present themselves as paragons of virtue and champions of human rights, abuses can and do occur (Marx, 1988; Fijnaut & Marx, 1995).

Covert policing is by no means the monopoly of state policing and security services. Private individuals, members of non-government organizations, and commercial entities have all engaged in investigation for a variety of motives, including a sense of civic responsibility, moral indignation, or commercial gain (Fronc, 2009; Tusikov, 2017; Brown, 1997). And just as agencies of the state may transgress the law and avoid accountability for their excesses, so too can non-state actors.

This article explores the use of covert online investigative methods by state agencies, and by individuals and institutions in civil society. Our focus is primarily on active investigations of online child exploitation. The universe of online undercover investigations may be mapped according to Figure 1. On the vertical axis, investigations may be passive or active. Passive investigations, are limited to the collection of information available in locations accessible to the public. Active investigations involve deceptive techniques such as impersonation of a child, or the facilitation of child exploitation online. The horizontal axis differentiates between state investigations conducted by public officials, and private activities undertaken by non-state actors.

We deal in this article with activities represented as taking place in the lower half of Figure 1. In particular, we shall be concerned with two types of investigative activity-- a) an investigator's active deceptive impersonation of a child or of a facilitator of child exploitation, online; and b) techniques of accessing and compromising information systems used for the purpose of child exploitation. While these investigative methods may have a legitimate place in contemporary crime control, they are not without downsides. We look first at their potential for abuse by state agencies, and the remedies available to

the targets of illegal or otherwise questionable state practices. We then turn to non-state investigators, and note that the targets of private investigation have even less protection. We conclude by articulating some standards by which the propriety of state and non-state covert online investigative activity may be evaluated.

It should be noted, of course, that many investigations involve co-operation between public and private actors. For example, police may draw on expertise or information held by individuals or corporations in the commercial world, such as the Microsoft Digital Crimes Unit (Microsoft Trust Center, 2018). Other examples of public-private interaction in law enforcement are plentiful (Ayling, Grabosky & Shearing, 2009).

Figure 1. Typology of online undercover investigation

	PUBLIC		PRIVATE
PASSIVE			
	Police "patrolling"	x	Private actors "patrolling"
	chatrooms	x	chatrooms
	Citizen "hotlines"	x	for reporting anomalies
ACTIVE			
	Police stings	x	Citizen vigilantes
	Undercover impersonation	x	Citizen hackers
	Police hacking	x	Citizen impersonators

1. Investigative Practices by State Agents

Covert investigation may be undertaken by means of various technologies. These can include telecommunications interception, the installation of listening devices, compromising and accessing information systems, imaging, infiltration of a target organisation, active deceptive impersonation, passive observation, and in recent years, "Big Data" analytics (Marx, 2016; Završnik, 2018; Harcourt, 2015).

Whatever the tools employed, investigation may serve a number of objectives. These include the acquisition of intelligence, the disruption of a criminal enterprise, and the collection of evidence for use in a criminal prosecution. This latter concern is the primary focus of our article.

With regard to the collection of evidence for use in a criminal prosecution, the use of technologies may necessitate a search warrant, the specificity of which will vary across jurisdictions. In the United States, whose constitutional foundation was influenced profoundly by the draconian system of crime control during the reign of George III, search warrants must specify in considerable detail the nature of evidence to be sought,

and the anticipated location of the evidence in question. Similar requirements exist in Australia.[3]

In the United States, the abuse of power by government agents did not end with the Revolutionary War. Decades of overzealous policing led to considerable restraints on state power, to the extent that evidence collected by illegal means, from coerced confessions to the fruits of warrantless searches, is generally inadmissible in criminal proceedings. Here we explore two basic principles relating to evidence obtained as a result of questionable practices by law enforcement: *entrapment* and *outrageous government conduct*.

1.1. Entrapment

In *Sorrells v. United States*, 287 U.S. 435 (1932), the US Supreme Court defined entrapment as the "conception and planning of an offense by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the officer." When the defense of entrapment is raised, the government, in order to negate or rebut it, must show that the accused was predisposed to commit the crime. Entrapment, in other words, relates to the state of mind of the defendant. Sorrells, found by the Court to have been "an industrious, law-abiding citizen," had sold a bottle of whisky following "repeated and persistent solicitation" by an undercover prohibition agent representing himself as a fellow veteran of WWI. In essence, the issue of entrapment is a question of fact, to be presented to the jury.

A more recent entrapment case involved a Mr Jacobson, an individual in the US who had purchased a publication containing pictures of underage males at a time when such publications were *entirely legal*. Some weeks later, following the enactment of the Child Protection Act 1984, this type of content became proscribed by law. As part of an aggressive campaign to enforce the new legislation, U.S. government agencies obtained the mailing lists of the bookseller from whom Jacobson had bought the magazine. Over the course of 26 months, the US Postal Service and US Customs Service sent Jacobson repeated overtures from bogus civil liberties and opinion research organizations, urging him to purchase the illicit materials. He finally did so, and was convicted. Jacobson appealed to the US Supreme Court, which found in his favour. The Court held that " …the prosecution must prove beyond reasonable doubt that the defendant was disposed to commit the criminal act prior to first being approached by Government agents" (*Jacobson v. United States*, 503 U.S. 540 (1992).

[3] For example, under s3E(5) of the *Crimes Act 1914* (Cth), a search warrant issued by an officer must state: (a) the offence to which the warrant relates; and (b) a description of the premises to which the warrant relates or the name or description of the person to whom it relates; and
(c) the kinds of evidential material that are to be searched for under the warrant; and
(d) the name of the constable who, unless he or she inserts the name of another constable in the warrant, is to be responsible for executing the warrant; and
(e) the time at which the warrant expires; and
(f) whether the warrant may be executed at any time or only during particular hours.

1.2. Outrageous Government Conduct

Outrageous government conduct, by contrast, focuses on the conduct of the police. In *Rochin v. California* 342 U.S. 165 (1952), the US Supreme Court held that evidence obtained by methods deemed "shocking to the conscience" was inadmissible. Rochin had swallowed two suspicious capsules in the presence of police officers following their warrantless entry to his residence. He was then forcibly taken to a hospital and immobilized while a tube was pushed into his mouth and an emetic solution injected into his stomach. The regurgitated capsules were found to have contained morphine. Unlike entrapment, which rests on a finding of fact by the jury, the determination of whether the conduct of law enforcement is sufficiently outrageous to constitute a denial of due process, is determined by the court. In *United States v. Russell*, 411 U.S. 423 (1973) the Supreme Court anticipated policing practices "so outrageous that due process principles would absolutely bar the government from invoking judicial process to obtain a conviction."

1.3. "Hybrid improprieties" in other common law jurisdictions

In contrast to US practice, in other common law countries there is no defence of entrapment, or of outrageous conduct *per se*. British law allows for the admissibility of evidence arising from inappropriate investigative conduct, which may include entrapment or otherwise outrageous practices, if the heinousness of the police conduct is outweighed by that alleged on the part of the defendant. In both cases, the determination of admissibility rests with the court (Hofmeyr, 2006). The Australian case of *Ridgeway* is illustrative:

Ridgeway was a convicted drug offender who, upon his release from prison, contacted a fellow ex-prisoner Lee, who had been deported to Malaysia. The objective was to import a quantity of heroin into Australia. Unbeknownst to Ridgeway, his accomplice had become a registered informer for the Royal Malaysian Police Force. A joint operation between Malaysian and Australian police services resulted in the arrival in Australia of Lee, his supervisor (an undercover Malaysian police officer), and the heroin. The operation culminated in Ridgeway's arrest when he took possession of the drugs. Ridgeway was convicted, and he appealed.

The High Court of Australia held that there was no substantive defence of entrapment under Australian law, but that a trial judge may exclude evidence that has been illegally or otherwise improperly obtained, when concerns for the integrity of the judicial process outweigh the public interest in convicting the guilty. At the time, Australian laws prohibiting the importation of drugs provided for no exceptions. Therefore, both Australian and Malaysian police had themselves engaged in criminal activities. The High Court noted that penalties for heroin importation were extremely severe. Ridgeway's conviction was quashed; the Parliament of Australia speedily enacted legislation authorizing subsequent "controlled operations" by police (*Ridgeway v The Queen* (1995) 184 CLR 19; 129 ALR 41; 69 ALJR 484. Hofmeyr, 2006).[4]

[4] Similar authorisations can be found in all Australian jurisdictions, including in Part IAB of the *Crimes Act 1914* (Cth), while Part IAC deals with assumed identities. Both kinds of authorisation may be used in the investigation of online child exploitation, though there is no legal requirement that necessitates their use.

1.4. Online Entrapment

Digital technology lends itself nicely to entrapment, as illustrated by the following case from the United States. Mark Poehlman, a married father of two children, disclosed to his wife that he had an irresistible desire to wear women's clothing. This confession met with her considerable displeasure, leading to their divorce. In addition, Poehlman was dismissed from US Air Force, where he had served honourably for 17 years.

In search of a new partner, he joined an online chat group devoted to alternative lifestyles. There, he made online contact with a person called Sharon. With complete candour, and seeking to establish a sustainable romantic partnership, he freely revealed his fashion preferences. Sharon seemed potentially receptive, but focused persistently on her three daughters. After a lengthy exchange of emails, it became clear that she was seeking a partner who would provide participatory sex education to her children. Desperate to find a companion, Poehlman agreed, and travelled to California to meet them. Sharon welcomed Poehlman to California, presented him with pornographic magazines and photographs of her children, and invited him to meet them in an adjoining room. There he was greeted not by "Sharon's" daughters, but by her colleagues: federal and state law enforcement agents.

Based on his conduct upon arrival in California, Poehlman was charged and convicted under state law of attempted lewd acts with a minor. As a result, he served one year in prison. Two years after his release, he was charged and convicted under US federal law for a crime relating to his behaviour leading up to the same incident—i.e. crossing state lines for the purpose of engaging in sex acts with a minor. For this, he was sentenced to 121 months in federal prison.

Poehlman appealed his conviction, claiming that the idea of crossing state lines for illegal purposes was implanted only after extensive email correspondence with the FBI (aka Sharon), and there was no evidence of predisposition. After all, he was only seeking a partner who would tolerate his eccentricities. His appeal was upheld. *Poehlman v. United States*, 217 F.3d 692 (2000).

1.5. Outrageous Government Conduct in Cyberspace

The case of outrageous government conduct is a difficult one to make, in cyberspace no less than in the physical world. A recent case from the State of Washington involved a female detective posing as a young girl in an online chatroom ostensibly catering for adults. She engaged with the defendant Solomon, who claimed that he had relied on the web banner statement that individuals in the chatroom were over 18 years old. During the conversation, the detective made the statement that "Oh, by the way, I'm 14, almost 15." Solomon replied "I'm not willing to get into trouble…..maybe hit me up in 3 years if your (sic) still around……. I take everything back not interested at all this is a setup by cops or a website good luck to you."

The detective persisted, despite Solomon's *seven* apparent attempts to discontinue the relationship, and the chats continued. The detective sent scores of messages, some shockingly explicit, to Solomon about wanting to meet him for sex. The suspect found them irresistible.[5] The trial judge called the language used by the detective in the messages

[5] The language used was too graphic for reproduction in this article. Readers whose prurient interest is irrepressible may obtain a better understanding of the detective's lush vocabulary from

"repugnant," and dismissed all charges. The State appealed, but the appeal was unsuccessful, the Court of Appeals holding that the trial court was entirely justified in its exercising its discretion to dismiss the charges against Solomon.

Elsewhere, seductive communication alone appears to have been insufficient to support a claim of outrageous government conduct. In one Ohio case, it was asserted by the defense that an undercover investigator had sent the suspect a photograph that was "so overly enticing that use of it by (the investigator) was outrageous." The appeals court held that "The photograph may have been sufficient in the Defendant's mind to warrant driving…… five hours from Tennessee, but is not so overwhelming to launch a thousand ships. The Helen of Troy Defense is not applicable here." *State v. Cunningham*, 156 Ohio App.3d 714, 2004-Ohio-1935.

An Ohio court held that a motion to dismiss based on outrageous government conduct required two factors: 1) that the offence in question was created by the state, and 2) the investigation involved an element of coercion. *State v. Bolden*, 2004-Ohio-2315, This could also be found to include repeated and persistent overtures, combined with evidence of significant reluctance on the part of the target, as reported in *Jacobson* and *Solomon*. (More, Lee and Hunt 2007)

Another case based on claims of outrageous conduct was that of *U.S. v Kim* 16-CR-191 (PKC) (E.D.N.Y. Jan. 27, 2017). In 2015, the FBI arrested the administrator of The Playpen, a child-pornography Internet bulletin board on the "dark web" (Chen, 2017; Mayer, 2018). Unbeknownst to the thousands of Playpen users, the FBI immediately took over administration of the site, and operated it for two weeks. The transition was seamless, and the bulletin board thrived under government stewardship. The FBI quickly obtained a warrant to install what it called a Network Investigative Technique (NIT) on the Playpen servers. The NIT consisted of malware allowing the FBI access to the computers of Playpen users, regardless of their location in physical space. Hundreds of arrests followed, including Kim's. Although many suspects in the Playpen investigation challenged the validity of the warrant on the grounds of jurisdiction and insufficient specificity, Kim took issue with the FBI's management of the website when it became apparent that at least 22,000 pictures, videos, and links to child pornography were downloaded during the period of FBI administration. Kim's counsel moved to dismiss the indictment, on the grounds that each of the downloads was a criminal offence, and that thousands of such actions thereby constituted outrageous government conduct.

The court held that any harm to 3rd parties was offset by benefits flowing from the investigation. The FBI maintained that its agents regularly assessed the continued benefits of the investigation, and shut down the website as soon as it concluded that the costs of the operation outweighed the benefits. In addition, it claimed to have continuously monitored postings to the website and took immediate action where it determined that a child was in imminent danger. Forty-nine children subjected to abuse were reportedly identified or rescued as a result. Most important for Mr Kim, the court held that his rights

---

the opinion of the Court of Appeals: *State v Solomon*, Court of Appeals of the State of Washington No. 76298-2-I. May 29, 2018.
Retrieved from http://www.courts.wa.gov/opinions/pdf/762982.pdf.

were not infringed; any harm that may have befallen third parties was irrelevant to his case.

In Australia, courts have discretion to exclude evidence obtained by illegal or improper means (*Evidence Act 1995* (Cth), s138). Despite some intriguing defence arguments, the power has not been used to exclude evidence of child grooming activities detected by undercover officers posing as children. Indeed, in an illustrative Australian Capital Territory Supreme Court case, the (then) Chief Justice quoted the Gospel of St Matthew in support of his view that community attitudes towards such offences and offenders "would support the use of covert operations to detect them in a manner that does not place an actual young person at risk". *R v Stubbs* [2009] ACTSC 63 (26 May 2009), per Higgins CJ at [69]-[70]. [6]

2. Investigative Practices by Private Actors

2.1. Vigilante Hacking

Police have traditionally drawn on 3rd parties such as individuals, community groups, and businesses to provide information and assistance in specific cases, or more broadly, to assist in crime prevention and surveillance. This information can be provided by 3rd parties unilaterally; as the result of an explicit request; or pursuant to an open invitation. The information in question may be collected by legal or illegal means. Its disclosure may be voluntary, or required by law (Ayling et al., 2009; Greenwald, 2014; Chang, Zhong & Grabosky, 2018). Our concern here is with unilateral private covert investigations by individuals or hacker groups.

Law enforcement and security agencies are not alone in their occasional inclination to engage in overzealous conduct. In 2011, the hacker group *Anonymous* undertook a unilateral campaign of harassment against online purveyors of child pornography, briefly disrupting the service of 40 sites, and publishing the names of 1500 alleged users of "Lolita City" (British Broadcasting Corporation News, 2011). Feminist groups have targeted online misogynists (Jane, 2016). In Thailand, fascist vigilante groups use Facebook to engage with political dissidents, and then report them to the police (Schaffar, 2016). "Cyber troops" in the Philippines, encouraged by the state, orchestrate campaigns of bullying and harassment against critics of the government (Sombatpoonsiri, 2018).

Individuals too have engaged in criminal conduct explicitly to assist law enforcement. In July 2000, police in Montgomery Alabama received an email from an anonymous individual, "Unknownuser," who claimed to be in Turkey. The message was accompanied by material depicting an adult person abusing a girl aged 5 or 6. Unknownuser wrote: "I know his name, Internet account, home address, and I can see when he is online. What should I do? PS he is a Doctor or Paramedic."

Unknownuser had accessed a chatroom frequented by devotees of child pornography. There he inserted a Trojan horse virus allowing him access to the computers of chatroom visitors, including one Dr Steiger. The matter was referred to the FBI, whose agents

[6] See also *R v Priest* [2011] ACTSC 18 (11 February 2011), which arrived at a similar conclusion in relation to a joint Australian-US covert operation that targeted a defendant who was engaged in grooming underage boys. Special police powers in Australia which authorise controlled operations have been used to compromise child exploitation websites and fora, to administer them for months at a time, and for evidence obtained in the process to be presented in court. See Bleakley (2018).

obtained a warrant and conducted a search of the suspect's residence. The search produced an abundance of incriminating evidence. Steiger was tried and convicted, and received a 17½ year prison sentence. He appealed on the grounds that the evidence was obtained pursuant to an illegal search by Unknownuser, who had become an agent of the state.

The US Court of Appeals held that Unknownuser had acted at all times as a private individual and that the government was a passive recipient of unsolicited information. Steiger's appeal was dismissed. The FBI agent who had been in contact with Unknownuser thanked him, and said "If you want to bring other information forward, I am available." *US v Steiger*318 F.3d 1039 (2003).

After a hiatus of several months, Unknownuser again contacted the Montgomery Police and identified another suspected child pornography offender, one William Jarrett. The Montgomery officer obtained the evidence collected by Unknownuser and forwarded it to the FBI. A prosecution ensued.

At trial, the defense argued that an agency relationship existed between the government and the hacker, and that evidence derived from Unknownuser should be suppressed. The trial court denied the motion, and Jarrett entered a conditional plea of guilty to one count of manufacturing child pornography. Prior to sentencing, the government disclosed an earlier email exchange between Unknownuser and the FBI. It revealed that following Jarrett's arrest, the FBI agent on the case had thanked Unknownuser for his assistance. The agent added "I cannot ask you to search out cases such as the ones you have sent us . . . but if you should happen across such pictures as the ones you have sent us and wish us to look into the matter, please feel free to send them to us . . . We also have no desire to charge you with hacking…"*US v Jarrett*, 338 F.3d 339 at 343. This disclosure prompted the defense to file a new motion to suppress the evidence on the grounds that an agency relationship existed between the government and Unknownuser. The motion succeeded and the evidence was suppressed. The government then appealed, successfully, with the court holding that *prior affirmative encouragement* by the state is required for a search to be deemed a government search. Communications after the arrest of the suspect had no bearing on the admissibility of evidence obtained earlier in the investigation. The court further held that the government was under no obligation to affirmatively discourage Unknownuser from hacking.

Far from the activities of the Turkish cyber-vigilante, a self-styled "private computer cop" from Canada devised a Trojan horse virus that allowed him access to between 2-3,000 computers being used to visit websites of interest to paedophiles. In May of 2000, a California judge visited such a website for reasons unrelated to his profession, and inadvertently downloaded the Trojan. The Canadian collected incriminating evidence, which he then forwarded to a citizens' group active against child pornography. The group in turn brought it to the attention of US authorities, and a prosecution followed. In federal court, the defence argued that the vigilante thought of himself as an agent for law enforcement, and that he was motivated to act for law enforcement purposes. This, said the defense, made him an agent of the state, and thereby implicated the Fourth Amendment bar to the admissibility of evidence gathered as a result of searches subsequent to and derived from vigilante's criminal act. The US Court of Appeals held that these considerations were insufficient. It reaffirmed that some degree of government knowledge of, and acquiescence in, the search *before the fact* is essential for the private party to be deemed a state agent.*US v. Kline*, 112 Fed Appx.562 (2004).

2.2. Entrapment by private actors

The issue of private entrapment has been easily resolved; at least as far as US law is concerned. In one case, an adult male attempted to contact a young female on her MySpace page. Upon learning of this, the child's mother set up her own MySpace page under an assumed name, pretending to be a 15 year old girl. The male made contact with her as well, and after a series of chats, he asked the undercover mother for sex. The mother reported this to the FBI, who took over the investigation. A conviction followed in due course. On appeal, the offender claimed that the person he thought was a minor was not a law enforcement officer, but was rather a private person who had entrapped him. The appeals court seized upon this opportunity to reaffirm that *there is no defence of private entrapment*, so there is no exclusionary rule applicable to evidence obtained in such a manner by private persons. The court held that if any remedy existed, it lay in prosecuting the vigilante. *US v Morris* 549 F. 3d. 548 (2008). In the United Kingdom, a defendant entrapped by a private party also remains culpable (Hofmeyr, 2006).

At least in theory, the remedy of prosecuting the vigilante is also available in cases of other 3rd party illegality such as hacking. However, this may be easier said than done, given jurisdictional complications. Both Unknownuser and the Canadian wannabe cyber cop were located outside the US. To activate the machinery of mutual assistance and extradition may be cumbersome and time consuming under the most urgent circumstances. It is not scandalous to suggest that law enforcement agents in most jurisdictions may be disinclined to turn against the very individual who has done them a service, even when s/he has broken the law in the process. A few notable exceptions are discussed below.

Online vigilantes may be at risk of committing numerous other crimes in the course of their efforts to assist the state. By providing illegal content to a target in an effort to establish trust, or create an opportunity to commit crime, a vigilante investigator may be committing an offence. By pretending to be a minor, s/he may be engaging in criminal impersonation, if the relevant law is sufficiently broad.[7] By inviting an adult suspect to engage in illegal activity, the vigilante may be implicated in a criminal conspiracy or be seen to be inciting, or aiding and abetting, a criminal act.[8] However, it would seem that absent egregious behaviour or evidence of ulterior motives on their part, vigilantes can usually operate with impunity.

A research exercise conducted by the child protection organisation Terre des Hommes in the Netherlands provides an interesting international example. Using an online avatar posing as a young Filipina girl called "Sweetie" in chatrooms known to be frequented by adults seeking webcam sex encounters with children, the researchers in 2013 detected

[7] Under New York law, criminal impersonation is committed when an individual"[i]mpersonates another and does an act in such assumed character with intent to obtain a benefit or to injure or defraud another"(N.Y. Penal Law § 190.25)

[8] Police are generally protected against liability for aiding and abetting the commission of criminal offences as part of their undercover work, by virtue of the fact that they lack the requisite accessorial criminal intent that the offence be completed; rather, they are usually engaged in the effort to prevent offences such as child abuse from occurring. However, where there is any doubt, mechanisms such as controlled operations and assumed identities authorities can be used, which serve both to protect investigators from liability and ensure the legality of the exercise and the admissibility of evidence thereby obtained.

thousands of apparent child predators and was able to provide identifying information to police in numerous cases, leading to prosecutions in Australia and elsewhere. A more sophisticated version, "Sweetie 2.0" involving artificial intelligence chatbot functionality shows that such investigations can in principle be automated and scaled up to new levels. However, the legality of police being able to use such techniques depends very much on each country's legislation and judicial limits regards covert online investigations, with some drawing the line at entrapment (Terre des Hommes, 2018; Schermer, Georgieva, van der Hof, & Koops, 2016). Such niceties are unlikely to be observed in the Philippines, where the extent of respect for the rights of the accused is reflected in the 12,000 extrajudicial killings that have been reported in recent years (Human Rights Watch, 2019).

2.3. Downside risks of online vigilante activity

Nearly 50 years ago, Marx and Archer (1971) noted that citizen involvement in terrestrial law enforcement processes posed a greater risk of miscarriage, and serious consequences of abuse, than did public policing alone. These warnings are no less apposite today. Notwithstanding the benefits of citizen contributions to the control of online child exploitation, private investigation can entail significant social costs. These may be borne by the targets of investigation, and/or by innocent third parties. In addition, vigilante investigations may impair the criminal process and erode the rule of law more generally (Kosseff, 2016). We focus first on the adverse unintended consequences of covert investigations to targets and to third parties.

One can readily appreciate that child exploitation may engender extreme outrage from some individuals. At times, this can result in overzealous reaction. In Adelaide, Australia, a vigilante who had reported two alleged child sex offenders to police was himself arrested and charged with aggravated assault against one of his targets while attempting a 'citizen's arrest.' In addition, the vigilante was charged with two counts of using a carriage service to menace, harass or cause offence, and one count of publishing the identity of a person charged with a sexual offence, an offence under South Australian law (Dowdell, 2017).[9]

In the UK, two men accused by a paedophile hunter were allegedly blackmailed by the vigilante, and later physically beaten by groups of people when their identities were disclosed. Both the vigilante and the two men were charged (Sabin, 2015). Elsewhere in the UK, members of a group called Letzgo Hunting identified a target, who was beaten and otherwise threatened when his image was posted online. He was compelled to quit his job and relocate elsewhere in Britain. Police reviewed the materials collected by the vigilante group and found no evidence of any sexual offences (Booth, 2018).

Being caught in a sting can result in much more than humiliation or a beating. Another target of Letzgo Hunting was tempted by an online impersonation of a 14 year old female, only to be confronted at their agreed meeting place by the impersonator, an adult male. The target committed suicide (British Broadcasting Corporation News, 2013).

"Perverted Justice," an anti-paedophile group in the United States, collaborated with local police and a major television network to orchestrate a sting targeting a public prosecutor in Texas. The operation was to be broadcast as part of the television series "To

[9] A "carriage service" is *not* a mode of transportation, but rather refers to a telecommunications facility.

Catch a Predator." For dramatic effect, the sting culminated in a raid on the suspect's home by a police SWAT team. As police entered his home, the suspect took his own life. His surviving sister sued the television network for damages; the case was settled out of court for an undisclosed amount. (Conradt v. NBC Universal, Inc., 07 Civ. 6623, U.S District Court, S.D. New York); Stelter, 2008).

Gratuitous harm to an alleged offender may arise from private motives such as revenge, vindictiveness or greed in addition to moral indignation and perceived civic responsibility. One case, ostensibly involving the intended public shaming of four suspected offenders, elicited accusations of ulterior motives on the part of the vigilante. Explicit "selfie" images and texts posted by the four to a person thought to be a young female were published on a website. A lawyer for the four implied that the website was a profit making venture, reliant on advertising revenue and donations for income. He is quoted as having said "This website is a total scam. They're not solving crimes. They don't report people to the authorities. They're just making money." The lawyer succeeded in having the website taken down, only to have it reappear shortly thereafter in another location. The four threatened to sue for criminal impersonation and for theft of intellectual property, claiming that their moral rights in their images and texts had been violated (Gregorian, 2015).

A group of teenage boys in the Australian Capital Territory targeted men through a gay dating app with a view towards exposing them as paedophiles. The primary motive was extortion, but one was found to have had "a self-serving sense of vigilantism." One of the group's targets subsequently committed suicide (Gorrey, 2017).[10]

In the UK, a 27 year old man presented himself on Craig's List as a fourteen year old girl, and invited an unsuspecting man to his home. Upon arrival, the victim was threatened with a hammer and directed to disrobe. The paedophile hunter then demanded and received £300, and insisted on regular payments of £150 as a condition of nondisclosure. The victim himself went to the police, and was charged with attempted child grooming; the vigilante was charged with blackmail and sentenced to 28 months jail (Rowe 2015).

A 33 year old man in Melbourne led two lives, one as a paedophile and one as a paedophile hunter. He sought to extort $10,000 from a businessman, to whom he had sent a video purporting to depict the businessman in a compromising position with a 14 year old. The businessman whom he had targeted, however, was not the individual depicted in the video, despite bearing the same name. The "poacher turned extortionist" was arrested when he arrived at a pre-arranged location to recover the extortion payment (Portelli 2014).

Then, there is the issue of secondary victimization—harm to third parties. This is not uncommon in the annals of police undercover investigation (Joh & Joo, 2015). The targets of a vigilante investigation may have family members or other close associates,

[10] Sentencing remarks are found in R v KB [2017] ACTSC 344 (1 November 2017), where the judge (Murrell CJ) imposed a custodial sentence of one year and 10 months on the teenaged offender, commenting (at [49]): *"Any form of vigilantism tends to undermine the rule of law and divide what is otherwise a tolerant community in the Australian Capital Territory. It is abhorrent to the public. The sentencing purposes of public protection and general deterrence are very important and must be strongly reflected in the sentence that is imposed".*

entirely innocent of wrongdoing, who themselves may be stigmatized and/or harassed as a result of disclosures.

2.4. Interference with police operations

Police value citizen assistance, but only to a point. "Wannabe cyber cops" can get underfoot. They can tamper with evidence, intentionally or accidentally (e Silva 2018). They can create crime, and as we have seen, use their purported "good works" to mask criminal activity of their own. Non-intrusive investigative methods may also go astray, and even genuine civic-minded individuals can impede police investigations. Nhan et al (2017) report that citizens seeking to contribute to identifying perpetrators of the Boston Marathon bombings in 2013 misidentified several individuals as potential suspects. Crowd sourcing is not always a perfect investigative strategy. In the Boston bombing case, police were deluged with communications from citizens, compounding the burdens they were facing, under time pressures in an urgent situation with the perpetrators still at large (Nhan et al., 2017).

To their credit, police in a number of jurisdictions have been known to issue public statements advising well-meaning citizens (and those not so well-meaning) to act within the law. Primary concerns are the risk of jeopardizing investigations, by inadvertently alerting the target, or impeding the collection of evidence. There is also the risk that the integrity of that evidence which has been collected, may have been corrupted.

Regarding the Adelaide case discussed above, a senior South Australian detective was quoted as warning "It is not appropriate for individuals to take matters into their own hands because no matter how well intentioned they may be, this can significantly obstruct and hinder what police are empowered to do." Noting the potential for violence in such matters, he added "There is a very real risk to both parties when someone chooses to take the law into their own hands" (Dowdell, 2017).

A 47 year-old Welshman, who 15 years earlier had been convicted for possession of indecent images of children, was convicted in 2015 after posing as a young girl and eliciting indecent images from unwitting men. By embedding computer viruses in his communications, he was able to obtain the men's personal details and additional incriminating material. Over a 2 1/2 year period, he made approximately £40,000 by blackmailing his targets. He was convicted of 31 offences and sentenced to nine years imprisonment. In response to this sentence, a South Wales Police Detective remarked "I hope this will send a clear message that we take blackmail and computer hacking offences very seriously – in whatever context they are conducted" (Readhead, 2015).

2.5. Aggravation of systemic pathologies

Unregulated private searches may have an adverse impact on the criminal process and on society more generally. When police passively condone, much less actively approve of vigilante illegality, it may be perceived as an implicit invitation to join in more of the same. When evidence illegally obtained by private actors is admitted in court, this may be seen as the court's implicit imprimatur. The court's reputation or authority may be tarnished by explicit indifference to inappropriate police conduct, or by implicit tolerance of questionable private conduct.

The normative unity of the criminal process is such that questionable behaviour by one institution, police, prosecution, or the judiciary- unless that institution is held

unambiguously to account-- reflects adversely on all three. If the provision for acquittal or for exclusion of evidence on grounds of outrageous conduct or entrapment is intended to protect the integrity of the judicial process, when would prosecution based on illegal or otherwise unsavoury activity by a "private party investigator" contaminate the system of crime control?

In theory, the independence of each of these institutions should serve as a check on the potential transgressions of the others. In practice, this is not always the case.

Conclusion

Undercover investigation appears to have become an indispensable method in response to cybercrime generally, and to online child exploitation in particular. In theory, abuses by government agents are subject to the accountability of the judicial process, at least in those jurisdictions that adhere to the rule of law and respect the rights of the accused. But the democratization of digital technology has enabled ordinary citizens to assume the role of amateur cyber cops, for better or worse. The advent of social media has been a boon for internet vigilantism. Not only has it created spaces to facilitate illicit overtures, but it has enabled the formation of vigilante communities. Today, any person with internet access can create his or her own sex offender registry. One might question the extent to which law or policy should foster an ethos of bounty hunting. It seems appropriate to advance a number of suggestions that might govern the use of undercover investigations by agents of the state, to lessen the risk of abuse.

First, they should not be employed gratuitously. Rare indeed is the law enforcement agency that can boast of more resources than it needs. If online child exploitation is as rampant as it is said to be, more strategic application of limited resources is in order.

Second, the targeting of investigations should be focused. Rather than lurking in websites ostensibly established for legitimate purposes, such as adult dating and alternative lifestyles, detectives should aim for sites more explicitly devoted to criminal activity.

Third, the procedures for engaging with targets should be closely circumscribed. Investigators should avoid persistent, unrelenting pursuit of a target who has expressed repeated reluctance to engage. It might be useful to compare the guidelines governing online investigations by the New Zealand Police with the investigative techniques employed in the *Solomon* case.[11]

The above guidelines, of course, pertain to state officials, and not to private individuals. Given the complexity and sensitivity of criminal investigation, private individuals are at risk of harming targets and third parties well beyond what the law will tolerate. The above cases illustrate an unfortunate paradox: protections from overzealous investigation by agents of the state, themselves far from perfect, are not matched by safeguards against abuses by private citizens.

There may be no simple solutions to this conundrum. The provision of official guidelines to non-state actors may render them agents of the state, which could risk contamination of any prosecution that might flow from their efforts. In the meantime, it seems appropriate for law enforcement agencies firmly to apply the law when it is transgressed by vigilantes, and to continue publicly to discourage vigilante activities based on criminal conduct. The situation is even more complex when the illegal investigative

[11] New Zealand Police, *Principles of Practice for Investigating On-Line Grooming of Children Under 16*. Reproduced in *R v Stubbs* [2009] ACTSC 63

activity, whether undertaken by citizen or by state agent, originates in a foreign jurisdiction. Of course, the state may still encourage the reporting of suspected criminal conduct occurring within public view, in cyberspace as on the street.

Rules of evidence and procedure quite rightly exist to protect the judicial process from contamination by the abuse of state power. But when the state passively condones private illegality in furtherance of public policy, it may subtly encourage high-tech lynching. If citizen involvement in online undercover investigation has a place in any jurisdiction, citizens should be held to the same level of accountability as are agents of the state.

References

Australian Cybercrime Online Reporting Network (2018). ACORN. Retrieved from https://www.acorn.gov.au.

Ayling, J., Grabosky, P., and Shearing, C. (2009). *Lengthening the Arm of the Law: Enhancing Police Resources in the Twenty-First Century*. Cambridge, UK: Cambridge University Press.

Balduzzi, M., Flores, R., Gu, L., Maggi, F., Ciancaglini, V., Reyes, R., & Urano, A. (2018). *A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks*. Trend Micro. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf.

Bleakley, P. (2018).Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating dark web child exploitation networks." *The Police Journal: Theory, Practice and Principles*. DOI: 10.1177/0032258X18801409

Booth, R. (2013, October 26). Vigilante paedophile hunters ruining lives with internet stings. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2013/oct/25/vigilante-paedophile-hunters-online-police.

British Broadcasting Corporation News (2011, October 24). Hackers take down child pornography sites. Retrieved from http://www.bbc.com/news/technology-15428203

British Broadcasting Corporation News (2013, September 18). Letzgo Hunting denies blame for man's suicide. Retrieved from http://www.bbc.com/news/uk-england-leicestershire-24145142.

Brown, J. (1997, March 14). Cyber Angels antiporn database dies. *Wired*. Retrieved from https://www.wired.com/1997/03/cyber-angels-antiporn-database-dies.

Chang, L., Zhong, L., & Grabosky, P. (2018).Citizen co-production of cyber security: Self-Help, Vigilantes, and Cybercrime."*Regulation and Governance, 12*(1), 101-114.

Chen, C. W. (2017). The graymail problem anew in a world going dark: Balancing the interests of the government and defendants in prosecutions using network investigative techniques (NITs). *Columbia Science & Technology Law Review,* 19, 185.

Cheong, P. H., & Gong, J. (2010). Cyber Vigilantism, Transmedia Collective Intelligence, and Civic Participation. *Chinese Journal of Communication*, *3*(4), 471-487.

Davidson, J., & Gottschalk, P. (eds.) (2011). *Internet Child Abuse: Current Research and Policy*. Abingdon-on-Thames: Routledge-Cavendish.

Dowdell, A. (2017, December 22). Self-proclaimed paedophile hunter arrested, charged with assault and revealing identity of person charged with sexual offence. *The Advertiser*. Retrieved from http://www.news.com.au/national/south-australia/selfproclaimed-paedophile-hunter-arrested-charged-with-assault-and-

revealing-identity-of-person-charged-with-sexual-offence/news-story/cbc35c6a9c42a1f4bcdbed074eb3964d.

e Silva, K.K. (2018).Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers and Technology*, *32*(1), 21-36.

Federal Bureau of Investigation (2018). *Internet Crime Complaint Center (IC3)*. Retrieved from https://www.ic3.gov/default.aspx.

Fijnaut & Marx, G. T. (1995). Undercover: Police Surveillance in Comparative Perspective. Alphen aan de Rijn, The Netherlands: Kluwer.

Fronc, J. (2009). *New York Undercover: Private Surveillance in the Progressive Era*. Chicago IL: University of Chicago Press.

Gorrey, M. (2017, May 12). Canberra teen locked up for 'calculated entrapment' of men in Grindr extortion. *Canberra Times*. Retrieved from https://www.canberratimes.com.au/national/act/canberra-teen-locked-up-for-calculated-entrapment-of-men-in-grindr-extortion-20170512-gw3b4r.html.

Grabosky, P., Smith, R., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge, UK: Cambridge University Press.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Gregorian, D. (2015, May 22). Four men ensnared by 'To Catch a Predator' type website sue to get personal information scrubbed from web. *New York Daily News*. Retrieved from http://www.nydailynews.com/new-york/4-men-sue-scrub-perv-info-web-article-1.2232881.

Harcourt, B. E. (2015). *Exposed: Desire and Disobedience in the Digital Age*. Cambridge MA: Harvard University Press.

Hofmeyr, K. (2006). The Problem of Private Entrapment *Criminal Law Review* 319-336.

Human Rights Watch (2019). Philippines' "War on Drugs. Retrieved from https://www.hrw.org/tag/philippines-war-drugs

Jane, E.A. (2016). Online misogyny and feminist digitalantism. *Continuum, 30*(3), 284-297.

Joh, E., & Joo, T. (2015). Sting victims: Third party harms in undercover police operations. *Southern California Law Review*, *88*(6), 1309-1356.

Kosseff, J. (2016). The hazards of cyber-vigilantism. *Computer Law and Security Review,* 32, 642-649.

Marx, G. T. (1988). *Undercover: Police Surveillance in America*. Berkeley: University of California Press.

Marx, G. T. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Marx, G. T., & Archer, D. (1971). Citizen involvement in the law enforcement process: The case of community police patrols."*American Behavioral Scientist*, *15*(1) 52-72.

Mayer, J. (2018). Government hacking. *Yale Law Journal,* 127, 570-660.

Microsoft Trust Center (2018). *Cybercrime*. Retrieved from https://www.microsoft.com/en-us/trustcenter/security/cybercrime.

More, R., Lee, T., & Hunt, R. (2007). Entrapped in the web? Applying the entrapment defense to cases involving online sting operations. *American Journal of Criminal Justice 32*, 87-98.

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston Marathon bombings. *The British Journal of Criminology,* 57(2), 341-361.

Portelli, E. (2014, April 14). Paedophile-hunter targeted innocent Melbourne businessman, court told. "*Herald Sun*. Retrieved from http://www.heraldsun.com.au/news/national/paedophilehunter-targeted-innocent-melbourne-businessman-court-told/newsstory/ef00b800a742e95095fdf2ce09045512.

Readhead, H. (2015, December 8). 'Paedophile hunter' jailed for hacking and blackmail. *Metro*. Retrieved fromhttps://metro.co.uk/2015/12/08/paedophile-hunter-jailed-for-hacking-and-blackmail-5551111/?ito=cbshare.

Rowe, J. (2015, December 10). "Adam Brookes lured victim to his home in Downham Gardens, Prestwich, by advertising on the Craigslist website." *Bury Times*. Retrieved from http://www.burytimes.co.uk/news/14136397.Online__paedophile_hunter__who_posed_as_14_year_old_girl_forced_lured_man_to_remove_clothes.

Sabin, L. (2015, April 20). Vigilante paedophile hunter arrested over 'assault' and 'blackmail' of two men accused of attempting to meet with underage girls." *The Independent*. Retrieved from https://www.independent.co.uk/news/uk/crime/vigilante-paedophile-hunter-arrested-over-assault-and-blackmail-of-two-men-accused-of-attempting-to-10188587.html

Schaffar, W. (2016). New social media and politics in Thailand: The emergence of fascist vigilante groups on facebook. *ASEAS – Austrian Journal of South-East Asian Studies*, *9*(2), 215-234.

Schermer, B., Georgieva, I., van der Hof, S., & Koops, B-J (2016). *Legal Aspects of Sweetie 2.0*. Leiden: Center for Law and Digital Technologies.

Sombatpoonsiri J. (2018). Manipulating civic space: Cyber trolling in Thailand and the Philippines" GIGA Focus, Asia (3) Retrieved from https://www.ssoar.info/ssoar/bitstream/handle/document/57960/ssoar-2018-sombatpoonsiri-Manipulating_Civic_Space_Cyber_Trolling.pdf?sequence=1.

Stelter, B. (2008, June 26).NBC settles with family that blamed a TV investigation for a man's suicide." *New York Times*. Retrieved from https://www.nytimes.com/2008/06/26/business/media/26nbc.html

Terre des Hommes (2018). *Sweetie 2.0: Stop Webcam Childsex*. Retrieved from https://www.terredeshommes.nl/en/sweetie-20-stop-webcam-childsex.

Tusikov, N. (2017).*Chokepoints: Global Private Regulation on the Internet:* Oakland CA: University of California Press.

Završ nik, A. (2018). *Big Data, Crime and Social Control London:* Routledge.