September 23, 2009

Shooting an Unarmed, Defenseless, Innocent Man: The Ineffectiveness of the Entrapment Defense in Cyberspace

James E Simmons

Available at: https://works.bepress.com/james_simmons/1/
Tom is an avid chat room, discussion board, forum attendee, and Internet blogger. He is 45 years old, lonely, and enjoys fantasies of meeting younger women. Tom enjoys the freedoms of cyberspace because he can go to different chat rooms, meet women, and he can do all of this anonymously under fabricated usernames. According to Tom’s fantasy, his “dream woman” is a young 18 year old who enjoys being “naughty” on occasion. In order to chat with women that fit these criteria, Tom only visits “barely legal” sites, which promote racy chat forums among young adults.

One day while chatting on a “barely legal” site, Tom met Blondie12 who said, “She and her sister enjoy getting to know older men.” Tom then asked what she meant by her post. Blondie12 responded by saying, “she likes older men that teach her little sister about the facts of life.” Blondie12 then disclosed that her sister was only 13 years old. Tom later realized that Blondie12 liked to watch older men perform sexual acts with her underage sister. Tom was enjoying his conversation with Blondie12 because she seemed like the “naughty” woman in his fantasy. He didn’t really approve of the comments Blondie12 made in regards to her sister, however, he did not want the conversation with Blondie12 to end. Tom did not address her comments about her sister, but he wanted to exchange email addresses so that they could continue getting to know one another.

Tom and Blondie12 began corresponding via email. Each correspondence from Blondie12 always centered on her 13 year old sister and how she wanted to watch a grown man show her things. Tom always tried to stray away from talking about
Blondie12’s sister because he was more interested in role-playing a relationship with Blondie12. However, in a subsequent email by Blondie12, she stated “if he showed her sister the facts of life, it would make her really happy.” Tom construed this to mean that Blondie12 wanted Tom to role-play her fantasy. Tom then agreed to pleasure her sister, and described some sexually explicit things that he wanted Blondie12 to see him do to her. Tom was only role-playing to satisfy Blondie12’s request, but he never really intended on performing these acts.

After two months of correspondence, Tom felt that Blondie12 could be the woman of his fantasies and he imagined what it would be like to meet her. Blondie12 would repeatedly ask when Tom would show her sister some “life experiences.” After the most recent request Tom decided to use this opportunity to set up a meeting with her. Tom and Blondie12 then arranged to meet at a restaurant the following week.

The next weekend Tom arrived at the restaurant and approached the woman that met the description that Blondie12 gave him. Blondie12 turned and said, “Tom is that you?” Tom nodded yes, and she said, “Nice to meet you, lets go outside so you can meet my sister.” Tom then followed the woman outside. As Tom stepped outside police screaming for him to “get on the ground” surrounded him! Tom realized that Blondie12, the potential woman of his dreams, was actually an undercover law enforcement agent. Tom was then arrested and tried in state court for attempting lewd acts with a minor. His role-playing email communications with Blondie12 were used as evidence to corroborate the States’ case against him. Tom tried to plead entrapment as a defense to the State’s accusations; however, the court found his email communications were sufficient evidence
to rebut his defense claim. Tom was subsequently found guilty and sentenced to 8 years in prison.

--End of Hypothetical--

**Introduction**

Cyberspace is a unique realm separate from the “real world” and poses problematic concerns where the traditional entrapment defense cannot effectively protect the innocent or prevent the abuse of authority by law enforcement. The entrapment defense, therefore, must be re-interpreted to accommodate the realm of cyberspace. The above hypothetical is analogous to many cases of cyberspace predation where innocent defendants are not afforded an effective entrapment defense. In order to remedy these concerns the traditional subjective and objective test of entrapment should be discarded in Internet predation cases. Instead, the legislature should implement a standard that defines predisposition in cyberspace and holds law enforcement to a higher reasonableness standard. Furthermore, law enforcement agencies should develop detailed restrictions regarding deceptive practices. This note exposes the flaws of the traditional Entrapment Defense as applied to Internet predation cases and attempts to determine effective alternatives. Part I discusses the history of the traditional entrapment defense as applied by both the subjective and objective tests. Part II of this note expresses the distinctions between cyberspace and the “real world.” Part III explains how the traditional entrapment defense has been applied to Internet predation cases currently and in the past. Part IV exposes the problems and concerns associated with applying the traditional entrapment tests to Internet predation cases. Finally, Part V discusses plausible remedies and
alternatives to the traditional entrapment defense that can be implemented to ensure
protection of the innocent and prevent abuse of law enforcement authority.

Part I

The history of the Entrapment Defense

The entrapment defense was created in order to resolve two primary concerns: first, it
protects innocent law abiding citizens from committing crimes due to deceptive police
practices, and secondly, it ensures the reasonable allocation of resources by police
agencies when they employ those deceptive practices.\(^1\) As the need to prevent consensual
crimes increased, the entrapment defense was also crafted to limit the scope of deceptive
practices employed by police agencies in apprehending suspects in such crimes.\(^2\)

Stemming from the early 1930’s courts have implemented two tests, the subjective and
the objective, in order to render the entrapment defense effective in preventing the abuse
of police authority and protecting the innocent who have been induced to committing
crime by law enforcement.\(^3\)

\(^1\) Jennifer Gregg, *Caught in the Web: Entrapment in Cyberspace*, 19 HASTINGS COMM. & ENT.
L.J. 157, 171 (1996) (stating that the Entrapment Defense should “balance individual rights and
liberties with legitimate law enforcement objectives…Additionally, the entrapment defense
should also promote the efficient allocation of police resources. The doctrine recognizes that it is
unproductive for police to expend time and energy, or engage in unlawful activity, in order to
induce otherwise law-abiding citizens to commit crime).

\(^2\) See, Fred Warren Bennett, *From Sorrells to Jacobson: Reflections on Six Decades of
Entrapment Law and Related Defenses in Federal Court*, 27 WAKE FOREST L. REV. 829, 831
(1992) (defining consensual crimes as: drug dealing, prostitution, gambling and bribery).

a. The Subjective Test For Entrapment

The 1932 Supreme Court decision in *Sorrells v. U.S.* was the first to apply the subjective test to the entrapment defense.\(^4\) In *Sorrells* the defendant was arrested for possessing and selling alcohol in violation of a prohibition statute when he sold whiskey to an undercover prohibition agent.\(^5\) At trial Sorrells offered testimony and called various witnesses to prove his good character to rebut the prosecution’s allegations that he had a reputation as a “rum runner.”\(^6\) Although the trial court could not produce any evidence that the defendant “ever possessed or sold any intoxicating liquor prior to the transaction in question,” it denied his entrapment defense and sentenced Sorrells to 18 months in prison.\(^7\) The North Carolina Court of appeals affirmed this decision.\(^8\)

This case was then appealed to the Supreme Court, where the Justices crafted the subjective test of entrapment to resolve the issue.\(^9\) According to the Justices, “artifice and stratagem may be employed to catch those engaged in criminal enterprises,”\(^10\) however, “it is unconscionable, contrary to public policy, and to the established law of the land to punish a man for the commission of an offense of the like of which he had never been guilty, either in thought or in deed, and evidently never would have been guilty of if the officers of the law had not inspired, incited, persuaded, and lured him to attempt to

---


\(^5\) *Sorrells*, 287 U.S. at 438.

\(^6\) *Id.* at 440-441.

\(^7\) *Id.*

\(^8\) *Id.*

\(^9\) *Id.*

\(^10\) *Id.* at 441.
commit it.”11 The Justices reasoned that the accused must be scrutinized to determine whether he was predisposed in committing the crime, even if the law enforcement agents never instigated their conduct.12 According to the Court’s subjective analysis, when law enforcement has induced an individual to commit or attempt to commit a crime, the burden shifts to the prosecution to prove beyond a reasonable doubt that the accused was predisposed to committing that crime in order to escape the entrapment defense.13 Since the prosecution could not offer evidence that Sorrells was ever predisposed to possessing or selling alcohol prior to the inducement of the undercover prohibition agent, the Supreme Court held that Sorrells was entrapped, and his conviction must be reversed.14

Sorrells laid the foundation for the subjective test for entrapment.15 Following Sorrells were a line of Supreme Court cases that further defined the importance of predisposition in cases where the accused raised the entrapment defense.16 These rulings solidified the standard for entrapment cases on the federal level to be analyzed using the subjective test.17 These cases have also added additional elements to the predisposition requirement, whereas currently, the accused must be shown to have been predisposed

11 Id. at 444-445 (stating that it is not the officers duty to “incite and create crime for the sole purpose of prosecuting and punishing it”).
12 Id. at 451-452.
13 Id.
14 Id. at 452.
15 Michael O. Zabriskie, If the Postman Always “Stings” Twice, Who is the Next Target? - An Examination of the Entrapment Theory, 19 J. CONTEMP. L. 217, 220 (1993); see also Hanson, supra note 4, at 537-538.
prior to or at the time of law enforcement contact. These Supreme Court decisions do not clarify what factors may be considered to prove predisposition, however, some have required proof that law enforcement was “extremely egregious” in their actions to rebut a claim that the plaintiff was predisposed. Some states, like California, have fashioned their own factors to determine predisposition, such as: the defendant’s character or reputation; whether the government first suggested the criminal activity; whether the defendant profited from the activity, whether the defendant demonstrated reluctance; and the nature of the government’s inducement.

b. The Objective Test of Entrapment

The Objective Test for Entrapment was adopted by a minority of jurisdictions based off of the concurring opinion of Justice Roberts in Sorrells. Under Roberts’ view, the jury should serve as a limit to the scope of authority of law enforcement agencies, and they must look more towards the agencies actions rather than the predisposition of the accused. This Objective Test was also supported by Justice Frankfurter’s concurring

---

20 U.S. v. Poehlman, 217 F.3d 692, 706 (9th Cir. 2000) (dissent stating “the defendant’s reluctance generally receives the greatest weight”).
21 Sorrells v. U.S., 287 U.S. 435, 455 (1932) (Justice Roberts Concurring); see also, Hanson, supra note 4, at 539-540 (stating, “The objective test emerges from his differing view about the fundamental justification for the entrapment defense. Justice Roberts advocated the entrapment defense to protect the integrity of the judicial system rather than to effectuate the intent of congress. For this reason, he did not undertake to evaluate the predisposition character of the defendant. Rather, he focused exclusively on the actions of the government”).
22 Maura F. J. Whelen, Lead us not into (Unwarranted) Temptation: A Proposal to Replace the Entrapment Defense with a Reasonable-Suspicion Requirement, 133 U. PA. L. REV. 1193, 1209-10 (discussing the ineffectiveness of the objective test).
opinion in *Sherman v. U.S.* The Objective test was crafted from concurring opinions and not the majority decisions, however, many states have still adopted the test in their own model penal codes. Therefore, even if the Federal Courts apply the Subjective test in Entrapment cases, there are a minority of states that hold law enforcement agencies under more scrutiny than the predisposition of the accused.

**Part II**

**Distinctions Between Cyberspace and the “Real World”**

a. **The Unique World of Cyberspace**

Cyberspace, as apposed to “face-to-face” interactions, allows users the ability of anonymity. Some servers require identification, however, for the computer savvy individual, fake identification can be easily produced. Therefore, in cyberspace one

---

23 *See, Sherman*, 356 U.S. at 383-384 (1958) (stating, that in holding out inducements (law enforcement agents) should act in such a manner as is likely to induce to the commission of crime only (those engaged in criminal conduct and ready and willing to commit further crimes should the occasion arise) and not others who would normally avoid crime and through self-struggle resist temptations).


27 *See, Sandra Pedicini, Vicious Practice Has Gone High-Tech*, Orlando Sentinel, June 19, 1994, at B1; *see also*, Gregg, *supra* note 1, at 169.
distinct characteristic from the “real world” is that it can be problematic to determine the identity of Internet users.28

Another characteristic of cyberspace is the ease of online access to information and contact with other individuals.29 This allows a wide range of people, especially adolescents, to join chat rooms, on-line bulletin boards, and adult-oriented forums to access varying types of material that they would usually not have access.30 Individuals who, in the “real world,” would not have access to certain types of information are granted admission via cyberspace, and various difficulties arise.31

Another unique characteristic of cyberspace is that individuals can express themselves without inhibitions due to the anonymity aspect of the Internet.32 Individuals can speak freely on subjects that would be socially unacceptable in “real world” contexts.33 Deception can also take new forms in cyberspace since determining identity is so problematic.34 Furthermore, cyberspace does not allow for qualities inherent in face-

28 Kim Murphy, Youngsters Falling Prey to Seducers in Computer Crime Web: Once Candy was the Lure. Now Strangers are using Cyberspace E-mail to Attract Minors into Harm’s Way, L.A. Times, June 11, 1995, at 1; see also, Gregg, supra note 1, at 169 (stating, “Consequently, on the Internet, where there is no central control, and on small bulletin boards run by amateurs, who do not always require individuals to identify themselves, it is difficult to track down a person hiding behind the computer screen).
29 Gregg, supra note 1, at 170.
30 Pedicini, supra note 30.
31 Id.
32 Goldman, supra note 29 at 1086 (discussing instances of internet users sending threats to the President of the United States).
33 Id.
34 Christa M. Book, Do you really know who is on the Other Side of your Computer Screen? Stopping Internet Crimes against Children, 14 ALB. L.J. SCI. & TECH 749, 754 (describing law enforcement posing as children to catch pedophiles).
to-face interactions such as voice inflection or body language, which can lead to confusion or increase the ability to deceive the recipient.\textsuperscript{35}

b. Cyberspace and Crime

In recent years many crimes have transitioned from “real world” settings to on-line settings in cyberspace.\textsuperscript{36} One of the most patrolled crimes in cyberspace is sexual predation of children.\textsuperscript{37} According to some commentators, pedophiles use the advantages of cyberspace in order to pursue their victims, associate with other pedophiles, and share child-porn images or stories instantly.\textsuperscript{38} As the crime of pedophilia has transitioned more to cyberspace, so has law enforcement efforts also moved to the Internet to prevent these crimes.\textsuperscript{39} Law enforcement has recently begun to use the same advantages of cyberspace employed by sexual predators in order to pose as children, then contact, lure, and capture these predators.\textsuperscript{40} These distinctions in cyberspace as opposed to the “real world” have

\textsuperscript{35} Goldman, supra note 29 at 1086; see also, Gregg, supra note 1, at 170 (stating, “While this is perfect for police undercover operations, it also creates the potential for police to abuse deceptive techniques).


\textsuperscript{37} See, Donald S. Yamagami, \textit{Prosecuting Cyber-Pedophiles: How can Intent be Shown in a Virtual World in Light of the Fantasy Defense?}, 41 Santa Clara L. Rev. 547, 550 (discussing the rise of Internet pedophilia and the government’s response).

\textsuperscript{38} Laura Myers, \textit{FBI Raids 120 Homes, Arrests Dozens in Child-Porn Probe}, Orange County Reg., Sept. 14, 1995, at AO4, see also, Vicki Torres, \textit{New Puzzle: High-Tech Pedophilia Technology: Computer Disks Confiscated in Glendora Arrest Contain Sexually Explicit Material Involving Young Boys. Police Say Greater Use of such Equipment is Difficult to Track Down}, L.A. Times, Mar. 5, 1993, at 3 (describing situations where the use of online services or bulletin board systems is rapidly becoming one of the most prevalent techniques for individuals to share pornographic pictures of minors, as well as to identify potential victims).

\textsuperscript{39} Book, supra note 36, at 744-45.

\textsuperscript{40} Stevenson, supra note 38, at 68 (stating, “It is easy, both in the sense of being simple and cheap, for officers or agents to troll on-line chat rooms posing as adolescents seeking sexual experimentation to lure pedophiles into extended correspondence while accumulating
created a set of entirely different variables in the pursuit to prevent sexual predation, and also have raised new questions regarding the Entrapment Defense.\textsuperscript{41}  

c. How Law Enforcement Ensnare Individuals on Cyberspace

The most common way law enforcement captures an individual targeted as an Internet predator is by a cyber-sting operation.\textsuperscript{42} Creating a cyber-sting operation is relatively simple and entails: creating a username and profile for a minor online; having an officer peruse the Internet on targeted chat rooms under this username; and once the predator initiates contact with the officer, the officer then conducts private conversations with the predator in the chat room or on an instant messaging program.\textsuperscript{43} Once the foundation of the cyber-sting is formulated the officer continues correspondence until it is determined by the officer that the target makes clear that his intent is to have sexual contact.\textsuperscript{44} Once this is determined the officer arranges a meeting with the predator and an arrest is subsequently made at that meeting.\textsuperscript{45}

\begin{itemize}
    \item[	extsuperscript{41}] Gregg, \textit{supra} note 1, at 160 (stating, “The undercover policing of child pornography distribution and related crimes in cyberspace creates the potential for new levels of police deception and creativity, and heightens the potential for abuse).\n    \item[	extsuperscript{42}] Rajiv Chandrasekaran, \textit{Undercover on the Dark Side of Cyberspace; Online FBI Agents Troll for those who Prey on Children but Cybercops Chill Critics}, Wash. Post, Jan.2 1996, at D1 (describing the increase of FBI and Florida Department of Law Enforcement sting operations on the Internet).
    \item[	extsuperscript{45}] Chandrasekaran, \textit{supra} note 41, at D1.
\end{itemize}
In prosecuting these Internet predators the state usually bases its claim on a federal statute enacted by Congress to deter child predation through the Commerce Clause.\textsuperscript{46} This statute places culpability on individuals for attempt of child predation, even if the intended victim is actually an adult.\textsuperscript{47} Therefore the defense of impossibility is not an option for individuals prosecuted under these actions.\textsuperscript{48} To bolster its’ case in a cyber-sting, where there is no real victim, the state must prove either attempt or conspiracy, whereas the defendant took a substantial step beyond mere preparation to commit the crime or an overt act in furtherance of the conspiracy.\textsuperscript{49} Proving a substantial step or overt act can be achieved by showing the defendants travel to meet the decoy minor.\textsuperscript{50} Therefore, in the majority of Internet predation cases defendants have taken a plea bargain and plead guilty to lesser charges in order to avoid possible punishment they would face in arguing a defense.\textsuperscript{51}

\textsuperscript{46} 18 U.S.C. § 2423(b) (2006) (defining travel with intent to engage in illicit sexual conduct as: “A person who travels in interstate commerce or travels into the United States, or a United States citizen or an alien admitted for permanent residence in the United States who travels in foreign commerce, for the purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both”).

\textsuperscript{47} Id at § 2423(e) (defining attempt and conspiracy as: “Whoever attempts or conspires to violate subsection (a), (b), (c), or (d) shall be punishable in the same manner as a completed violation of that subsection).

\textsuperscript{48} State v. Farner, 251 F.3d 510, 513 (5th Cir. 2001) (holding that defendant’s impossibility defense was unwarranted).

\textsuperscript{49} See, Illinois vs. Patterson, 734 N.E.2d 462, 468 (Ill. App. Ct. 2000) (stating that attempt is satisfied when the defendant “does any act which constitutes a substantial step in the commission of that offense,” and that the impossibility of completion of that act cannot be a defense).

\textsuperscript{50} See, State vs. Heitman, 629 N.W.2d 542 (2001) (ruling that defendant’s actions of going to a motel, renting a room and bringing condoms, Viagra, and other items of a sexual nature to the room proved that he was engaged in an overt act in furtherance of the conspiracy).

\textsuperscript{51} Debra Baker, When Cyber Stalkers Walk, A.B.A J., Dec. 1999, at 51. (Discussing how most defendants in Internet predation cases are willing to take lighter sentences instead of having the burden of going to court).
Part III

How Entrapment has been applied to Cyberspace

a. Setting Precedence: *Jacobson v. United States*

The majority of cyberspace predation cases where the accused raises the entrapment defense rely on the subjective test outlined by *Jacobson v. U.S.* In *Jacobson* the defendant purchased a legal magazine that depicted young men in the nude. Subsequently, the law regarding child pornography changed and Jacobson, the defendant, was targeted by law enforcement agencies due to his name being listed under this magazine’s purchase orders. Posing as various political organizations advocating for First Amendment freedoms, the Government was finally able to induce Jacobson into ordering a pornographic catalog depicting children in sexual situations. Jacobson was then arrested and convicted at trial for violating 18 U.S.C. § 2252(a)(2)(A.). The appeals court affirmed the decision denying Jacobson’s Entrapment Defense.

The only issue the Supreme Court had to determine in Jacobson’s Entrapment Defense was whether Jacobson was predisposed to purchasing child pornography prior to the Governments repeated contact spanning over the previous two years. In their

---

54 Id. at 543.
55 Id. at 546-547 (stating, “When petitioner was asked at trial why he placed such an order, he explained that the Government had succeeded in piquing his curiosity”).
56 Id. at 547.
57 Id. at 547-48.
58 Id. at 549 (stating, “Indeed the proposition that the accused must be predisposed prior to contact with law enforcement officers is so firmly established that the Government conceded the point at oral argument, submitting that the evidence it developed during the course of its
analysis the Justices reasoned that if Jacobson had been ready and willing to purchase child pornography as soon as the opportunity presented itself, Jacobson would have satisfied the predisposition element barring his entrapment claim. The government, however, did not prove that his predisposition was independent and not the “product of the attention that the Government had directed at petitioner” since the two years prior. Therefore the Court concluded that the prosecution failed to show beyond a reasonable doubt that Jacobson was predisposed to ordering child pornography, and ruled in favor of Jacobson’s entrapment defense.

Since Jacobson dealt with the distribution of child pornography through the mails, many defendants in cyberspace predation cases rely on Jacobson in order to rebut their predisposition in committing the crime. Jacobson applied the subjective test for the entrapment defense, and the defendants in these cases had to show that they were not predisposed prior to the governments contact and that they were not ready or willing to commit the crime when offered the opportunity. This proved to be a rigid obstacle to investigation was probative because it indicated petitioner’s state of mind prior to the commencement of the Government’s investigation”)

59 *Id.* at 549-550 (stating, “In such a typical case, or in a more elaborate “sting” operation involving government-sponsored fencing where the defendant is simply provided with the opportunity to commit a crime, the entrapment defense is of little use because the ready commission of the criminal act amply demonstrates the defendants predisposition”).

60 *Id.* at 550-551 (reasoning that Jacobson’s original order predating the first solicitation by the government did not prove his predisposition because the magazine ordered was not an illegal form of child pornography at the time).

61 *Id.* at 554.

62 *See generally, U.S. v. Cherian,* 58 Fed. Appx. 596 (5th Cir. 2003); *U.S. v. Curtin,* 489 F.3d 935 (9th Cir. 2006); and *U.S. v. Morris,* 549 F.3d 548 (7th Cir. 2008).

63 *Id.*
overcome since cyberspace poses different variables, however, some defendants have been able to effectively plead their entrapment defense.64

b. No Uniformity, A Steep Hill to Climb

Circuits have not applied the entrapment defense articulated in Jacobson in a uniform fashion.65 This is primarily because many Circuits rule that the entrapment defense should be applied as the State sees fit.66 Even when federal case law allows for a less stringent entrapment analysis,67 state courts have applied their own standard.68 In one state, law enforcement can contact an individual first, induce him into crime through friendship, and deny his entrapment claim based on predisposition evidence obtained before he even knew the actual age of the “victim.”69 In another state these same factual similarities warrant the affirmative defense of entrapment.70 There is no uniformity on the state level regarding the entrapment defense and defendants are left subject to the definition of inducement and predisposition interpreted by their state.71

64 See, U.S. v Poehlman, 217 F.3d 692 (9th Cir. 1999); U.S. v. Curtin, 489 F.3d 935 (9th Cir. 2006).


68 People vs. Grizzle, 140 P.2d 224, 227 (2006) (denying defendant’s entrapment defense because he did not admit the culpable mental state for two of his attempt charges).

69 Heitman, 692 N.W.2d at 558 (2001).

70 Poehlman, 217 F.3d at 705 (2000) (like in Heitman, the defendant was repeatedly contacted by agent, induced through friendship and trust, and defendant produced evidence proving lack of predisposition. However, the court ruled in favor of Poehlman as opposed to Heitman’s conviction).

71 See generally, U.S. v Poehlman, 217 F.3d 692 (9th Cir. 1999); U.S. v. Curtin, 489 F.3d 935 (9th Cir. 2006); State v. Heitman, 692 N.W.2d 542, 557 (2001); and People vs. Grizzle, 140 P.2d 224, 227 (2006).
Even when role-playing or mere exploration of fantasy is alleged, circuits have applied little weight to the evidence.\textsuperscript{72} Instead, courts rebut these assertions based on state law of conspiracy or attempt, where the defendant’s conception of the “victim’s” age is irrelevant to find him culpable.\textsuperscript{73} Furthermore, some courts have found predisposition where there is no evidence that the defendant previously engaged in sexual activities with minors, only intended friendship with “victim,” and showed apparent caution in becoming sexually active with the “victim.”\textsuperscript{74} Instead, these courts give less weight to this type of evidence unless it is shown that evidence against such findings is clearly wrong or clearly adverse to law.\textsuperscript{75} Therefore, defendants in cyberspace predation cases have had a “steep hill to climb” when asserting entrapment.\textsuperscript{76}

\textbf{Part IV}

Problems with Applying the Traditional Definition of Entrapment to Cyberspace

a. The Subjective Test is Inadequate

Currently courts use the subjective test of \textit{Jacobson} in Internet predation cases, however, this test has been found to be an ineffective defense for the accused in these

\textsuperscript{72} \textit{Grizzle}, 140 P.2d at 227 (2006) (discussing the courts awareness that cyberspace could “ensnare an otherwise law-abiding citizen with sexual fantasies involving conduct which is illegal, immoral, taboo, upon which he or she would not otherwise act were the opportunity not presented to them”).

\textsuperscript{73} \textit{State v. Campbell}, 473 N.W.2d 420 (1991) (defining Nebraska conspiracy law as holding individuals culpable irrespective of consent or reasonable mistake as to age of the victim); \textit{see also, People v. Bath}, 890 P.2d 269 (Colo. App. 1994) (applying strict liability as to the victim’s age in Colorado).

\textsuperscript{74} \textit{Heitman}, 692 N.W.2d at 557 (2001).

\textsuperscript{75} \textit{See generally, State v. Parks}, 324 N.W.2d 673, 676 (1982) (discussing the standard of review in entrapment cases and applying a weighted scale for egregious acts of law enforcement in order to reverse a lower court’s ruling); \textit{see also, State vs. Ransburg}, 148 N.W.2d 324 (1967.)

cases.\textsuperscript{77} One commentator, states that “predisposition, usually the critical element under the subjective test, is a forgone conclusion in almost all of the cases because the defendants actively log onto certain chat rooms and engage in repeated, typed communications with their intended victims.”\textsuperscript{78} Others feel that these communications are a poor indicator for predisposition because users can “remain anonymous, identity is disguisable, and role-playing may take place.”\textsuperscript{79} Along with the potential of “role-playing” there is a risk that some of these individuals may only be making incriminating statements because of their lack of inhibitions due to the cyberspace atmosphere, which challenges the reliability of these statements in predisposition analysis.\textsuperscript{80} Furthermore, in cases where law enforcement agencies claim that they have targeted suspects only after receiving complaints from another user or amateur system operator, the courts will need to determine whether these accusations indicate sufficient predisposition to warrant stings involving undercover agents, or user identification requests.\textsuperscript{81} Finally, it would be problematic to prove predisposition in instances where the Government agents, posing as adolescents and using suggestive user names, repeatedly contact individuals creating an


\textsuperscript{78} Stevenson, supra note 38, at 69.

\textsuperscript{79} See, Yamagami, supra note 36, at 566 (describing the Internet as a fantasy world where people role-play while hiding behind anonymity); see also, Gregg, supra note 1, at 187.

\textsuperscript{80} Gregg, supra note 1, at 187 (stating, “The chief difficulty is how to factor the inherent propensity for “big talk” by users in the fantasy-like atmosphere of the Internet, into a predisposition analysis. Caught up in the free-flowing atmosphere of the medium, individuals are prone to “say” things they might not say elsewhere because of the anonymity and the false intimacy of cyberspace interactions).

\textsuperscript{81} Id. at 187.
“un-artificial” situation that would not be presented in the “real world”\footnote{Simmons 18} (Emphasis Added.)

b. The Objective Test is also Ineffective in Cyberspace

Individuals will not have an efficient Entrapment Defense in states that employ the objective test.\footnote{See, Steven Duke, Entrapment Defense Languishes in a Permanent State of Confusion, NAT’L L.J., Mar. 21, 1983, at 32; see also, Gregg, supra note 1, at 188 (discussing, “The repeated inducements of online undercover agents posing as teens using suggestive user names presents such an un-artificial situation. As in Jacobson, this type of inducement is an example of law enforcement challenging an individual’s morality. Such conduct violates the unifying aim of both the subjective and objective approaches to limit undercover techniques, which unproductively create crime).} Scrutinizing law enforcement procedure would be difficult because some restrictions, (like sexual relationships with the suspect,) would be unacceptable in the “real world,”\footnote{Hanson, supra note 4, at 545-546.} however in cyberspace, (cybersex,) may be necessary to lure a target.\footnote{See, Commonwealth vs. Thompson, 484 A.2d 159, 166 (1984) (ruling in favor of defendant’s entrapment defense where agents employed a female to “kiss and socialize” with defendant for months inducing him into crime); see also, People vs. Wisneski, 292 N.W.2d 196, 199 (1980) (finding entrapment where agent used sex to induce crime).} Under the objective test “sympathy, pity, or close personal friendships” would constitute prohibited activities for law enforcement;\footnote{Hanson, supra note 3, at 546 (stating, “For example, fostering sexual relationships to encourage crime is generally outside the range of acceptable law enforcement behavior in the real world. In cyberspace, sex is not possible in the conventional sense. Would the offer of sexual favors be off limits in cyberspace without a real chance of them occurring? If an agent through words satisfies someone’s desires, is such conduct also off limits even though no physical contact occurred?)} however, there has not been consensus on how courts should weigh these prohibitions in cyberspace.\footnote{Sherman vs. U.S., 356 U.S. at 371 (1958).}

\footnote{Simmons 18}
interactions in the “real world” a person could be given clues about the nature of the relationship with the undercover agent, in cyberspace however, these clues are reduced and law enforcement is allowed greater influence over individuals while maintaining traditional police procedure to avoid Entrapment.88 One final note that commentators make regarding the ineffectiveness of the objective test in cyberspace is that “the conduct and conversations of the agents can be very difficult to trace or verify,” thereby inhibiting accountability.89

c. Other Concerns Regarding Traditional Entrapment and Cyberspace

Commentators have also highlighted other considerations regarding the effectiveness of the Entrapment Defense in cyberspace.90 One concern is that “private entrapment” has increased, meaning that citizen vigilantes have employed deceptive tactics to capture pedophiles, vitiating any Entrapment Defense the individual may have had.91 Evidentiary issues are also called into question in cyberspace, where courts would have to decide

88 See, Yamagami, supra note 36, at 562 (describing the internet as a forum for individuals to omit, exaggerate or falsify aspects of a person’s appearance, social characteristics, or standing); see also, Hanson, supra note 4, at 546-547.

89 Stevenson, supra note 38, at 69-70 (stating, “There is less accountability for government where the enforcement method is cheap and relatively invisible when orchestrated. Traditional stings typically require a host of armed “backup” agents nearby in case the primary undercover operative encounters trouble. Catching pedophiles can be done mostly from a cubicle in an office. In addition, the Internet enables a single officer to entrap multiple individuals at once, as through on-line bulletin board postings. This feature of on-line entrapment may not be undesirable from a policy perspective, but it is a significant change from the traditional arrangement that the entrapment defense contemplated).”

90 See, Zabriskie, supra note 15, at 243-248; Gregg, supra note 1, at 188-191; and Stevenson, supra note 38, at 70-72.

91 See, U.S. v. Morris, 549 F.3d 548, 550-551 (7th Cir. 2008); see also, Stevenson, supra note 38, at 70 (stating, “Traditional entrapment rules do not allow consideration of “private entrapment.” Individuals tempted, induced or set up by anyone besides a state agent cannot raise an entrapment defense to criminal charges. 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. Private entrapment was therefore a rare occurrence. The Internet has changed this…”).
what type of “cybertalk” constitutes requisite predisposition enough to establish probable cause to issue warrants for arrest. 

Other evidentiary issues that arise as well are introduction of past crimes evidence at trial and hearsay problems due to the fact that most predisposition evidence is contained in previous communications saved on a computer’s storage system where the communication can be easily manipulated. 

One final concern is whether predisposition, a jury question, should be heard by a jury of the “real world” community or by a jury consisting of the defendant’s cyberspace community. 

Initially this concern surrounds the ability to be tried by a jury of one’s peers, and a determination of acceptable practices in cyberspace, which probably differ from acceptable practices in the real world.

92 Gregg, supra note 1, at 188-189 (discussing that “in practice, if the agents need more than just “cybertalk” to show predisposition, they would first have to record the online exchanges, get the user’s identity, and then conduct a background check. This undermines the requirement that the government must have a reasonable suspicion prior to targeting a particular individual).

93 See, State vs. Bolden, 2004 W.L. 1043317, at *7- *9 (Ohio Ct. App. 2004) (describing States failure to produce missing logs of Internet conversations); U.S. v. Poehlman, 217 F.3d at 695 (2000) (discussing the States inability to produce the original emails at trial); and Stevenson, supra note 38, at 71 (stating that, “unlike physical evidence, these records are easily altered, redacted, and otherwise manipulated after the arrest, without detection or evidence of the alteration).


95 Gregg, supra note 1, at 188-189 (reasoning that “In the context of such a “community,” the communication between suspected pedophiles (which some argue should qualify as predisposition) could be viewed as merely “big talk,” boasting, or fantasizing of having sex with a minor. Users who frequent the forum are likely to be more willing than “real world” juries to recognize the distinction between predisposition to act and predisposition to talk suggestively with a minor).
Part V

Recommendations/Alternatives to Traditional Entrapment

a. Discard Subjective and Objective Test, then Create New Standard

It is important to note that various commentators have shared views on how to remedy the ineffectiveness of the traditional entrapment defense, however, many of their ideas should be incorporated cohesively in order to resolve the issue. According to these commentators, the subjective and objective tests are ineffective in protecting the innocent or preventing law enforcement abuse of authority. Therefore these tests should be discarded when applied to cyberspace and a new standard should be incorporated. The legislature rather than the courts should craft this new standard since the courts currently rely on cases that use the traditional tests for entrapment. The legislature should implement new evidentiary guidelines solely for Internet cases where they devise a bright-line definition of what constitutes predisposition in cyberspace. Expounding on this thought, the Legislature should decide what prior communications, postings, or sites visited determine the likelihood that an individual will commit a crime regardless of Government involvement; and they should also consider how much probable cause these

96 See, Yamagami, supra note 36, at 562; Zabriskie, supra note 15, at 243-248; Hanson, supra note 4, at 541; Gregg, supra note 1, at 186-187; and Stevenson, supra note 38, at 69-72.

97 Id.

98 See, Laura Davis, et al., Controlling Computer Access to Pornography: Special Conditions for Sex Offenders, 59 FED. PROBATION 43 (June 1995) (discussing areas of cyberspace that the Legislature has proposed regulation).

99 See generally, U.S. v Poehlman, 217 F.3d 692 (9th Cir. 2000); U.S. v. Cherian, 58 Fed. Appx. 596 (5th Cir. 2003); U.S. v. Curtin, 489 F.3d 935 (9th Cir. 2006); and U.S. v. Morris, 549 F.3d 548 (7th Cir. 2008).

100 See, Gregg, supra note 1, at 196.
actions create to satisfy warrant requirements. This procedure should also make considerations for communications that can be argued as role-playing or “big talk,”\(^\text{101}\) to exclude criminal liability for individuals who only exhibit diminished inhibitions in cyberspace. Thus the new standard implemented by the legislature should include a bright-line definition of predisposition as it relates to cyberspace cases.

Aside from addressing predisposition, the Legislature should also determine limitations on law enforcement’s use of deceptive tactics in cyberspace. According to commentators, law enforcement in cyberspace should have a higher reasonableness standard implemented to determine whether the tactics employed had rational means.\(^\text{102}\) This reasonableness standard should not only apply a sliding scale of deception to warrant whether police action was justified, but it should also provide a basis for a Trier of fact to determine whether the actions of the police were appropriate given the circumstances distinguishing cyberspace from the “real world.”\(^\text{103}\) Some commentators also believe that the implementation of a reasonableness standard should also mandate law enforcement to seek judicial approval for an operation by showing that they had a reasonable suspicion that the suspect has committed or will commit a crime based off of

\(^{101}\) Id. at 187 (defining “big talk” as comments made by individuals in cyberspace that they would not usually say in “real world” settings, but do so due to their ability to remain anonymous on the internet).

\(^{102}\) See, Zabriskie, supra note 15, at 237-238; Hanson, supra note 4, at 547-551; and Gregg, supra note 1, at 196.

\(^{103}\) Gregg, supra note 1, at 196 (reasoning that “The inducement standards need to recognize the varying degrees of deception allowed by the unique qualities of cyberspace; e.g., there is a distinction between pretending to be a thirteen year old girl and pretending to be an adult interested in child pornography. In the “real world,” an agent would not have the freedom to engage in the former category of conduct. This raises a concern that such deception may be too egregious”).
Accordingly the Legislature should also incorporate a higher reasonableness standard to apply to cyberspace cases in order to determine whether police actions employed rational means.

b. Law Enforcement Regulations on Cyberspace Interactions

One of the major concerns regarding the Internet entrapment defense is that law enforcement procedures are not drafted to consider the unique realm of cyberspace. As stated earlier, some procedures are unacceptable in the “real world,” such as sexual relationships with the suspect, but may not be applicable to cyberspace, just as “cybersex” may be useful in determining predisposition. Therefore federal law enforcement procedures addressing cyberspace and its distinctions from the “real world” should be created. These procedures should regulate how to effectively locate the predators the officer is seeking, define what would classify a target as predisposed, explain how to offer the opportunity for crime without inducing the target, and describe how to use deceptive techniques in the most effective manner without wasting resources.

Law enforcement agencies should also create guidelines to prohibit officers from inducing individuals through “sympathy, pity, or close personal relationships.” This can be accomplished by mandating officers to make clear to the target that correspondences are opportunities to commit crime only, with no other relationship ties. Commentators

104 Hanson, supra note 4, at 548.
105 Id. at 545.
106 Hanson, supra note 4, at 542.
107 See, Gregg, supra note 1, at 195; Hanson, supra note 4, at 548-549; and Stevenson, supra note 38, at 73-74.
108 Zabriskie, supra note 15, at 244.
also feel that procedure should be implemented that defines the requisite intent for
criminal liability on-line. 109 Furthermore, law enforcement agencies need to bolster the
reliability of evidence produced, 110 therefore these procedures should instruct officers to
collect evidence on secure computer systems that can trace their conduct and
conversations. One final suggestion is for law enforcement agencies to specify what
qualifies as a “substantial step” for attempt in cyberspace so that courts can determine
when an Internet user has gone beyond mere preparation and has begun to act on his
intended crime. 111 For these reasons, law enforcement agencies should consider the
distinctions between cyberspace and the “real world” and incorporate procedures that will
be more applicable to the Internet setting.

c. Other Recommendations

Commentators have explained that one problematic concern with the ineffectiveness
of the entrapment defense is that “private entrapment” has increased. 112 In order to deter
this rising concern, federal laws should be implemented to penalize individuals who
conduct private sting operations for the sole purpose of vigilantism. That way citizens
will refrain from taking law into their own hands and allow law enforcement to police

109 Audrey Rogers, New Technology, Old Defenses: Internet Sting Operations and Attempt
Liability, 38 U. RICH. L. REV. 477, 510-23; see also, Stevenson, supra note 38, at 73-74
(discussing proposals to “build entrapment safeguards into the elements of attempt, rather than
having entrapment function as an affirmative defense.” Also suggesting incorporation of “a
clearer definition of the requisite intent for criminal liability on-line to account for varying levels
of user error or confusion”).

110 Stevenson, supra note 38, at 71.

111 Id. at 74 (stating, “Almost all the cases involve stings that culminated in an arranged meeting
at a motel or restaurant. Requiring some sort of incriminating statement at the supposed
rendezvous confirming the defendant’s continuing intention would not be particularly
burdensome on the police and it would make the results of the cases more predictable and certain.

112 See, note 100.
cyberspace. Another concern relates to the manipulation of predisposition evidence produced from Internet site visits, communications, and web postings. Mandating the use of secure computer programs to identify, collect, and store evidence while restricting subsequent manipulation can alleviate this issue.

One final concern relates to the jury the accused in a cyberspace case should be entitled. Since the majority of evidence obtained in these types of cases is obtained from cyberspace, it only seems equitable to grant the accused with a jury that is adequately oriented with Internet terminology, usage, and experience. The accused should be considered an individual of a particular “cyber-community” and as such should be entitled to a jury of his/her “cyber-community” peers. Accordingly, the jury pool for a defendant in a cyberspace case should only consist of individuals adequately knowledgeable of the cyberspace realm to promote fairness and equity.

Conclusion

The traditional Entrapment Defense was designed to protect innocent law-abiding citizens from committing crimes due to deceptive police practices, and ensure the reasonable allocation of resources by police agencies when they employ those deceptive practices. In applying the defense, federal courts employ the subjective test, which scrutinizes whether the accused was predisposed to committing the crime regardless of law enforcement involvement. Conversely, there is a minority of states that employ the objective test, which analyzes the government’s actions in the inducement of the crime.

113 See, note 102.
114 Byasee, supra note 93, at 204-07, 218-19.
115 Id.
116 Id.
The flaw with the traditional entrapment defense is that it cannot effectively transpose either the subjective or objective test to cyberspace, leaving defendants in Internet predation cases without an effective defense. This is because Internet communications are a poor indicator for predisposition due to anonymity, possible role-playing, and potential “big talk.” Another concern relates to the ability to apply the same law enforcement procedure in both cyberspace and the “real world,” since some unacceptable behavior in the “real world” has not been questioned in its application to cyberspace. Furthermore, communications produced as evidence from cyberspace is easily manipulated by law enforcement, and reliability of this evidence is problematic.

Since the traditional entrapment defense is ineffective at providing the innocent a defense in cyberspace cases, alternatives must be employed. First, the subjective and objective tests should be discarded. The legislature should then incorporate a new standard for Internet predation cases where cyberspace predisposition is defined, and law enforcement is held to a higher reasonableness standard. Secondly, Law enforcement agencies should employ regulations on police procedure to promote effective targeting, prevent unjust inducements, and promote reasonable use of resources. Lastly, individuals in cyberspace cases should be entitled to a jury of their “cyberspace-community” that is knowledgeable of the cyberspace realm to ensure fairness and equity.

With the popularity and growth of cyberspace, it is imperative that law adapts to accommodate this unique realm. As on-line crime increases, so does the presence of Internet policing, leaving the innocent subject to both dichotomies. Without an adequate Entrapment Defense, unsuspecting individuals can be induced by agents to commit crimes while their very own innocent communications and postings further condemn
their actions. It is time to re-evaluate the entrapment defense as it is applied to cyberspace in order to prevent law enforcement from “shooting an unarmed, defenseless, innocent person.”