Cultivating a Relationship That Works: Cyber-Vigilantism and the Public Versus Private Inquiry of Cyber-Predator Stings*

I. INTRODUCTION

The Federal Bureau of Investigation saw a 2062 percent increase over the last decade in open cases initiated through its Innocent Images National Initiative.[1] The FBI Initiative combats all aspects of computer-based attacks on children, including catching sexual predators online.[2] Access to the Internet has increased tremendously over the last decade.[3] As a result, the Initiative has expanded to twenty-eight FBI field offices[4] and has "secure[d] nearly 3,000 convictions."[5]

The above-mentioned statistics show that online predation against children is one of the most troubling trends in the digital age.[6] J. Allan

---

* *Christopher P. Winters*. J.D. candidate 2009, University of Kansas School of Law; B.A. 2004, Brigham Young University. I wish to extend my gratitude to Professor Stephen McAllister for his helpful comments and suggestions throughout the writing process. I also want to thank my wife Tiffany and daughters Bailey and Alyssa for their love and support.

1. FBI, Innocent Images National Initiative, http://www.fbi.gov/publications/innocent.htm (last visited Aug. 26, 2008) (noting that opened cases rose from 113 to 2443 between 1996 and 2007). "The Innocent Images National Initiative (IINI), a component of FBI's Cyber Crimes Program, is an intelligence driven, proactive, multi-agency investigative operation to combat the proliferation of child pornography/child sexual exploitation (CP/CSE) facilitated by an online computer." *Id.*

2. *See id.* (discussing the Initiative's focus on online exploitation of children, child pornographers, those possessing child pornography, as well as predators' online efforts to engage in sexual activity with a minor).

3. Przemyslaw Paul Polański, CUSTOMARY LAW OF THE INTERNET: IN THE SEARCH FOR A SUPRANATIONAL CYBERSPACE LAW, at VII–IX (Aernout H.J. Schmidt et al. eds., Information Technology and Law Series No. 13, 2007). According to recent estimates, there are 1,463,632,361 Internet users worldwide, roughly 20% of the world's population. *World Internet Usage Statistics News and World Population Stats*, http://www.internetworldstats.com/stats.htm (last visited Aug. 26, 2008). The number reaches an astounding 73.6% of the North American population alone. *Id.*

4. FBI, *Ten Years of Protecting Our Children: Cracking Down on Sexual Predators on the Internet*, Dec. 2, 2003, http://www.fbi.gov/page2/dec03/online120203.htm.

5. *Id.*

6. *See* J. Allan Cobb, *Evidentiary Issues Concerning Online "Sting" Operations: A Hypothetical-Based Analysis Regarding Authentication, Identification, and Admissibility of Online Conversations—A Novel Test for the Application of Old Rules to New Crimes*, 39 BRANDEIS L.J. 785, 786–87 (2001).

Cobb illustrated the enormity of the situation by comparing children on the Internet to "young zebra on the plains of the Serengeti—stalked from the fringes by big game predators."[7] Susan Brenner and Leo Clarke argue that the legal community faces a real dilemma in regards to cybercrime.[8] Specifically, Brenner and Clarke posit that "[c]ybercrime raises new and difficult challenges for a society's need to maintain internal order; the challenges arise not from the need to adopt new law criminalizing the activity at issue, but from law enforcement's ability to react to it."[9] This Comment addresses the challenge of integrating private-party participation in law enforcement into legally acceptable investigative techniques.[10]

As evidenced by the FBI Initiative and other law enforcement programs, one solution to this problem has been the online sting.[11] Justification for this tactic is not hard to find. In Justice Roberts's dissenting opinion in the seminal entrapment case of *Sorrells v. United States*,[12] he comments:

> Society is at war with the criminal classes, and courts have uniformly held that in waging this warfare the forces of prevention and detection may use traps, decoys, and deception to obtain evidence of the commission of crime. Resort to such means does not render an indictment thereafter found a nullity nor call for the exclusion of evidence so procured.[13]

National awareness of cyber-pedophilia grew tremendously with the premiere of a *Dateline NBC* series: "To Catch a Predator."[14] Cloaked in anonymity online, predators were unceremoniously unmasked in front of the viewing audience by *Dateline* host Chris Hansen.[15] The show boasts

---

7. *Id.* at 787.

8. *See* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 666 (2005).

9. *Id.*

10. *See id.* at 674.

11. *See* Audrey Rogers, *New Technology, Old Defenses: Internet Sting Operations and Attempt Liability*, 38 U. RICH. L. REV. 477, 477 (2004) (stating that "Internet sting operations to catch adults preying on children have grown as exponentially as the public's use of the Internet").

12. 287 U.S. 435 (1932).

13. *Id.* at 453–54 (Roberts, J., dissenting in part).

14. *See* Steve Thompson, *Murphy*, *NBC Stung by Criticism of Sex-Predator Cases*, DALLAS MORNING NEWS, Aug. 14, 2007, at 1A; *see also* Chris Hansen, *Reflections On 'To Catch a Predator*,' http://www.msnbc.msn.com/id/17601568 (last visited Aug. 27, 2008) (stating that host Chris Hansen has even testified in front of Congress to bring this problem to light).

15. *See* Luke Dittrich, *Tonight on Dateline This Man Will Die*, ESQUIRE, Sept. 2007, at 235 (stating that when a would-be-predator arrives at the decoy house, "Chris Hansen confronts him with a printout of . . . [the] chat transcripts" and upon leaving the house "local cops . . . arrest him and

a large number of convictions and has raised awareness of a major problem.[16] However, "To Catch a Predator" has also faced its share of skepticism.[17]

In his article, *The Shame Game*, Douglas McCollam argues that "*Dateline* hasn't so much covered a story as created one."[18] According to McCollam, one of the most troubling aspects of the show is *Dateline NBC*'s relationship with its "decoys," Perverted Justice.[19] Perverted Justice is a watchdog group with a stated purpose of creating a "chilling-effect" in chat-rooms so that would-be pedophiles will think twice about inducing minors into sexual encounters.[20] Perverted Justice contracts with *Dateline NBC* to conduct the stings depicted on the program.[21] In some documented instances, Perverted Justice was also deputized by law enforcement,[22] while at the same time allegedly receiving a "consulting fee" of $100,000 from the show.[23] "To Catch a Predator" host, Chris Hansen, asserts that the show and law enforcement run parallel investigations[24] with an impenetrable "Chinese wall";[25] however, the above-mentioned facts seemingly contradict this assertion. McCollam states, "[I]t is clearly a [journalistic] no-no, even at this late date in the devolution of TV news, to directly pay government officials or police officers."[26] When Perverted Justice is deputized, the conflicts of interest are evident. To Perverted Justice's credit, when not working for the show, it works with local law enforcement for free.[27]

The legal issues at the heart of "To Catch a Predator" have largely been ignored due to the fact that most suspects just plead guilty.[28] One man caught in a *Dateline* sting, however, "has launched [an] aggressive

charge him with online solicitation of a minor").

16. *See* Douglas McCollam, *The Shame Game*, COLUM. JOURNALISM REV., Jan.–Feb. 2007, at 28, 30 ("To date, by the show's own count, it has netted 238 would-be predators . . . . Hansen regularly gives talks to schools and parents groups . . . and he was even summoned to Washington to testify before a congressional subcommittee investigating the problem . . . .")

17. *See id.*

18. *Id.* at 33.

19. *Id.* at 31–32.

20. Perverted-Justice.com, http://www.perverted-justice.com/index.php?pg=faq (follow "What is the goal of Perverted-Justice.com? A.+" hyperlink) (last visited Aug. 18, 2008).

21. Dittrich, *supra* note 15, at 235.

22. John Simerman, *TV Show on Trial along with Suspect*, CONTRA COSTA TIMES, Aug. 4, 2007, at A1.

23. McCollam, *supra* note 16, at 31.

24. *Id.*

25. *Id.*

26. *Id.*

27. Perverted-Justice.com, Information Sharing Agreements, http://www.perverted-justice.com /?pg=policeinfo (follow "Info for Police" hyerlink) (last visited Aug. 18, 2008).

28. Simerman, *supra* note 22, at A1.

fight" in court.[29] Dr. Maurice Wolin, a Piedmont, California oncologist, took the bait when he chatted with a Perverted Justice decoy online.[30] According to reports, Wolin first said he "couldn't do anything"; however, the Perverted Justice decoy taunted Wolin and called him "just a chicken and a liar and a ditcher and a player."[31] Eventually, Wolin agreed to meet with the person whom he believed to be a minor.[32] However, when Wolin arrived to meet the "minor," he was greeted by law enforcement and subsequently arrested.[33] Wolin hired a celebrity attorney and has already raised the defense of entrapment.[34] As of October 2, 2008, Dr. Wolin has yet to stand trial, and he continues to maintain that he was entrapped by the Perverted Justice decoy.[35]

Apart from the entrapment defense, it is also clear Wolin and his attorney are fighting the organizational structure in place between the police, *Dateline*, and watchdog group Perverted Justice.[36] During the preliminary hearing, the defense argued that the "Petaluma police [acted] as more puppet than master of an operation."[37] Wolin's attorney, Blair Berk, also claimed that the Perverted Justice decoy was "paid" and "untrained" and that the decoy "badgered and cajoled him into committing a crime."[38] Clearly, Berk's goal is to cast doubt on the legal viability of the alliance between the police, *Dateline*, and Perverted Justice.

Wolin's case is a rarity. According to Wolin's attorney: "Everybody pleads (guilty). Everybody's so humiliated by the rack and screw

29. Linda Davis & John Simerman, *Decision Due in Wolin Case*, CONTRA COSTA TIMES, Jan. 18, 2008.

30. Simerman, *supra* note 22, at A1.

31. *Id.*

32. *See id.*

33. *See id.*

34. John Simerman, *Sting on "Dateline NBC" Show Called into Question*, CONTRA COSTA TIMES, Aug. 8, 2007, at A3.

35. *See* Linda Davis, *Wolin's Lawyer Files Discovery Motion*, CONTRA COSTA TIMES, Oct. 2, 2008. (stating that Wolin's attorney maintains that his client was "goaded" into meeting the Perverted Justice Decoy). The trial date for Maurice Wolin is currently scheduled for February 6, 2009. *Id.*

36. *See* Simerman, *supra* note 22, at A1 ("Similar arguments are common in pedophile sting operations. What's different is that the show and its unusual arrangement among police, NBC and a controversial online vigilante group called Perverted Justice have largely escaped courtroom scrutiny.").

37. John Simerman, *Lawyer Questions Officials' Role in TV Sex Sting*, CONTRA COSTA TIMES, Sept. 6, 2007, at A3.

38. Lori A. Carter, *Wolin Wants Charge Tossed*, PRESS DEMOCRAT, Jan. 11, 2008, http://www.pressdemocrat.com/EarlyEdition/article_view.cfm?recordID=8398&publishdate=01/11/2008.

they've been put on . . . ."[39] Berk further states, "I'm ashamed about how little these issues have been litigated."[40] The implications of this trial could change some of the tactics and practices of law enforcement, *Dateline*, and Perverted Justice.[41]

Another much publicized "To Catch a Predator" sting led a county prosecutor, William Conradt Jr., to commit suicide when the SWAT team entered his house to arrest him over his online communications with a Perverted Justice decoy.[42] Conradt's untimely death led his sister Patricia to file suit against NBC Universal, claiming tort and civil rights violations against the network for its involvement with the online sting.[43] NBC brought a 12(b)(6) motion, and although "many of [Conradt's] claims [were] dismissed," the judge did allow "the principal claims to survive."[44] U.S. District Judge Denny Chin ruled:

> [A] reasonable jury could find that NBC crossed the line from responsible journalism to irresponsible and reckless intrusion into law enforcement. Rather than merely report on law enforcement's efforts to combat crime, NBC purportedly instigated and then placed itself squarely in the middle of a police operation, pushing the police to engage in tactics that were unnecessary and unwise, solely to generate more dramatic footage for a television show.[45]

It is not surprising that a few months after Judge Chin's ruling, NBC Universal settled its claims with Patricia Conradt and her deceased brother's estate.[46]

These situations show the potential problems inherent with the police's association with cyber-vigilantes even if the vigilante groups do a public service. Perverted Justice has organized stings in almost all U.S. jurisdictions and boasts a highly impressive conviction rate.[47] When these cases do go to trial, entrapment is a commonly raised defense.[48]

---

39. Simerman, *supra* note 22, at A1.

40. *Id.* at A1.

41. *See* John Simerman, *Judge to Consider "Predator" Chat Logs*, CONTRA COSTA TIMES, Sept. 11, 2007, at A4 ("Wolin's defense, if successful, could also provide a template for others to fight charges stemming from the controversial show.").

42. *See generally* Dittrich, *supra* note 15.

43. *See* Conradt v. NBC Universal, Inc., 536 F. Supp. 2d 380 (S.D.N.Y. 2008).

44. *Id.* at 383.

45. *Id.*

46. *See NBC Settles Suit over 'Dateline: Predator' Episode*, CNN.com, June 26, 2008, http://www.cnn.com/2008/CRIME/06/26/dateline.predator.ap/index.html.

47. Perverted-Justice.com, *supra* note 27 (stating that Perverted Justice has conducted sting operations across the nation and the group's "evidence was used to arrest 256 suspects during sting operations in 2006" alone, with a "100% conviction rate").

48. Jarrod S. Hanson, *Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion*,

The law clearly does not allow use of this defense when a private party entraps another.[49] This appears to disqualify the defense of entrapment when Perverted Justice is involved. However, this Comment will show that in certain circumstances such a generalization is inaccurate.

Although there may be debate over the relationship between Perverted Justice and law enforcement, this Comment will show what could occur should a court rule that cyber-vigilante groups are agents of the government during a coordinated online sting. This Comment will show the need for cyber-vigilantes to abide by the same statutory and constitutional standards of investigative conduct that law enforcement follows. The ultimate issue is whether it is worth the risk. Especially when considering that a cyber-vigilante who fails to follow law enforcement standards of conduct could put convictions in jeopardy. It is imperative that private groups such as Perverted Justice realize the legal risks associated with conducting online stings with law enforcement. Private groups that understand these risks will be more likely to use discretion in combating cyber-pedophilia.

If an alliance is formed between police and cyber-vigilantes, there must be strict protocols. The protocols must include training in the rules of evidence, and also training on how to avoid situations in which a defendant could argue entrapment. Ultimately, each jurisdiction will have to address the accountability it expects from a cyber-vigilante. Whether it is through immediate supervision or some other means, law enforcement must be more of a player in how joint stings are conducted.

The rest of the Comment analyzes scenarios where cyber-vigilantes reach the status of government agents as well as the consequences of such a classification. To reach this end, Part II of this Comment outlines how Perverted Justice and law enforcement conduct cyber-stings. Part II also explains the standards a court will likely follow to determine whether a cyber-vigilante is a state actor. Finally, Part II addresses entrapment law and other constitutional implications a cyber-vigilante may face.

Part III of the Comment then analyzes how a court will decide if a cyber-vigilante is a state actor. Part III further addresses situations where a cyber-vigilante crosses the line, and the implications of doing so. Finally, this Comment analyzes why a ruling of state action will modify

1996 U. CHI. LEGAL F. 535, 536 (1996) (stating that because of "[t]he ease with which law enforcement officials can assume false identities in cyberspace . . . [d]efendants are . . . likely to invoke the entrapment defense with increasing frequency").

49. *See* United States v. Manzella, 791 F.2d 1263, 1269 (7th Cir. 1986) ("There is no defense of private entrapment.").

the way cyber-vigilantes conduct stings and coordinate with law enforcement. Regardless of what the courts decide, cyber-vigilante groups must be ready to face the scrutiny of the courts to ensure successful conviction of cyber-predators.

II. BACKGROUND

A. How Perverted Justice Operates

Groups like Perverted Justice work exclusively with law enforcement as decoys to wage war against online predation of minors.[50] They do so by setting up sting operations, often with law enforcement's approval.[51] The basic function of a sting "is that through covert means, the authorities create or facilitate the very offense of which the defendant is convicted. Normally this is done by having an undercover agent hold out some sort of bait, or opportunity to commit a crime, and then punishing the person who takes the bait."[52] Once an adult initiates sexually explicit dialogue, the trap is then laid to facilitate a meeting with the pedophile.[53] The pedophile believes he will meet a minor, but instead is often apprehended by law enforcement.[54]

The group's website states: "We essentially strive to serve as a tool for [law enforcement] to use . . . and are trained exclusively on how to make solid, easily prosecutable cases that are guaranteed to put internet predators in jail—and we provide this service [to law enforcement] for free."[55] In order to establish a working relationship with law enforcement, the website states:

> [Law enforcement] emails us, we speak with them on the phone, and work out the details of jurisdiction and what they'd like to see out of the chat-logs we do. Then, we make a note for the Contributors of where Information First contacts are, what areas they cover and how to get ahold [sic] of them. Contributors then work Information First areas

50. Perverted-Justice.com, *supra* note 27.

51. *See id.*

52. Bruce Hay, *Sting Operations, Undercover Agents, and Entrapment*, 70 MO. L. REV. 387, 388 (2005).

53. *Id.* at 390; *see also* Perverted-Justice.com Homepage, http://www.perverted-justice.com (last visited Aug. 18, 2008) (highlighting the details of various sting operations).

54. Hay, *supra* note 52, at 388.

55. Perverted-Justice.com, *supra* note 27.

> and turn over the information, first, to the already-stated interested and proactive police contact in that area.[56]

Finally, Perverted Justice emphatically describes its association with law enforcement. Perverted Justice proclaims, "What more can we say about how hand-in-hand we work with law enforcement across the nation?"[57] It is this "hand-in-hand" relationship that helps strengthen the argument that Perverted Justice and similar cyber-vigilantes may be classified as government agents during the scope of the stings they coordinate with law enforcement. It is also this "hand-in-hand" relationship that creates a need for cyber-vigilante groups to be well-trained and aware of the potential pitfalls of violating the public trust.

B. How Law Enforcement Conducts a Cyber-Sting

In J. Allan Cobb's 2001 article, he sets out a hypothetical scenario of a law enforcement officer setting an online sting.[58] Although fictional, the account gives good insight on the intricacies of the procedure and rules of evidence, and why it is so important for those working in law enforcement to be properly trained. The story follows the fictional Sergeant Stan Sirius, "a veteran of many sting operations," as he navigates through the world of online stings.[59]

When Sergeant Sirius receives the assignment, he first asks for specialized training; his police chief says there is no time.[60] However, according to a law enforcement contact, Chief Justice, setting a sting is easy and requires: "(1) [Creating] a username and member profile for a minor . . . [o]nline; (2) [A]n officer using the username of the minor goes in-and-out of 'appropriate' chat rooms; (3) [O]nce the sexual predator initiates contact with the minor, private conversations take place in chat rooms, 'Private Rooms,' or via 'Instant Messages' (IM's)."[61] Once the trap is set, it requires waiting until the "predator makes clear his intent to have sexual contact."[62] When this occurs, the decoy sets up a meeting

---

56. *Id.*

57. Perverted-Justice.com, http://www.perverted-justice.com/index.php?pg=faq#cat6 (follow "Just HOW Cooperative is PeeJ with Police?" hyperlink) (last visited Aug. 18, 2008) (emphasis added).

58. Cobb, *supra* note 6, at 805–21.

59. *Id.* at 807.

60. *Id.*

61. *Id.* at 807–08.

62. *Id.* at 808.

and an arrest can be made.[63] According to Chief Justice, this process is "like shooting fish in a barrel."[64] It does not take much to realize that Chief Justice was being overly-simplistic in his assessment.

Section III analyzes the importance for cyber-vigilantes to understand the intricacies of a sting, and why training must be required before a private party works with law enforcement.

C. How a Private Party Can Become an Agent of the Government

Any factual inquiry into whether a defendant's constitutional rights were violated must first start with whether or not the cyber-vigilante sting constituted state action, as well as whether the private party was an agent of the government.[65] If the courts rule that such a defined state relationship exists, then they could next determine whether a defendant's rights were also violated.[66]

In *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n*, one of the more recent Fourteenth Amendment cases, the Supreme Court discussed the requirement of state action.[67] The Court held that "state action may be found if, though only if, there is such a 'close nexus between the State and the challenged action' that seemingly private behavior 'may be fairly treated as that of the state itself.'"[68] This appears to open the door to a constitutional claim extending to groups like Perverted Justice. The result is conceivable in instances in which a private party's conduct is intertwined enough with the government so that courts could find state action.[69]

The Court appears to admit that any inquiry into state action is complex,[70] and that as a result the fact intensive inquiry "lack[s] rigid simplicity."[71] For each case, the Court denotes that there will be a full factual inquiry before determining state action, and that "no one fact can function as a necessary condition across the board for finding state action; nor is any set of circumstances absolutely sufficient, for there may be some countervailing reason against attributing activity to the

63. *Id.*

64. *See id.* at 809.

65. United States v. Jarrett, 338 F.3d 339, 344–45 (4th Cir. 2003).

66. *See id.* at 346–47.

67. 531 U.S. 288, 295 (2001).

68. *Id.* (quoting Jackson v. Metro. Edison Co., 419 U.S. 345, 351 (1974)).

69. *See id.* at 302.

70. *See id.* at 295 (stating that the Court's cases "try to plot a line between state action subject to Fourteenth Amendment scrutiny and private conduct (however exceptionable) that is not").

71. *Id.*

government."[72] This is the issue that occurs with cyber-vigilante cases. There is no one set of facts to look at in determining whether groups like Perverted Justice meet the definition of state actor. Each case must be viewed separately. The Court does provide guidance by showing specific instances in which the Court found state action.[73] The Court states:

> We have, for example, held that a challenged activity may be state action when it results from the State's exercise of "coercive power," when the State provides "significant encouragement, either overt or covert," or when a private actor operates as a "willful participant in joint activity with the State or its agents." We have treated a nominally private entity as a state actor when it is controlled by an "agency of the State," when it has been delegated a public function by the State, when it is "entwined with governmental policies," or when government is "entwined in [its] management or control."[74]

Obviously each instance is different. However, these numerous examples illustrate the strong need for cyber-vigilantes to be educated as to their potential status as state actors. This helps ensure that they follow legal means during a sting.

D. What Constitutes Entrapment

As the case of Dr. Wolin illustrates,[75] a suspected pedophile caught in an online sting will almost always raise the entrapment defense.[76] The issue is whether it will be successful against a private party who, although working for law enforcement, ultimately conducted the sting. Perverted Justice answers the question of whether its actions constitute entrapment by stating: "No. Not on any level. . . . Entrapment is a situation where you go out of your way to entice a citizen *as law enforcement* to commit a crime they otherwise would not commit."[77]

---

72. *Id.* at 295–96.

73. *See id.* at 296 ("Our cases have identified a host of facts that can bear on the fairness of such an attribution [to the state].").

74. *Id.* (citations omitted).

75. *See supra* text accompanying notes 29–41.

76. *See* Hanson, *supra* note 48, at 535–36 (stating that "[d]efendants are . . . likely to invoke the entrapment defense with increasing frequency" due to the "potential for overzealous law enforcement in cyberspace").

77. Perverted-Justice.com, http://www.perverted-justice.com/index.php?pg=faq (follow "Is it entrapment? A.+" hyperlink) (last visited Aug. 18, 2008) (emphasis added).

Entrapment has been a cornerstone defense for criminals when an arrest has been the result of a government coordinated sting.[78] The issue of private groups conducting online stings is relatively new; however, there are many similar situations where private citizens have worked hand in hand with the government.[79] It is important to analogize cases where entrapment has been successful with the more unique situation where cyber-vigilantes work with the government to catch sex-predators.

An entrapment defense consists of two elements: first, "government inducement of the crime," and second, "lack of predisposition on the part of the defendant to engage in the criminal conduct."[80] Further, entrapment is defined as "[a] law-enforcement officer's or government agent's inducement of a person to commit a crime, by means of fraud or undue persuasion, in an attempt to later bring a criminal prosecution against that person."[81] In referring to the entrapment defense, the Ninth Circuit in *United States v. Davis* ruled that "[i]nducement must be provided by someone acting for the government."[82] However, it also stated that "the government cannot make use of an informer and then claim disassociation."[83] The court concluded that if "the informant was clearly acting on behalf of the government before inducing a defendant, the informant is an agent of the government."[84] It is crucial to understand that the government inducement prong only becomes applicable to cyber-vigilantes should they first be classified as government agents. The case above suggests that it is entirely plausible to find a private party "acting for the government" for purposes of the entrapment defense.

Although the stings at the heart of this paper do not involve hacking into another's computer, the most analogous case in determining whether an agency relationship is formed between groups like Perverted Justice and law enforcement is *United States v. Jarrett.*[85] In *Jarrett*, the court

78. *See* Hanson, *supra* note 48, at 536 ("The ease with which law enforcement officials can assume false identities in cyberspace and the suitability of cyberspace for consensual or victimless crimes indicate a probable increase in undercover sting operations. Defendants are therefore likely to invoke the entrapment defense with increasing frequency.").

79. *See, e.g.*, United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003) (determining whether a computer hacker was acting as government agent when he searched the defendant's computer for pornography).

80. Mathews v. United States, 485 U.S. 58, 63 (1988).

81. BLACK'S LAW DICTIONARY 573 (8th ed. 2004).

82. 36 F.3d 1424, 1430 (9th Cir. 1994).

83. *Id.* at 1430 n.2 (citing Sherman v. United States, 356 U.S. 369, 375 (1958)).

84. *Id.* (citing *Sherman*, 356 U.S. at 345; United States v. Busby, 780 F.2d 804, 806–07 (9th Cir. 1986)).

85. 338 F.3d 339 (4th Cir. 2003).

was faced with the issue of whether a computer hacker was acting as a government agent when he searched Jarrett's computer for child pornography.[86] If the hacker was a government agent at the time of the search, it would have been in violation of Jarrett's Fourth Amendment rights.[87] Although the court and the parties both conceded that an agency relationship existed, the timing of the formation was crucial to determining the outcome.[88] The court stated that "[b]ecause the Government did not know of, or in any way participate in, the hacker's search of Jarrett's computer at the time of the search, the hacker did not act as a Government agent."[89]

The facts of the case are not controverted.[90] The computer hacker, referred to as Unknownuser, acting on his own initiative hacked the computer of an alleged child pornographer, Dr. Bradley Steiger.[91] Unknownuser found evidence of child pornography and anonymously sent the information to the FBI and local law enforcement.[92] Steiger attempted to appeal his conviction on the grounds that Unknownuser was a government agent; however, the Eleventh Circuit "reason[ed] that Unknownuser acquired all of the relevant information about Steiger before he contacted law enforcement, and thus was, at all material times, acting as a private individual."[93] After the fact, the agent in charge of the Steiger case e-mailed and telephoned Unknownuser in order to gauge his interest in testifying and further helping law enforcement.[94] The agent, James Duffy, stated in an e-mail to Unknownuser, "If you want to bring other information forward, I am available."[95]

It was not until five months later that Agent Duffy again tried contacting Unknownuser to see if he would be interested in appearing as a witness in the Steiger trial.[96] Unknownuser responded in the negative.[97] Then the agent received an unsolicited e-mail from Unknownuser stating that he had "found another child molester."[98] The

86. *See id.* at 340.
87. *Id.*
88. *See id.* at 346 (noting that Jarrett's computer was hacked by Unknownuser *before* government contact or involvement).
89. *Id.* at 340–41.
90. *Id.* at 341.
91. *Id.*
92. *Id.*
93. *Id.* at 341 n.1 (citing United States v. Steiger, 318 F.3d 1039, 1045–46 (11th Cir. 2003)).
94. *Id.* at 341.
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.* at 342.

reference to "another child molester" was the defendant, William Jarrett.[99] Upon receipt of the incriminating evidence, the government applied for and received a search warrant.[100] The search and subsequent arrest took place on December 13, 2001.[101] Shortly thereafter, Agent Margaret Faulkner contacted Unknownuser and, according to the court, "engaged in what can only be characterized as the proverbial 'wink and a nod.'"[102] The exact e-mail is as follows:

> I can not [sic] ask you to search out cases such as the ones you have sent to us. That would make you an agent of the Federal Government and make how you obtain your information illegal and we could not use it against the men in the pictures you send. But if you should happen across such pictures as the ones you have sent to us and wish us to look into the matter, please feel free to send them to us . . . . But as long as you are not "hacking" at our request, we can take the pictures and identify the men and take them to court.[103]

In further response, the hacker "suggested in no uncertain terms that he would continue to search for child pornographers using the same methods employed to identify Steiger and Jarrett."[104] As a result of the e-mail chain, the district court ruled that, "the Government and Unknownuser had 'expressed their consent to an agency relationship,' thereby rendering any evidence obtained . . . inadmissible."[105] The Government appealed the suppression ruling.[106]

The appellate court was faced with the task of determining whether Unknownuser was acting as a private individual or a government agent.[107] If Unknownuser was a government agent, then surely Jarrett's Fourth Amendment protections were violated.[108] The Fourth Circuit stated that "[d]etermining whether the requisite agency relationship exists 'necessarily turns on the degree of the Government's participation in the private party's activities, . . . a question that can only be resolved "in light of all the circumstances."'"[109] The court further reasoned that "[i]n order to run afoul of the Fourth Amendment . . . the Government

99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.* at 343.
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.* at 344.
108. *See id.*
109. *Id.* (quoting Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989)).

must do more than passively accept or acquiesce in a private party's search efforts, [but] [r]ather, there must be some degree of Government participation in the private search."[110]

The standard set by the court is as follows: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation."[111] Part III addresses how this standard can be modified in order to determine whether groups like Perverted Justice are in fact government agents.

United States v. Gamache is another case that illustrates how a defendant may successfully raise the entrapment defense.[112] Local law enforcement conducted the sting operation that caught the defendant; however, because of the "traveling in interstate commerce" implications, the case was tried in federal court.[113] The First Circuit looked at the issues and determined that the defendant met the burdens required to receive an entrapment instruction.[114] As a result, the conviction was thrown out and a new trial set.[115]

The facts in *Gamache* are relatively straightforward. The sting began in 1995 when law enforcement in New Hampshire placed a classified ad in a swingers-magazine which stated, "female, 31; Single mom, two girls, one boy, seeks male as partner and mentor, seeks fun, enjoys travel and photography."[116] Law enforcement knowingly used the word "mentor" in the hopes that it would "draw out only persons who were interested in 'inter-generational sexual interaction between adults and children.'"[117] Gamache responded to the advertisement, but believed mentor meant the woman was just "looking for somebody to take care of her kids like they do nowadays . . . [f]inancially, take them fishing, hunting, whatever."[118] The correspondence continued and each time the government piqued the defendant's curiosity more, until the defendant committed the crime.[119] The court concluded that the Government initiated contact with Gamache and also continued sending correspondence, even when "it became apparent, from the initial letters,

110. *Id.*
111. *Id.*
112. 156 F.3d 1 (1st Cir. 1998).
113. *Id.* at 8.
114. *Id.* at 12.
115. *Id.*
116. *Id.* at 3.
117. *Id.*
118. *Id.*
119. *See id.* at 3–7.

that appellant was on a different wavelength than the detective."[120] The court reasoned that it was through the government's persistence that "[a]ppellant ultimately became ensnared by the detective's artifice."[121] The court ultimately concluded "that it was the Government's insistence and artful manipulation of appellant that finally drew him into the web skillfully spun by the detective."[122]

E. Constitutional Implications

The state action doctrine comes from the United States Supreme Court's interpretation of the Fourteenth Amendment prohibition, "[n]o State shall."[123] The "general principle" is easily stated: constitutional rights "operate only against the government."[124] This Comment analyzes several possible scenarios where a defendant caught in a cyber-sex sting could assert constitutional claims.

First, the Fourth Amendment gives private citizens the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[125] Part III analyzes a hypothetical instance in which a cyber-predator's Fourth Amendment rights are violated by a cyber-vigilante. Second, the Fifth Amendment states that no person shall "be deprived of life, liberty, or property, without due process of law."[126] As discussed later in Part III, this Comment purposefully does not address in detail the relevant implications of the Fifth Amendment Due Process Clause, nor the *Miranda v. Arizona* [127] problems that undoubtedly exist. A mention of the Fifth Amendment, however, is included to reiterate the potential pitfalls that await a cyber-

120. *Id.* at 10.

121. *Id.*

122. *Id.*

123. Alan R. Madry, *Private Accountability and the Fourteenth Amendment; State Action, Federalism and Congress*, 59 MO. L. REV. 499, 500 (1994). Amendment XIV, Section 1 of the U.S. Constitution states:

> All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. *No State shall* make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

U.S. CONST. amend. XIV, § 1 (emphasis added).

124. David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1229 (1999).

125. U.S. CONST. amend. IV.

126. U.S. CONST. amend. V.

127. 384 U.S. 436 (1966).

vigilante who fails to follow law enforcement protocols, including all relevant constitutional standards of conduct.

Finally, the Fourteenth Amendment's applicability goes beyond the initial prohibition against certain state action.[128] The Fourteenth Amendment's Due Process Clause states, "nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."[129] As Part III analyzes, this becomes almost the catch-all provision that a defendant will likely use if they do assert a constitutional violation.

If a court first finds that there was a constitutional violation, the defendant could seek redress through 42 U.S.C. § 1983. The applicable portion of § 1983 states:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress . . . .[130]

As with entrapment, these claims are only applicable when the defendant was a representative acting on behalf of the state.[131] The Supreme Court in *Lugar v. Edmondson Oil Co.* held that "conduct satisfying the state-action requirement of the Fourteenth Amendment satisfies the statutory requirement of action under color of state law."[132]

Ultimately, a defendant has several options should a cyber-vigilante group cross the line during an online sting. However, the first question will always be whether or not the cyber-vigilante is an agent of the government.

---

128. *See* U.S. CONST. amend. XIV, § 1 (stating the prohibition, "[n]o State shall").

129. *Id.*

130. 42 U.S.C. § 1983 (2000).

131. *See* 14A C.J.S. *Civil Rights* § 369 (2006) ("[T]he wrongdoer must actually represent the State whereby his or her act is the act of the State." (quoting Warren v. Cummings, 303 F. Supp. 803, 805 (D. Colo. 1969))).

132. 457 U.S. 922, 935 n.18 (1982).

III. ANALYSIS

A. The Possibility of a Cyber-Vigilante Reaching Government Agent Status

The advent of cybercrime, specifically cyber-pedophilia, has increased governmental attention to a national problem.[133] Concurrently, the trend of private groups joining the war against cyber-pedophiles appears to be an "unavoidable reality."[134] When private groups work anonymously and outside the knowledge of law enforcement, it is easy to conclude that their conduct "is generally not encompassed by the constitutional and statutory restrictions that apply to law enforcement investigations."[135] The difference arises when law enforcement is aware of the private-party's conduct and subsequently creates a strong connection to the actions of the private party. Recruitment by law enforcement and use of resources to investigate crime are just a few things that would justify a leap from the realm of private action to that of a government agent.[136] Brenner and Clarke suggest that this collaboration offers headaches in the legal world of public-private investigative activities.[137] They state: "Our law assumes public efforts or private efforts; it is not calibrated to deal with public-private efforts. . . . [T]he statutory and constitutional standards that govern law enforcement do not apply to civilians unless, and until, law enforcement officers recruit a civilian to participate in reacting to a crime."[138]

A valid defense against a cyber-vigilante first requires a determination of the group's association to law enforcement. Anthony Dillof argues in his article, *Unraveling Unlawful Entrapment*, that privately and publicly entrapped pedophiles have the same mindset in regards to their belief that the person they communicated with on the Internet was in fact a minor.[139] Even so, the only time a valid defense or constitutional challenge may be raised is if the private party's status reaches that of a government agent.[140] As the court in *United States v.*

133. *See* FBI, *supra* note 1 (Between 1996 and 2006, opened cases rose from 113 to 2135).

134. Brenner & Clarke, *supra* note 8, at 674.

135. *Id.*

136. *Id.* at 675.

137. *Id.* at 685.

138. *Id.*

139. Anthony M. Dillof, *Unraveling Unlawful Entrapment*, 94 J. CRIM. L. & CRIMINOLOGY 827, 846 (2004).

140. *See id.* ("Governmentally and privately entrapped individuals share the same subjective beliefs about the circumstances surrounding their illegal conduct, and therefore, all things equal, are

Barnett held, "'[e]ntrapment as a defense occurs only when criminal conduct is the product of the creative activity of government officials or those private citizens acting under government direction.'"[141] It is when cyber-vigilantes like Perverted Justice coordinate with law enforcement and provide their expertise and cooperation that they arguably become agents of the government. If cyber-vigilantes are agents of the government, then they must be trained in the rules and procedures of law enforcement. Otherwise, convictions will be put at risk.

To illustrate how a private party may become an agent of the government, one author writing on instances of "private entrapment" analogized using the Biblical story of Job to show the interconnectedness of the principal (God) and his agent (Satan) in tempting Job.[142] He stated:

> Only in Job has the one seeking to induce the wrong been *commissioned by the one who would punish it*. Similarly, in our temporal justice system, only when the one inducing or prompting the crime is working as an agent of the state does entrapment even enter into the picture.[143]

If Perverted Justice or another cyber-vigilante group works alone and conducts stings through its own initiative, then there does not appear to be a problem. However, if that same cyber-vigilante works intimately with law enforcement, the court could find the group was acting as a government agent. Ultimately, under theories of entrapment law, if the cyber-vigilante is acting as a private party, then there is no entrapment; conversely, if the courts find cyber-vigilantes are government agents, then an entrapment defense *may* lead to an acquittal.[144]

Each case is extremely unique and each sting a cyber-vigilante conducts provides the facts a judge will look at as the basis for the ruling.[145] Therefore, it is altogether likely that in some instances a court will find a cyber-vigilante group's connection with law enforcement is so interrelated that state action exists, while in other circumstances it does not reach that level. It is these uncertainties that must alert cyber-vigilantes to the potential risks of their operation.

---

equally culpable. Yet private entrapment is no defense.").

141. 197 F.3d 138, 143 (5th Cir. 1999) (quoting United States v. Dodson, 481 F.2d 656, 657 (5th Cir. 1972)).

142. Andrew Carlon, *Entrapment, Punishment, and the Sadistic State*, 93 VA. L. REV. 1081, 1083 (2007).

143. *Id.*

144. Dillof, *supra* note 139, at 842.

145. United States v. Jarrett, 338 F.3d 339, 345 (4th Cir. 2003).

Cyber-vigilantes must use effective methods of investigation that mirror law enforcement standards. If these groups do not act according to law enforcement methods, they are putting into jeopardy the successful conviction of their targets. Private groups working with law enforcement must be prepared to face the court's ruling regardless of the outcome.

The risks associated with lack of training include a predator escaping conviction and an assured conviction forfeited. It is clear that cyber-vigilante groups and law enforcement must work toward a common purpose, and that any action the parties take must be on sound legal footing. Ultimately, it is this private versus public inquiry that is at the heart of this paper.

B. Entrapment Law—How Analogous Cases Shed Light on the Private/Public Inquiry

In *United States v. Jarrett*, the court set forth a standard that helps future cases analyze the public versus private dilemma.[146] As described in Part II, *Jarrett* involved a private citizen who hacked into computers in order to catch persons possessing child pornography.[147] The standard set forth in *Jarrett*, which is applicable to cyber-predator stings as well, looks to: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation."[148] A modified standard applicable to cyber-vigilantes and sex-predator stings would require the court to determine: (1) whether the Government knew of and allowed a cyber-vigilante group to conduct a sting operation, and (2) whether the group was motivated to help law enforcement convict potential child-predators.

For the first factor, "'[k]nowledge and acquiescence . . . *encompass the requirement* that the government must also affirmatively encourage, initiate or instigate the private action.'"[149] In the cases with Perverted Justice, it is often local law enforcement that initiates the dialogue.[150]

146. *Id.* at 344.

147. *Id.* at 340–41.

148. *Id.* at 344.

149. *Id.* at 345 (quoting United States v. Smythe, 84 F.3d 1240, 1242–43 (10th Cir. 1996)).

150. *See* Perverted-Justice.com, http://www.perverted-justice.com/index.php?pg=faq#cat1 (follow "What is your policy on working with law enforcement" hyperlink) (last visited Aug. 26, 2008) ("If a law enforcement department, detective or agency wants the 'Information First,' they email us, we speak with them on the phone, and work out the details of jurisdiction and what they'd like to see out of the chat-logs we do.").

Also, "[i]t is only by the exercise of some form of control that the actions of one may be attributed to another. Mere knowledge of another's independent action does not produce vicarious responsibility absent some manifestation of consent and the ability to control."[151] So the dialogue on the part of law enforcement must not be mere passive support for the sting, but something more.[152] The easy case is when Perverted Justice decoys are deputized by local law enforcement. It would appear obvious that Perverted Justice would be a state actor for both constitutional purposes and entrapment purposes. Although Perverted Justice has been deputized for some sting operations,[153] the exact number of times is unknown. As a result, the court must employ a case-by-case analysis since no generalized determination could be confidently made.

The argument that groups like Perverted Justice will make is that law enforcement does not assert control over their actions. In *Jarrett*, the government conceded that the e-mail exchange with Unknownuser likely created an agency relationship.[154] The only reason this was not determinative in *Jarrett*, however, was because the Government's acquiescence came after Jarrett's computer had already been hacked.[155] It is clear that control is important; however, it was the time of control and acquiescence that determined the outcome of the case.[156] The Fourth Circuit ruled that "[s]uch after-the-fact conduct cannot serve to transform the prior relationship between [a private party] and the Government into an agency relationship with respect to the search of [defendant]'s computer."[157] In the end, the courts must look to the unique facts of each case to determine what type of relationship was formed, and if a private sting in fact becomes a government operation.[158]

The Fourth Circuit also analyzed the agency relationship as well as the importance of looking at the government's intent when it held:

---

151. *Jarrett*, 338 F.3d at 345 (citing United States v. Koenig, 856 F.2d 843, 850 (7th Cir. 1988)).

152. *Id.* at 346 ("[T]here must be some evidence of Government participation in or affirmative encouragement of the private search before a court will hold it unconstitutional. Passive acceptance by the Government is not enough.").

153. McCollum, *supra* note 16, at 31.

154. *Jarrett*, 338 F.3d at 346.

155. *Id.*; *see also id.* at 347 (stating that although "no such relationship existed" with the government at the time of the computer-hacking, it is probable that the "Faulkner e-mails" would have been sufficient to form an agency relationship had they come before).

156. *Id.* at 346.

157. *Id.*

158. *See id.* at 345 ("[C]ourts should look to the facts and circumstances of each case in determining when a private search is in fact a Government search.").

> [I]n order to bring [a private party] within the grasp of an agency relationship, [the defendant] would have to show that the Government made more explicit representations and assurances . . . that it was interested in furthering its relationship with [the private party] and availing itself of the fruits of any information that [the private party] obtained.[159]

A similar argument can be made between law enforcement's dealings with groups like Perverted Justice. In the Wolin case, the Petaluma police captain stated that the department planned to conduct its own sting, but "sought Perverted Justice for technical assistance."[160] Also, in the events that led up to the Conradt sting and his untimely death, it was Perverted Justice that reached out to law enforcement.[161] Perverted Justice previously assisted the Murphy, Texas Police Department with a small sting; however, soon after, Perverted Justice raised the stakes and offered to have a full scale *Dateline* program on its Murphy stings.[162] According to one source, the Murphy Chief of Police "didn't hesitate" and hoped that the *Dateline* sting operations would "put Murphy on the map."[163] Ironically, it did "put Murphy on the map," but not in the way Chief Myrick likely envisioned.[164]

The statements above reflect law enforcements' willingness to coordinate with Perverted Justice and reap the benefits of a sting. That willingness goes directly to the intent of law enforcement, which was so critical in the *Jarrett* case.[165] Although each case offers unique facts and circumstances, it is entirely possible that cyber-vigilante groups like Perverted Justice are state actors during the limited scope of the sting. The two examples above show more than just "passive acquiescence," which arguably puts the burden on the government to show that it was not in collusion with the cyber-vigilante group. This result propels the private party into state actor territory and allows a defendant to put into question the constitutional validity of the sting.

---

159. *Id.* at 347.

160. Simerman, *supra* note 22, at A1.

161. Dittrich, *supra* note 15, at 238.

162. *Id.*

163. *Id.* at 238–39.

164. In the aftermath of Conradt's suicide, the police, *Dateline*, and Perverted Justice received their share of negative publicity when the local district attorney refused to prosecute any of the twenty-three men originally arrested in the Murphy sting. *See id.* at 243.

165. United States v. Jarrett, 338 F.3d 339, 347 (4th Cir. 2003) ("Jarrett would have to show that the Government made more explicit representations and assurances . . . that it was interested in furthering its relationship [with the sting].").

C. When a Sting Goes Too Far—The Affirmative Defense of Entrapment

When a cyber-vigilante works with law enforcement, the rules undoubtedly change. If a cyber-vigilante's true goal is to put predators behind bars, then there should be enough of an incentive to comport with law enforcement standards. "This is not a game of 'Gotcha!'"[166] Wolin's attorney made this simple argument to the judge during his preliminary hearing, and maintained that such stings are to be used to catch actual sex predators and not to seduce an innocent person into breaking the law.[167] There is an obvious potential for untrained cyber-vigilantes to carry a sting too far. As a result, it is not surprising that the few defendants who have gone to trial raise entrapment as an affirmative defense.[168]

The seminal case of entrapment law is *Sorrells v. United States*.[169] The Court stated that law enforcement may use "[a]rtifice and stratagem" in order to "catch those engaged in criminal enterprise."[170] The difference between what constitutes entrapment and what does not often turns on the motivation of the government.[171] The issue is whether law enforcement officials are trying to induce an otherwise innocent person to commit an offense merely so the government may prosecute.[172] The Supreme Court in *Sorrells* adhered to the general principle of *Butts v. United States*[173] where the Court held:

> The first duties of the officers of the law are to prevent, not to punish crime. It is not their duty to incite to and create crime for the sole purpose of prosecuting and punishing it. Here the evidence strongly tends to prove, if it does not conclusively do so, that their first and chief endeavor was to cause, to create, crime . . . .[174]

It is the very nature of a sting which creates the "potential for overzealous law enforcement" to go too far.[175] It is not hard to imagine a scenario in which a person operating a sting gets frustrated when a

166. John Simerman, *Doctor Will Go to Trial Based on TV Sting*, CONTRA COSTA TIMES, Oct. 19, 2007, at A3.

167. *Id.*

168. *See* Simerman, *supra* note 22, at A1.

169. 287 U.S. 435 (1932).

170. *Id.* at 441 (citing Grimm v. United States, 156 U.S. 604, 610 (1895)).

171. *Id.* at 442.

172. *Id.*

173. 273 F. 35 (8th Cir. 1921).

174. *Id.* at 38.

175. Hanson, *supra* note 48, at 535.

suspected predator does not take the bait. Out of frustration, a cyber-vigilante could cross the line in trying to induce the crime. Obviously, this puts convictions in jeopardy and is precisely what occurred in the highly publicized case of *Jacobson v. United States*.[176] In *Jacobson*, the petitioner was convicted of "violating a provision of the Child Protection Act of 1984" for knowingly receiving child pornography.[177] Over the course of twenty-six months, the government tried various methods to entice Jacobson to order child pornography.[178] Finally, Jacobson ordered a catalog depicting child pornography.[179] When asked about the catalog he stated that "the Government had succeeded in piquing his curiosity."[180] Jacobson argued entrapment, but his defense failed and he was convicted.[181] The court of appeals affirmed the conviction on the ground that the second element of entrapment was not met, namely that Jacobson was "predisposed to break the law and hence was not entrapped."[182] Ultimately, the Supreme Court reversed, saying that the government "overstepped the line between setting a trap for the 'unwary innocent' and the 'unwary criminal.'"[183]

The Court's inquiry in *Jacobson* focused not only on the petitioner's predisposition to commit the crime (there is no dispute he committed a crime), but also whether the government went too far in its inducement.[184] The Court reasoned that the government's zeal cannot "implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute."[185] The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations instruct that "[e]ntrapment must be scrupulously avoided."[186] Federal officials receive training on how to "ensure, insofar as it is possible, that entrapment issues do not adversely affect criminal prosecutions."[187]

176. 503 U.S. 540, 542–43 (1992).
177. *Id.* at 542.
178. *Id.* at 542–44.
179. *Id.* at 547.
180. *Id.*
181. *Id.*
182. *Id.* at 547–48.
183. *Id.* at 542 (quoting in part Sherman v. United States, 356 U.S. 369, 372 (1958)).
184. *Id.* at 542–44.
185. *Id.* at 548 (citing Sorrells v. United States, 287 U.S. 435, 442 (1932)).
186. OFFICE OF LEGAL POLICY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON FEDERAL BUREAU OF INVESTIGATION UNDERCOVER OPERATIONS 16 (2002), *available at* http://www.usdoj.gov/olp/fbiundercover.pdf.
187. *Id.*

These same techniques must be followed by cyber-vigilantes working with law enforcement in order to avoid similar adverse impacts.

According to *Jacobson*, the reason to apply such a stringent standard is to avoid circumstances where "the Government's quest for convictions leads to the apprehension of an otherwise law-abiding citizen who, if left to his own devices, likely would have never run afoul of the law."[188] In such a circumstance, the courts have the discretion to intervene and allow an entrapment instruction to be offered to the jury for consideration.[189]

In Part II of this Comment, the case of *United States v. Gamache* illustrated a scenario in which law enforcement went too far, allowing the alleged predator to mount a successful entrapment defense.[190] To bolster Gamache's argument, "the detective testified that appellant did not even fit a pedophile profile and that there was no evidence that linked him to prior sexual activities with children."[191] Ultimately, it was the government that initiated everything:[192]

> It was the Government that first mentioned the "children" as sex objects; it was the Government that first used sexually explicit language involving the "children"; it was the Government that escalated the subject of sex with children; and it was the Government that first brought up the use of photographic equipment.[193]

Because the Government was the aggressor and initiator, the Court stated that "the evidence raises a reasonable doubt that the Government improperly induced a citizen to commit crimes that he was not predisposed to commit, yet crimes for which he was charged and convicted."[194]

This is where the problem lies. In a noble effort to secure convictions, law enforcement at times crosses the line. If law enforcement has a propensity to be over-eager, how much more do cyber-vigilantes? If cyber-vigilantes do not understand that they are required to follow the protocols of government, then they may potentially initiate and continue dialogue that crosses the line.[195]

188. *Jacobson*, 503 U.S. at 542, 553–54.

189. *Id.*

190. 156 F.3d 1, 2 (1st Cir. 1998).

191. *Id.* at 10.

192. *Id.*

193. *Id.* at 10–11.

194. *Id.* at 12.

195. *See* Donald S. Yamagami, Comment, *Prosecuting Cyber-Pedophiles: How Can Intent Be Shown in a Virtual World in Light of the Fantasy Defense?*, 41 SANTA CLARA L. REV. 547, 567 (2001).

Unfortunately, the consequence is that a defendant may raise an entrapment defense and thus possibly escape conviction. This Comment's purpose is to clarify any potential misconceptions about the agency relationship with government so that cyber-vigilantes may be better prepared to meet court scrutiny. It is possible that a court could rule that a cyber-vigilante was not a government agent at the time of a sting. However, it is in society's interest to have cyber-vigilantes acting according to government protocols, because the ultimate goal is to protect the innocent while prosecuting only those who are guilty.

Therefore, cyber-vigilantes should receive training that is at least on par with law enforcement training. The reason is simple. Training will reduce the likelihood of successful defenses against prosecution. Donald S. Yamagami argues that: "[t]raining the FBI to execute successful sting operations . . . will reduce the likelihood that successful defenses will prevail in court."[196] Thus, law enforcement should never turn over a sting operation to a private party without first providing the private party with the legal means to accomplish it.

According to Yamagami, the fact that the internet transcends physical geographical boundaries "makes it especially difficult for law enforcement agencies to monitor and to apprehend Internet criminals because they cover areas of conflicting police jurisdictions."[197] Cyber-vigilantes have done a public service inside the Internet domain. Often local law enforcement does not have the means to conduct stings, and vigilantes wanting to work with government can help, but there needs to be better training and more accountability when doing so.

To illustrate the danger of losing a case to entrapment, Yamagami analyzes a Ninth Circuit case holding that the defendant was entrapped.[198] The court ruled that "[t]he agents, in overstepping their bounds, offered the recently divorced transvestite via e-mails the possibility of family if he agreed to teach three girls how to have sex."[199] The opinion concluded, "[t]here is surely enough real crime in our society that it is unnecessary for our law enforcement officials to spend months luring an obviously lonely and confused individual to cross the line between fantasy and criminality."[200] Cyber-vigilantes must realize that if they cross the line, all the good they do can be compromised.

196. *Id.* at 550.
197. *Id.*
198. *Id.* at 558 (citing United States v. Poehlman, 217 F.3d 692, 705 (9th Cir. 2000)).
199. *Id.* (citing *Poehlman*, 217 F.3d at 695).
200. *Id.* (citing *Poehlman*, 217 F.3d at 705).

It can certainly be argued that entrapment is not that successful of a defense; so why does it matter? In Yamagami's article, he states: "Even though entrapment has not been found in many of these cases, many judges are wary of undercover agents acting as young girls and encouraging otherwise innocent people to commit crimes."[201] Yamagami quoted a Maryland public defender who stated: "Agents are likely to encourage, or at least continue a conversation that turns sexual when an actual child likely would end it."[202] Yamagami further opines that "[a]lthough FBI agents have always had to pass the rigorous FBI academy and go through specialized training on investigations of computer-related child exploitation crimes, the training must be more legally focused."[203] If the FBI recognizes the need for specialized training, it would be naïve and presumptuous to suggest that private groups are better equipped to handle the intricacies of the law without such focused and intense training. Even though entrapment may not be successful, the potential for over-zealousness needs to be reined in to assure a legal sting occurs. Effective training is the key to reach that end.

D. How Constitutional Implications Could Affect the Cyber-Vigilante/Law Enforcement Relationship

Entrapment is historically only a statutory or common law defense.[204] However, imagine a scenario in which a defendant challenges a sting based on a claim that his constitutional rights were violated. As with entrapment, the courts would need to address whether the private party's participation was state action.[205] If a court determines that there is state action, then the court can address the question of whether a constitutional violation occurred.

In Alan Madry's article on private party accountability under the Fourteenth Amendment, he states that "[i]f a state sufficiently 'involves' itself in private conduct, then the private conduct is itself state action, the private party a state actor, and the conduct is subject to the standards of the Fourteenth Amendment."[206] As a result, the state action doctrine is generally inapplicable to excluding evidence uncovered by private

201. Yamagami, *supra* note 195, at 567.

202. *Id.*

203. *Id.* at 574 (footnote omitted).

204. *See* Dru Stevenson, *Entrapment by Numbers*, 16 U. FLA. J.L. & PUB. POL'Y 1, 7 (2005).

205. *See* 14A C.J.S. *Civil Rights* § 369 (2006) ("The wrongdoer must actually represent the state whereby his or her act is the act of the state, or there is no action under color of state law." (quoting Warren v. Cummings, 303 F. Supp. 803, 805 (D. Colo. 1969))).

206. Madry, *supra* note 123, at 501.

individuals, even if the private individual used means that would otherwise have resulted in a constitutional violation.[207] David Sklansky argues in his article regarding private police work that "[p]rivate policing poses challenges for the state action doctrine because it straddles the divide between ordinary private citizens—a concerned neighbor or vigilant storekeeper—and uniformed police officers."[208]

In determining the existence of state action, the easy case would be if the private party was deputized by law enforcement before carrying out investigative functions.[209] In one instance where Perverted Justice was deputized, it appears that it was local law enforcement that suggested it.[210] This underlines the importance of control and entwinement, theories present in the *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n*[211] case discussed in Part II of this Comment. If similar cyber-vigilantes comply with law enforcement's request to deputize, they must know that they are without question acting as law enforcement, and therefore, the state action doctrine is applicable to their conduct. Any violation during their investigative duties would result in a potential loss of conviction or the defendant invoking other constitutional means of redress.[212] This alone is sufficient to alert cyber-vigilantes of a need to follow strict law enforcement guidelines, specifically while conducting an online sting with the government's approval.

A deputized cyber-vigilante is the easy case. However, what about cases in which the vigilante is not deputized? What level of connection to law enforcement must be evident for the constitutional restrictions to extend to their behavior? This scenario is obviously more common, and thus, the unique facts of each case require a more in-depth analysis on the part of the court.

David Sklansky analyzes *Lugar v. Edmondson Oil Co.*[213] to determine what constitutes state action.[214] In *Lugar*, the court states:

> [T]he party charged with the [constitutional] deprivation must be a person who may fairly be said to be a state actor. This may be because he is a state official, because he has acted together with or has obtained

207. Sklansky, *supra* note 124, at 1229.
208. *Id.*
209. *Id.* at 1229–30.
210. McCollam, *supra* note 16, at 31.
211. 531 U.S. 288, 288–89 (2001).
212. *See infra* Part III.D.3 (discussing 42 U.S.C. § 1983).
213. 457 U.S. 922 (1982).
214. Sklansky, *supra* note 124, at 1247.

> significant aid from state officials, or because his conduct is otherwise chargeable to the State.[215]

Sklansky then looks to a more current case that describes the above elements as fact-intensive.[216] In *Edmonson v. Leesville Concrete Co.*, the court states:

> [O]ur precedents establish that, in determining whether a particular action or course of conduct is governmental in character, it is relevant to examine the following: the extent to which the actor relies on governmental assistance and benefits, whether the actor is performing a traditional governmental function, and whether the injury caused is aggravated in a unique way by the incidents of governmental authority.[217]

A court would obviously be required to look at each of these elements and determine the likelihood that state action occurred. The first element would require a fact-specific study in order to determine the level of reliance a cyber-vigilante had on law enforcement. The second element seems obvious as a cyber-vigilante is clearly performing a traditional government function that is typically reserved to law enforcement. As compared to the entrapment analysis earlier in this Comment, it is evident that the burden on a defendant to prove state action is quite heavy. Nonetheless, logic dictates that training would lessen the chance that a defendant could successfully raise a constitutional challenge.

1. Fourth and Fifth Amendment Possibilities

The Fourth Amendment prohibits "unreasonable searches and seizures," and grants privacy considerations to each person, his or her house, papers, and effects.[218] Perverted Justice uses a decoy to chat online with a predator; if a call is placed, Perverted Justice relies on public phone directories to find out the identity of the perpetrator.[219] There is no apparent violation for using such publicly accessible information, and therefore, construed under this light, there would likely be no search. The author can only hypothesize of an unlikely scenario where a cyber-vigilante posing as law enforcement coerces a private company to disclose the identity of a computer user. It would be this

215. *Id.* (citing *Lugar*, 457 U.S. at 937).
216. *See id.* at 1247–48.
217. *Id.* (quoting Edmonson v. Leesville Concrete Co., 500 U.S. 614, 621–22 (1991)).
218. U.S. CONST. amend. IV.
219. Dittrich, *supra* note 15, at 236.

scenario that could offer a defendant the right to succeed on Fourth Amendment grounds, assuming that a court first finds the private party's conduct to be state action.

The facts necessary to support a Fourth Amendment claim are not likely present in most online sting operations; however, the Court's ruling in *Conradt v. NBC Universal, Inc.*[220] shows that it can happen. *Dateline* was allegedly heavily involved in the decision to secure a warrant and to use a SWAT team.[221] As a result, Judge Chin denied NBC's motion to dismiss the Fourth Amendment claim and stated that "a reasonable jury could find that the intrusion on Conradt's privacy substantially outweighed the promotion of legitimate governmental interests."[222] Obviously the *Conradt* case is unique because *Dateline*'s alleged misconduct did not come directly out of the online sting, but through the enforcement and legitimacy of the warrant. However, the fact that a private party's conduct could potentially lead to a successful Fourth Amendment claim must put cyber-vigilantes on notice.

This Comment will also not spend time looking into the Fifth Amendment as a source for possible constitutional violations. The scope of this paper is narrow, and includes only half of the debate as to issues surrounding *Dateline*'s "To Catch a Predator." Another paper could be written which looks at the interaction of the media in relation to the alleged predators. Such a paper might focus on whether *Dateline*'s affiliation with Perverted Justice, who in turn works with law enforcement, constitutes some type of state action on the part of the media.[223]

2. The Fourteenth Amendment—Due Process Implications and State Action

If a defendant argues that his constitutional rights were violated by a cyber-vigilante coordinated sting, the most likely avenue for a claim is the Due Process Clause. However, even a Due Process claim will be extremely hard to prove. In an article on sting operation procedures and the potential entrapment defense, Bruce Hay suggests: "Sometimes a defendant may establish that the government's conduct was so

220. 536 F. Supp. 2d 380 (S.D.N.Y. 2008).

221. *Id.* at 390.

222. *Id.*

223. *See, e.g.*, Wilson v. Layne, 526 U.S. 603, 604 (1999) (noting similar issues of police-media cooperation); *see also* Dittrich, *supra* note 15, at 244 (arguing that NBC used the police to do what they themselves could not ethically do as journalists).

outrageous that it violated the federal Due Process Clause, but this is exceedingly unusual. Virtually all entrapment cases are based on common law or (in the case of some states) on statutes."[224] Kansas case law suggests that if a court does not find outrageous conduct, and thus no Fourteenth Amendment violation, then entrapment is always a fall-back.[225] This implies that the outrageous conduct standard for a Fourteenth Amendment violation is a heavy burden for a defendant to prove.

The Kansas Supreme Court requires four elements to prove outrageous government conduct: "the type of criminal activity involved, whether the activity is preexisting or instead 'instigated' by the government, whether the government is directing the activity or merely participating in it, and the causal link between the government's conduct and the acts of the defendant."[226] A court must look to the facts of the case and individually determine whether the "outrageous conduct" elements were met. Because of the fact-intensive nature of this constitutional challenge, it would be difficult to show how often this sort of claim would be successful. However, one court stated: "In order to constitute a due process violation, the government's conduct must be so outrageous as to shock the conscience of the court."[227] If state action were to be found, it is possible that a complaining defendant might bring facts sufficient to "shock the conscience" of the court. Once again, *Conradt v. NBC Universal, Inc.* offers insight into the potential for success on Fourteenth Amendment grounds.[228] Judge Chin denied NBC's motion to dismiss the Fourteenth Amendment claim stating that the "complaint also asserts a *plausible* claim that the police and NBC acted with deliberate indifference to Conradt's rights and the risk of suicide, and that they acted in a manner and with a state of culpability that would shock one's conscience."[229] Although it is true that this claim was never decided by a jury on the merits, it still shows that such a claim is possible. It gives continued credence to the notion that cyber-vigilante groups working with law enforcement must be trained properly in order to avoid even the small chance that a constitutional claim could be successful.

224. Hay, *supra* note 52, at 399 n.31.
225. *See* State v. Van Winkle, 864 P.2d 729, 731 (Kan. 1993).
226. *Id.* at 734 (citing State v. Nelson, 822 P.2d 53, 58 (Kan. 1991)).
227. United States v. Osborne, 935 F.2d 32, 36 (4th Cir. 1991).
228. 536 F. Supp. 2d 380, 394–95 (S.D.N.Y. 2008).
229. *Id.* (emphasis added).

3. 42 U.S.C. § 1983 Claims for Redress

What happens if a defendant argues that his constitutional rights were violated, whereupon, the court finds the cyber-vigilante's conduct was state action? The defendant's likely recourse would be to bring a § 1983 civil rights claim against the government seeking redress. Section 1983 allows a claimant to bring a civil claim when he or she alleges that his or her constitutionally secured rights were violated by a person acting under the "color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia."[230]

Section 1983 claims are only a problem if a court first decides that there is state action. In such an instance, a "state or local government may be responsible . . . for the acts of a private entity if the state has exercised coercive power or has provided such significant encouragement, either overt or covert, that the private action must be deemed state action."[231] Obviously the language stating that "coercive power" and "significant encouragement" must be present, make this a pretty large hurdle to overcome. However, once again it is important to note that the risks are too high to gamble on "what-ifs?" Without proper training, a scenario could occur where the zeal to convict a cyber-predator leads the government to enlist the help of a cyber-vigilante group, and thereafter, the government goes too far in its encouragement and control. Should this scenario occur, it is possible that a defendant predator could bring a § 1983 claim against the government so long as the court first determined that a constitutional violation occurred.

E. Cyber-Vigilantes Must Be Trained and Accountable to Law Enforcement Before Conducting Cyber-Predator Sting Operations

This section addresses the possible solutions to the cyber-vigilante problem. It is first important to understand the difficulty of setting a legal sting. Audrey Rogers states: "To sufficiently establish a defendant's intent, law enforcement must conduct sting operations in a manner that makes it abundantly clear that the defendant is aware that he is communicating with an apparent 'child.'"[232] Some of the other factors Rogers mentions are "time frame, quantity, and content of the

230. 42 U.S.C. § 1983 (2000).

231. *See* 1 CIVIL ACTIONS AGAINST STATE AND LOCAL GOVERNMENT: ITS DIVISIONS, AGENCIES, AND OFFICERS § 7:95, at 403 (Jon L. Craig ed., 2d. ed. 1992) (citing Sibley v. Lutheran Hosp. of Md., Inc., 871 F.2d 479 (4th Cir. 1989); Wong v. Stripling, 881 F.2d 200 (5th Cir. 1989)).

232. Rogers, *supra* note 11, at 516.

communications [which] are crucial in assessing the defendant's intent."[233] Apart from admissibility implications, evidence must be gathered scrupulously to ensure the court can determine the intent of the cyber-vigilante. This information is also necessary to prove whether or not a defendant was entrapped.

In Dru Stevenson's article, *Entrapment by Numbers*, he discusses the accountability of law enforcement and what it must do to ensure that their methods comport with the law.[234] He specifically discusses the negative consequences of shoddy police work.[235] Stevens states: "It is easy, both in the sense of being simple and cheap, for officers or agents to troll on-line chatrooms posing as adolescents seeking sexual experimentation to lure pedophiles into extended correspondence while accumulating incriminating evidence from conversations and e-mailed images."[236] If it is easy and cheap for law enforcement to get involved in setting cyber-stings, it follows that it is also easy for private citizens to get involved. Stevens concurs by stating that "[c]atching pedophiles can be done mostly from a cubicle in an office."[237] The proliferation of the Internet has created the cyber-vigilante phenomenon.[238] Stevens states: "Historically this was not a problem because most individuals, even if they had the motivation to entrap others, did not have the resources to orchestrate a sting while protecting themselves from retaliation if caught. . . . The Internet has changed this, for better or worse . . . ."[239] And for better or for worse, cyber-vigilantes working with law enforcement must be properly trained.

The evidence chain is intricate, and it is important that non-law-enforcement personnel understand how it works. Perverted Justice does appear to have a solid evidence gathering chain.[240] However, as was

233. *Id.*

234. Stevenson, *supra* note 204.

235. *Id.* at 68–69.

236. *Id.* at 68.

237. *Id.* at 69.

238. *Id*. at 70.

239. *Id.*

240. *See* Perverted-Justice.com, http://www.perverted-justice.com/?pg=faq (follow "How can this stuff be used in a court of law? A.+" hyperlink) (last visited Aug. 18, 2008) ("For example, each conversation we have with a wannabe pedophile is double-recorded . . . . When a contributor logs onto Yahoo, their conversations are automatically recorded in an encrypted format not only on that contributor's computer, but a secure server located in another state. A server that the individual contributor cannot get access to. That means that every keystroke is captured in picturesque condition on two different computers. To say that the 'conversation was made up' would require a defense attorney to alledge [sic] that two different people, in two different states, who have likely never met in person . . . conspired together to 'frame' someone else who neither had any previous knowledge of."). The rest of Perverted Justice's techniques remain a mystery. They claim: "[W]e

argued by the district attorney in Texas, even the best planned evidence can be compromised.[241]

Finally, as Monica Shah states in her article about the influence of private parties in cyberspace: "If the case law on electronic vigilantism opens the door for other private entities to utilize aggressive investigative techniques to combat cybercrime, cyberspace will look much more like a gated community, a university patrolled by private police, or a department store with its own holding cell and armed guards."[242] Although Shah's article is mainly directed at cyber-vigilante hackers instead of groups like Perverted Justice, it is clear that one reason law enforcement utilizes cyber-vigilantes is because of their expertise.[243] Cyber-vigilantes can be a valuable asset to law enforcement so long as the training is accomplished first. Law enforcement must always question first whether working with a cyber-vigilante group is in the department's best interest. If it is worth it, then the cyber-vigilante group must consent to training. All the expertise is worthless if cyber-vigilantes do not understand how to avoid the pitfalls of entrapment and other constitutional challenges.

IV. CONCLUSION

Audrey Roger's article on sting operations offers perspective in the way in which law enforcement should confront the phenomenon of cyber-sex crimes.[244] She argues: "The ability to perpetrate crimes against children by use of the Internet is unprecedented . . . . Just as pedophiles have vastly increased access to children through the Internet, law enforcement must have access to pedophiles by means of sting operations."[245] There is a societal interest in catching cyber-predators before they prey on unsuspecting children; however, the methods used must be legal and follow strict evidentiary protocols. Each jurisdiction is unique, and thus, specialized training is required. When amateurs are

---

also use other forms of evidence-collection that we cannot reveal, except to interested law enforcement as we're not apt to give up all our tricks and technology up [sic] publicly." *Id.* The author sent an e-mail to Perverted Justice on September 15, 2007, requesting the undisclosed information. Perverted Justice has yet to respond.

241. Dittrich, *supra* note 15, at 243.

242. Monica R. Shah, Comment, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace*, 105 COLUM. L. REV. 250, 273 (2005).

243. *See id.* at 271 (arguing that "law enforcement is well aware of the skills of well-intentioned [cyber-vigilantes] and intends to capitalize on any help it can get").

244. Rogers, *supra* note 11, at 523.

245. *Id.*

working with law enforcement, the standard must be equal to that of law enforcement officials.

"[R]ights of suspected and convicted pedophiles are routinely violated and nobody cares. The rules of evidence are stretched . . . [though] as a parent, . . . I'm okay with it."[246] This statement, although understandable, highlights the need for greater scrutiny on cyber-vigilantes. When cyber-vigilantes like Perverted Justice are trained and prepared, justice more often than not will prevail. It is possible to secure a conviction on legal and ethical principals which leaves no doubt as to a convicted person's guilt. Therefore, cyber-vigilantes value to law enforcement increases in direct proportion to their preparedness.

This Comment shows a need for cyber-vigilantes and government to understand the implications of working together. Both parties must address the viability of such an option. First, does law enforcement want to work with private citizens, and if so, what level of control should it assert over the operations? Second, do cyber-vigilantes want to have an arms-length approach like that of Unknown user in *Jarrett*? Both parties must make these determinations before they forge any type of relationship. The stakes have been raised and cyber-vigilantes who work with law enforcement must be extremely careful to avoid constitutional pitfalls should they be classified as state actors. Even though this Comment has addressed the unlikelihood that state action would be present in *all* such coordinated stings, it is in the best interest of both law enforcement and private cyber-vigilantes to be prepared. Training should be required specifically when law enforcement works "hand in hand" with private parties. The benefit of these extra precautions will be well worth it when all cyber-predators caught receive their just punishment.

246. Yamagami, *supra* note 195, at 565–66 (quoting Bill Bickel, *The War Against Pedophiles* (Jan. 3, 2000), http://crime.about.com/library/weekly/aa101299.html).