CyberPredators: Police Internet Investigations Under Florida Statute 847.0135

Michael W. Sheetz

Follow this and additional works at: http://repository.law.miami.edu/umlr

Recommended Citation
Available at: http://repository.law.miami.edu/umlr/vol54/iss2/8
CyberPredators: Police Internet Investigations Under Florida Statute 847.0135

I. INTRODUCTION ...................................................... 405
II. THE ANATOMY OF A POLICE INVESTIGATION .............................. 407
III. THE TARGET ........................................................ 416
   A. Know Your Enemy: Understanding the Pedophile Offender .......... 416
IV. THE LAW ........................................................... 421
   A. Fear Spurs Action ............................................. 421
   B. Florida Statute 847.0135 ...................................... 421
V. THE PROBLEMS ...................................................... 422
   A. Double-Inchoate Crimes ....................................... 422
   B. The “Guilty Thoughts” Problem to the nth Power .............. 426
   C. Entrapment ..................................................... 428
      1. OVERVIEW OF ENTRAPMENT AS THE DEFENSE .......... 428
      2. FEDERAL ENTRAPMENT — THE EXEGESIS OF THE DEFENSE . 430
         i. The Subjective Standard ................................ 431
         ii. The Objective Standard ................................. 431
      3. THE FLORIDA STANDARD .................................. 432
         i. The Cruz Test ............................................ 432
         ii. The Legislative Answer to Cruz and the Court’s Response: In Through the backdoor ................................... 433
D. Application of the Principle to the Problem .......................... 435
   1. DUE PROCESS VIOLATIONS .................................... 435
   2. THE SUBJECTIVE APPROACH ................................ 438
E. Application of Entrapment to Cyberspace ............................ 441
F. The Proposed Solution ............................................ 446
VI. CONCLUSION ........................................................ 448

I. INTRODUCTION

Within 10 minutes, my gorgeous little angel would walk in for her evening bath. She closed the door behind her, and began to undress for her hidden audience of one. Once in the tub she was out of sight, but as she was undressing, drying and putting on her night shirt, she was my little vision. I gazed lovingly at the light brown skin that covered her nearly perfect body. No body hair and slightly dark nipples on her chest was just too much to take. I could not help myself. . . .

This excerpt, from an article written by an admitted pedophile, stirs powerful and often uncontrollable emotions in everyone. Whether the emotions are the lust stirred in a pedophile or feelings of anger, disgust, and repugnance felt in the rest of us, they are, unequivocally, powerful emotions. It is undisputed that the First Amendment protects this per-

son's right to express his or her beliefs. It is also undisputed in the scientific community, that persons aroused by this type of eroticism suffer from a personality disorder characterized as abnormal behavior.\(^2\) This type of aberrant behavior strikes deep at the heart of a community's soul. It has served as the catalyst for the enactment and enforcement of an array of laws designed to protect our children from the boogeyman on the information superhighway.

This comment is not a diatribe against people who are diagnosed as pedophiliacs. Nor is it a categorical condemnation of efforts to police the Internet. Instead, this comment attempts a detached critical analysis of Florida Statute 847.0135, and police enforcement activity that has emerged since its passage.

The analysis draws from a variety of sources. The approach to this problem cannot be one of myopic legal analysis with no medical, statistical or empirical considerations. Because this problem is essentially influenced by human behavior, the article explores the disorder most commonly associated with sexual abuse of children — pedophilia. In reaching conclusions, the article calls upon the most contemporary, scholarly thoughts on the subject, as well as empirical and anecdotal data personally collected during fifteen years of law enforcement. Most of the anecdotal data has been developed through innumerable contacts on the Internet in an investigative role, and for obvious reasons requires the appropriate level of skepticism.

The decision to explore this problem solidified as I came to question the efficacy of society's own activities. The result of challenging my own convictions is the comment that follows. While the analysis has assuaged my concerns somewhat, the underlying current of concern still flows swiftly.

My approach to this problem is from both an academic and a clinical perspective. In the context of purely academic profundity, police conduct is often dissected with the kind of surgical accuracy that only 20/20 hindsight and the leisure of extended deliberation can provide. It is my goal to conduct this type of analysis, juxtaposed against the type of "real-world" functionality that police officers and prosecutors must grapple with daily. The result, I hope, is a salient, practical examination that is of value to both academicians and practitioners.

The analysis occurs in several steps. First, a frank and thorough examination of the logistical "nuts and bolts" of police investigations in this realm is offered. After an introduction to the inner workings of police on-line investigations, I begin to examine the problems raised by

\(^2\) See Diagnostic & Statistical Manual of Mental Disorders § 302.20 (3d ed. 1987).
the anonymous nature of cyberspace and the influence of psychological
deviance. Because the world of cyberspace is wrought with fantasy and
role playing, it is very difficult to punish what society perceives to be
criminal conduct under the law without coming dangerously close to
punishing "guilty thoughts." This fact, combined with serious entrap-
ment concerns, must be addressed if we are to successfully and legally
protect our children. To solve the problems addressed in the comment, I
offer an amendment to existing law. This amendment provides height-
ened protection from punishment of innocent conduct, yet it allows pre-
vention of criminal conduct that actually threatens our youth. Through
this analysis it may be seen that protection of children from on-line
pedophiles is both a necessary expenditure of law enforcement resources
and legally possible within the confines of our existing system of jurisprudence.

II. THE ANATOMY OF A POLICE INVESTIGATION

Most police investigations evolve along one of two paths, proactive
or reactive. Proactive policing is a strategy of investigating crimes
before they occur. Reactive investigations refer to the customary
detective work carried on only after a crime has occurred. Historically,
reactive policing has been the favored method. In the early 1800s,
throughout England and the United States, the lack of a professional
police force necessitated using private investigators to recover property
and to deliver criminals for trial. Beginning with the 1829 reform
movement in England, orchestrated by Sir Robert Peel, policing eventu-
ally became an organized professional enterprise. During this era,
proactive methods of investigation were largely held in disrepute.

Proactive methods were rejected over reactive investigative tech-
niques, due in large part to the extremely close resemblance of the inves-
tigative conduct to fraud, misrepresentation, and extortion. Additionally, with the advent of Scotland Yard and the burst of scientific
and technological advances such as fingerprinting, microscopic exami-
nation, and record keeping, English criminal investigators all but aban-
doned the use of proactive techniques. In America, the march toward
professional unified police forces was even less rapid than in England.

4. See id. at 5-2.
5. See id. at 5-12.
6. See id.
7. See id.
8. See id. at 5-15.
9. See id.
Throughout this time both methods of investigation were used, but the reactive method was favored for all of the above reasons.

Over time, the criminal justice system has gradually recognized that effective management of the police investigative function requires the integration of both methods. It has become apparent that reactive techniques are ill-suited to the investigation of some types of crimes, in particular, vice crimes and those crimes of an organized nature. As we begin to explore the world of the pedophile, it becomes clear that the use of proactive techniques are well suited because of the high incidence of under — or non-reporting by victims. Because the victim is reluctant and hard to identify, few, if any, cases may be investigated after the fact.

Additionally, pedophilic molestation of children falls into a class of crimes against which society categorically wishes to guard. It is a crime we seek to prevent at all costs. It is true that societies seek to prevent all types of crime. Even opponents to police activity in this area, however must admit that investigating the sexual exploitation of a child is rather like closing the barn after the horse has already left. The damage society seeks to reduce is the psychological and emotional trauma to the victim. Clearly, limiting our investigation of these crimes only to reactive investigation of pedophilic encounters would be a gross disservice to our children. A stolen television may be recovered after the fact in substantially the same condition as when stolen. The same cannot be said of a molested child’s emotional condition. For this reason, proactive investigative techniques are valuable tools in helping to curb this type of crime.

A more adequate understanding of the unique nature of conducting investigations on-line requires a basic working knowledge of the computer and computer communications. With limited exception, all present-day investigations of on-line activity are conducted using the Internet. Not long ago, the Internet was practically nonexistent. Before the burgeoning growth of the Internet, on-line law enforcement activity, the little that existed confined itself to local computer systems called Bulletin Boards Systems (BBS).

In 1957, the USSR launched Sputnik prompting the United States Department of Defense to sponsor the Advanced Research Project Agency (ARPA) — the progenitor of the Internet. Under the auspices of the Department of Defense, computers on various military posts were linked through this new communications protocol. The goal of this pro-

10. A Bulletin Board System is a computer, or series of computers linked together, into which a user may call directly from his computer. A BBS is distinguished from the Internet in that the Internet is a series of computers virtually linked together forming a “web” of machines.

ject was total interconnectivity among military installations. Eventually, the network, originally called ARPANET, was expanded to include academic and research institutions. This network underwent drastic change over its lifetime, and it eventually became known as the Internet. The Internet is essentially the physical backbone of interconnected computers over which the World Wide Web (WWW) is constructed.12 In 1993, the WWW had an estimated 130 sites. As of December 1998, less than seven years later, the web has grown to approximately 3,689,227 sites.13 This rapid rate of expansion of a communications medium is unparalleled in history, and it is expected to continue.

When police initiate undercover operations on the Internet, it is most frequently done through a concept known as Internet Relay Chat (IRC). To do this, the investigator must first have Internet access. Access to the Internet is obtained through an Internet Service Provider (ISP). ISP's are located everywhere—literally. They range from small "mom-and-pop" type operations, to commercial giants. An ISP generally provides a subscribing user with access to a private account through which the user may reach the Internet, one or more electronic mail accounts (e-mail), and usually a small portion of computer storage space on the system in which the subscriber may construct a home page.14 Larger ISPs often have chat areas and discussion groups available for on-line discussions between co-subscribers. The two most popular, and arguably the largest, ISPs are Compuserve and America Online (AOL). In some cases, subscribers will be given an account on the ISP called a "shell" account, which gives the subscriber the ability to access actual time on the system processor. These accounts are very popular with clandestine "hacker"15 groups because they usually provide access to the ISP's UNIX16 shell directories.

A unique feature of smaller ISPs is that they may accept a sub-
scriber's information without verification. This means that criminals
and law enforcement alike can obtain an ISP account under a false name

12. See id.
13. See id.
14. A home page is a virtual presence on the WWW upon which the owner can place text, images, video clips, or music files.
15. Hacker is a term frequently used to describe both a computer aficionado who dedicates large amounts of time and energy to the legal use of computers and a computer criminal who commits acts of unauthorized access to computer systems. In the context of this article the term hacker will be used only to denote the latter, not the former.
16. UNIX is a high-level computer programming language created by Bell Laboratories in the late 1960's. It is essentially the language of choice on large mainframe computers, and is usually the underlying operating system on most ISP sites. The hackers who consider themselves among the "elite" will use shell access to write and run clandestine hacking programs. The shell account is a good launching place for clandestine attacks on other computers.
and address. This can prove to be both a benefit and bane to law enforcement. Once an ISP account is obtained, the undercover work can begin.

Internet Relay Chat (IRC) is a computer program that permits two-or-more users to conduct live (real-time), typed conversations. IRC is run through a virtual network of servers into which the user logs using a computer program called a client. Two popular client programs are MIRC and PIRCH, running under the Windows computer environment. These client programs create "windows" in which text may be typed and read simultaneously, creating a two-way, instantaneous written conversation between multiple people located anywhere in the world. Depending upon the sophistication of both the client program and the computer user, enhancements such as live video conferencing and file sharing are not only possible, but no more than a mouse-click away. After being logged on, a nickname is selected so that the user can be contacted by other users.\(^\text{17}\)

The choice of nicknames is frequently of considerable importance. Most users of IRC select a descriptive nickname germane to the user's purpose or personality. Users are often limited in their name selection only by the simultaneous existence of the same name. In other words, no two users may simultaneously log on with the same name. A service called "NickServ" first will warn the second user attempting to use the same name and, then, if the warning goes unheeded, will automatically rename the user. On one particular server, "UNDERNET," the server maintains a registry of nicknames. Through this registry, a user may sign up for a specific nickname, provided it is not already in use, and then keep the nickname for his own use from session to session. Generally speaking however, most servers do not store nicknames from session to session, and they are issued on a first come first served basis.

Because IRC is largely self-regulated, there are few restrictions placed on the choice of nicknames people may choose. Examples of acceptable nicknames are HARD4U and Bi-Fem-Amanda.\(^\text{18}\) Each conveys a very specific message. After selecting a login name you may either enter a pre-existing channel\(^\text{19}\) or create your own. With the exception of several server-run channels, a user can create any channel they wish. A typical example of a channel name is "!!!00000dads&daughtersex." Within the channel users, can chat in

\(^{17}\) This process is somewhat analogous to the CB radio.

\(^{18}\) These nicknames have been taken from actual users seen during on-line investigative sessions by the author.

\(^{19}\) A channel is a specific area within the server and is usually dedicated to specific topics. Depending upon the day and time, there may be any number of active channels on a server. During the author's most recent log-on session, Dal-net contained over 9,000 individual channels.
"public" mode where all members of the channel can see the conversation, or two users can chat in private mode, where they are the only two users that can see the conversation. This is often called whisper mode and is analogous to a two-party telephone call. With the exception of a few server-moderated channels, all channels on the servers are user-moderated, and anything goes. Because of this, IRC channels can be distinguished from services such as AOL and Compuserve, where most forums and discussion groups are server-moderated and conversations are frequently monitored. Because of this uncontrolled and unregulated atmosphere, the realm of IRC has been referred to by law enforcement as "cowboy country." This is the new frontier where practically anything goes. This area is where most law enforcement activity originates and is largely unregulated and uncontrolled.

The next step in the investigation is dictated by the manner in which the police receive the information. If the police receive a complaint from a user or an ISP, targeting has already been done. In this situation the undercover officer is armed with a nickname and usually a channel the target frequents. At the very least the police have an e-mail address. With these pieces of information it is a simple matter of entering the chat room and looking for that person. If complaints about a channel have been received, but not about a particular individual, then an "open trolling" operation begins. In either case, the "bait" used to lure the target is the undercover nickname. As discussed earlier, the choice of nicknames is frequently very descriptive. Most often, as an undercover officer, the choice is obvious. When looking for a pedophile, assume the personal characteristics of a young user, either male or female depending upon the target. A common tactic among investigators is to suffix the descriptive name with an age. Rachel-12 is quite common, as are other variations on that theme. The plan of attack is simple. Sit and wait — usually not for long. It has been my experience as an investigator that when using a female sounding name and a youthful persona, so many requests for private chat occur within five minutes that immediate response to all would be impossible.

Invariably the first question asked by "Ken_for_boys" or "Dad_4_daughter," is A/S/L, which is computer chat room short-hand for age, sex, and location. The normal response to that question is your assumed age, sex, and where you are calling from. In my estimation, in


21. This is a term used in law enforcement parlance, of which the derivation is unknown to the author. It is believed to refer to a fishing technique of sending out a baited hook and waiting for a fish strike.
approximately eight out of ten encounters on-line, the target asks for a photograph within the first five minutes of conversation. In my experience, getting a picture is the goal of the conversation. There are many collectors of photographs who make contact with someone on-line simply to add to their collection of images. If the undercover officer does not provide a picture, the conversation is usually terminated. When asking for a picture, the target is usually referring to a picture of the child with whom he believes he is talking. If this is unsuccessful, the target may ask for any pictures that the person may have collected. It must be kept in mind that at this stage, the target is not actually asking for the exchange of child pornography. The target is merely asking for a personal picture of the child — a legal request.

Because so many responses occur in a short period of time, the investigator must prioritize targets. This process is generally not capable of description, it is a learned art that I analogize to the ability of a car salesman to sort out the “lookie-loos” from the “real” customers. It is developed only after compiling hours of on-line experience, is an inexact science, and is frequently wrong. Many times I have relied upon gut instinct and experience, only to find that the target was merely interested in a brief on-line encounter, not a face-to-face meeting.

In the prioritization stage, it is essential that the investigator make no reference to anything sexual. Because entrapment in any undercover operation is an ever-present concern, inducement must be minimized. Conversations generally begin with very benign topics such as school, hobbies, and home life. It is helpful to assume an identity of some naivete. This allows for the deflection of difficult sexually-oriented questions without arousing the suspicions of the target.

Once the target has been selected, or perhaps more appropriately, has selected you, email addresses are usually exchanged. While chatting, sophisticated software programs are used to identify the target’s ISP. These programs, such as “Netlab” and “Neotrace,” operate undetected by the target.\(^2\) This check provides the undercover officer with a series of numbers known as an Internet Protocol (IP) address.\(^3\)

Each computer on the Internet, and every computer on local networks for that matter, is assigned a unique IP address. Without this series of numbers, the electronic traffic on the Internet would not reach the appropriate destination. The IP address is essentially a unique physi-

---

\(^2\) Undercover officers’ ISPs may also be obtained by the target; therefore, as in all undercover operations, during the choice of a cover story it is imperative that the story match with any information the target may obtain through the ISP.

\(^3\) An IP address is similar to a full street address. It is a series of four sets of numbers separated by periods.
cyber address assigned to each computer that identifies it in the Internet world. This address is associated with a domain name using many of the same programs the officer used to obtain the IP address. Armed with a domain name or IP address, the undercover officer then retrieves the information necessary to serve the ISP with a subpoena for records.

As part of the protocol of the Internet, all domain names are required to be registered with a service known as the InterNic. This service maintains an accurate and current database of the relations between IP addresses and the computer to which they are assigned. A simple query of the database provides the officer with a complete name and address for the person in charge of the domain name.

ISPs have become necessary because not every household computer has a permanent connection to the Internet. If every computer on the Internet was directly connected, then every computer in every home, university, or business would have a unique IP address. Because this is not the case, ISPs are often assigned several IP addresses. Under this configuration, ISP subscribers call into the bank of telephone lines owned by the ISP and are then “routed” to the Internet using the IP addresses assigned to the ISP. This dynamic system of IP assignment makes it possible for worldwide access to the Internet without having to have static IP addresses for every computer in the world.

This system also makes it more difficult to identify the target of an investigation. Obviously, if every computer on the Internet had its own address, InterNic would provide a specific user on every query. Because that is not the case, InterNic often provides only the information about the ISP, including the administrative contact for the provider, address and telephone number. Because a large provider may have hundreds or even thousands of simultaneous users logging in and “leap frogging” onto the Internet, a single IP address cannot discretely identify the target of the investigation. This is where the service of legal process becomes necessary.

Procedures vary from state to state. In Florida, the information sought may be released through the use of a State Attorney’s investigative subpoena. Through the subpoenaed information, the target’s name and address are learned. Usually each ISP maintains an access log. This access log identifies the users logged into the system at every sec-

24. Domain Name is a mnemonic used to represent textually the difficult-to-remember series of numbers. An example of a domain name is Microsoft.com. It is merely shorthand notation for humans.


26. The ISP processes only that information required for a user to obtain an account. If no verification is done by them, then the user’s information will more than likely be false. Most do, however, maintain a record of the incoming calls through an Automated Number Identifier (ANI).
ond of every day. From this information it is possible, although diffi-
cult, to identify which user was dynamically assigned to which IP
address. By matching the exact date and time of the on-line encounter
with the records of the ISP, it is often possible to identify the user
account from which the conversation originated.

The pursuit does not stop there. Many ISPs maintain a database
compiled from their ANI system. The ISP can, and usually does, iden-
tify the specific telephone line from which the login call was placed.
This ANI data is critical to the next step in the investigation.

The goal of the investigation is to arrange for a face-to-face meet-
ing between the target and the child. The semantics of how this is
accomplished are tricky. Most often, when the target suggests a meet-
ing, he suggests that the undercover travel to his location. Because of
jurisdictional and cost concerns, the preferred arrangement is for the tar-
get to meet at the undercover’s location. This arrangement gives the
police much more control over the meeting environment, providing for a
safer arrest with less chance of injury to the defendant, an officer, or an
innocent bystander. This arrangement also helps reduce the cost and
logistical problems of traveling to a remote meeting site. When the tar-
get agrees to this, it is frequently called a traveler case.27

Similar to narcotics investigations, the undercover officer places a
telephone call to the target and completes the arrangements for the meet-
ing on the telephone. The telephone calls are treated no differently than
recorded telephone calls placed for narcotics, gambling or any other
undercover operation. In Florida, the recording of telephone calls
between targets of a criminal investigation and a police undercover
officer is permitted.28 In fact, the recordings are powerful evidence of
the target’s willingness to engage in sexual acts, knowledge of the par-
lance of the criminal conduct and as well help to establish the target’s
belief that the undercover is a child.29

The final phase of the investigation is dictated mostly by the path
the target chooses. As stated earlier, the goal of the investigation is the
arrangement of a face-to-face meeting between the target and the under-
cover officer. By arranging this meeting, two issues are resolved. First,

An ANI is similar to caller-id and will provide the telephone number from which the user called.
From that the phone company can provide the rest.

29. For obvious reasons, the telephone calls are often placed by officers other than the
undercover. For example, a particular female officer, whose voice readily passes for that of a 14-
year-old-girl, places the call. Her assistance enables the target to openly discuss, on tape, the
various sexual acts that she will be asked to perform. This also removes many aspects of the "role
play" problem. See infra Part III.
the identity of the offender is established, and second, the offender’s true intentions are readily known. For example, in one particular Florida case, the offender arranged for a meeting with one he believed to be a child he had met on the Internet for the purpose of engaging in a sexual act.\textsuperscript{30} If the offender arrives at the meeting place, it corroborates the defendant’s intention to commit sexual acts with a child. Depending upon the approach taken by the offender and the circumstances perceived by investigators, an alternative strategy is to obtain a search warrant.

Based upon the officer’s investigation and the identification provided by the ISP, search warrants for the suspect’s residence and computer are obtained and executed. The actual manner in which the search warrant is executed may be of key importance in these cases.

As previously indicated, it is essential that the offender is positively identified as the person with whom messages have been exchanged. Without the benefit of a face-to-face meeting, it may be impossible to put the offender “behind-the-keyboard,” and thus prove he is in fact the same person. It is conceivable, and well within the range of reasonable doubt, that a person other than the genuine account holder, or telephone subscriber, could have been using the computer during the on-line conversations. It is possible to reduce this doubt by timing the search warrant execution to coincide with the offender’s on-line chat session. After obtaining the warrant, the undercover officer makes contact with the offender on-line, and begins chatting. The police then execute the warrant while the suspect is on-line chatting with the undercover officer. This allows the police to document that the person with whom the undercover is conversing is in fact the subject arrested.\textsuperscript{31}

Even in traveler cases, a secondary goal of the investigation is to obtain and execute a search warrant on the target’s personal computer. This is routinely done where the evidence supports it, and physical constraints allow. In my experience, offending pedophiles who go to the difficulty and risk of meeting with a child will possess child pornography, contact lists, and documentation of other meetings or other like-minded computer users. All these items, when seized legally, provide powerful evidence of the criminal act.

\textsuperscript{30} See State v. Duke, 709 So.2d 580 (Fla. 5th D.C.A. 1998).
\textsuperscript{31} This method poses the risk of the offender being able to delete information, or erase files at the time the warrant is being executed. For this reason, some agencies dislike this method in some situations.
III. THE TARGET

A. Know Your Enemy: Understanding the Pedophile Offender

In the struggle to reconcile the need for effective, efficient enforcement and prevention of child sexual abuses with the legal issues raised by the Internet phenomenon of chat rooms and pedophile solicitors, this article explores both the scientific definition of the disorder known as pedophilia, and empirical data of admitted pedophiles. This data has been collected in the hope that the methodologies in use by law enforcement can be reconciled with the requirement of fair and just adjudication.

The sexual predator addressed by section 847.0135, Florida Statutes, is commonly referred to by various names, ranging from pedophile to child molester, but all are characterized by one common denominator — the unnatural sexual attraction to children. Not all sexual predators are pedophiles, and not all pedophiles are sexual predators. Pedophilia, a specific medical diagnosis, is often thrown about with reckless abandon when discussing this particular type of sex offender. The true diagnosis of pedophilia falls into a class of disorders known as paraphilias and include such disorders as travestitism, exhibitionism, and sadism.

There are two distinctly different sub-groupings within the paraphilic subclassification of pedophilia. The classic pedophile, whose desire for sexual contact is directed at prepubertal children, and hebophiles, whose sexual interests run toward postpubertal children. Of the two, the pedophilic sex offender is most often the offender with the lowest rate of rehabilitation. Conversely, the hebophile has a comparatively higher rate of rehabilitation. In the clinical context, offenders in the hebophilic category may be referred to as child molesters instead of pedophiles. Both offenders, however, are characterized by an abnormal affinity for youthful sexual partners. To be clinically diagnosed as suffering from pedophilia, an offender must meet the criteria established by The Diagnostic and Statistical Manual of Mental Disorders. A diagnosed pedophile has 1) an impairment that lasts at least six months, with recurrent and “intense sexually arousing fantasies, sexual urges, or behaviors” that involve sexual activity with a prepubescent child or children (generally 13 years old or younger); 2) “fantasies, sexual urges, or behaviors [that] cause clinically significant distress or impairment in

34. See id.
35. See id. at 137.
social, occupational, or other important areas of functioning”; and, 3) the impaired person is at least aged 16 years, and at least five years older than the child or children.36

From this definition it is easy to see that not every on-line sexual predator can be easily categorized as a pedophile. If that is true, then with whom are we really dealing while we are on-line.

A number of on-line sites claim to cater to the prurient interests of pedophiles and advocate the freedom to associate with, and love anyone of your choosing. These sites range from the web site of the National Man-Boy Love Association (NAMBLA)37, to the Pedophile Liberation Front (PLF).38 The PLF site is broken down into four sections with each dedicated to individual areas of interest, including hyperlinks39 to other pedophile-oriented pages, alleged letters of support from former child-lovers of pedophiles, and pages contributed by members of the PLF. According to the PLF site:

[o]ne of the basic standpoints of the PLF is that sex is not harmful to children in itself. We believe that any harm happening to children in consequence of sexual activity with other children or with adults is caused by society’s reaction to such behaviour [sic]. It is the guilt and taboo associated with children’s sexuality (and with sexuality in general) that may cause psychological troubles to sexuate children.40

The PLF also takes a stance on the issue of child pornography. It feels that child pornography is no different from any other kind of pornography and that children are not victimized. They are simply encouraged to participate willingly.41 On the whole, the web site is a conglomeration of “don’t hate us, were not bad people” rhetoric with a dash of “allow me to educate you as to why you are wrong and we are right” hyperbole. The site advocates healthy sexual experimentation, decries forced sexual intercourse with children, and calls for the recognition of pedophilia as being no different or less acceptable than homosexuality or heterosexuality.

Of the articles found on the site, one is interesting enough to discuss further. The article is entitled, A Different Kind of Sexuality What


39. Hyperlinks are highlighted areas of text within a web page, that when clicked upon, will immediately take the reader to a new page or site.


41. See id.
“Real” Adults Cannot Understand. The author of this article, for obvious reasons, has chosen to use a pseudonym. This article, while very startling, attempts to define a rudimentary difference between pedophilic sexual attractions and normal non-pedophilic attractions. The author admits to the inability to relate sexually with adult women, and he explains this behavior as having to do with an adult woman’s greater demand for sexual closure — the need to see the sexual act through to the end. Children and pedophiles, however, are more attuned to the feelings involved, and they will not pressure a partner to continue with the sexual act. The on-line author claims that, in fact, the pedophile is just as content to stop all sexual exploration with a child, and turn his attention elsewhere. The impression given, and surely intended, by the on-line author is that pedophilic sexuality is somehow better, more caring, and more focused on feelings than non-pedophilic sexuality.

Reading the articles, manifestos, and short stories contained within the pages of this web site creates a mental picture of the pedophilic offender. This picture, however, is quite unlike the group of offenders found on-line. A few persons with whom I have engaged in conversation on-line exhibited traits similar to those espoused by the PLF. The majority, however, were much less emotionally attached, and more sexual gratification oriented. If the on-line authors of the articles truly adhere to their manifesto, the sexual contact with the child would be secondary to the conversational aspect of companionship. This is not primarily the case in real life. This finding begs the question, are those persons with whom on-line chats are occurring real pedophiles and the PLF rhetoric is merely public relations hype, or, are the on-line conversations occurring with sexual offenders who are not truly pedophilic offenders. Unfortunately, insufficient research data has been compiled to provide a reliable answer. A plausible explanation, however, does emerge.

According to William Prendergast, a distinction may be drawn between pedophiles and hebophiles. Pedophiles prefer prepubescent children, and hebophiles prefer postpubescent children. The stories and articles on the web site seem to exclusively address prepubescent attraction. On-line, however, a preponderance of the persons encountered are interested in children between thirteen and fifteen. This age range clearly encompasses postpubescent children and raises the plausible con-
Conclusion that when a child is described on-line as a postpubescent adolescent — between the ages of thirteen and fifteen — the dynamic of the entire conversation changes. This explanation accounts for the difference between the behavior of the PLF subjects and those actually encountered. Accordingly, this conclusion may sufficiently explain the differences observed between the self-proclaimed tendencies of the PLF supporters and actual on-line contacts.

If investigative targets are in fact pedophiles, what predisposes them to congregate on-line? A number of factors combine to make the on-line world an exceptionally attractive venue for pedophiles to prowl. Studies indicate that pedophiles have an active sexual fantasy life composed mainly of sexual encounters with children.\textsuperscript{46} A pedophile may seek relief from the internal discord created by his\textsuperscript{47} overwhelming desire to have sexual contact with a child, and his recognition that there are severe consequences to his actions, by self-gratification.\textsuperscript{48} This cycle of erotic cravings and fantasy coupled with masturbatory gratification reinforces the pedophile’s need for contact with childlike partners.\textsuperscript{49} This vicious cycle of deviant fantasy and reward-based reinforcement intensifies the offender’s desires, until almost every erection and ejaculation must be accompanied by a deviant fantasy.\textsuperscript{50} The strength of these fantasies has been characterized as irresistible.\textsuperscript{51} The non offending pedophile, trapped beneath the weight of his own repressed deviant behavior and unable to quell the deviant urges within him, naturally turns to the anonymity of the Internet for solace.

Research clearly indicates that pedophilic males tend to become aroused while listening to audio-taped depictions of sexual activity with children.\textsuperscript{52} The predominant research also adheres to the previously discussed cycle of stimulus and response. As the cycle repeats more frequently, arousal will be reinforced more strongly;\textsuperscript{53} therefore, sexual fantasies of pedophilic sex offenders play both a causal and maintenance role. Studies of sexual deviants have found that the majority

\textsuperscript{46} See Fred S. Berlin, \textit{Sex Offenders: A Biomedical Perspective and a Status report on Biomedical Treatment}, in \textit{THE SEXUAL AGGRESSOR} 83 (Joanne G. Greer & Irving R. Stuart eds., 1983).

\textsuperscript{47} See id. Pedophilia is almost exclusively a disorder afflicting males.

\textsuperscript{48} See id. at 85.

\textsuperscript{49} See id. at 88.

\textsuperscript{50} See Paul A. Walker et al., \textit{Antiandrogenic Treatment of the Paraphilias}, in \textit{GUIDELINES FOR THE USE OF PSYCHOTROPIC DRUGS} 427, 429 (Harvey C. Stancer et al. eds., 1984).

\textsuperscript{51} See BERLIN, supra note 46, at 88.


reported masturbating to deviant fantasies based upon the deviation of their preference.\textsuperscript{54} Hence, an environment renown for its fantasy-like qualities lends itself quite well to the deviant fantasies of pedophiliacs. This fantasy-release continuum appears to be a benign way to control deviant behavior. Research suggests however, that if this cycle continues to self-perpetuate, eventually the fantastic behavior is no longer satisfactory, and the pedophile must resort to more tactile stimulation. This segue from fantasy to reality may very well be the bridge between the debatably harmless role player and the predisposed child sex offender.

Because not all pedophiliacs assault children, they should be divided into two categories — non offending pedophiles and offending pedophiles. It is well established that a non-offending pedophile is guilty of no crime.\textsuperscript{55} Conversely, the offending pedophile is subject to liability for any statute his conduct violates. Both the offending and non offending pedophiles may use the Internet for legitimate, non-criminal purposes as well as the currently criminal end of child solicitation. For this reason — the inability to distinguish harmful solicitation from mere fantasy release — proponents of strict regulation of solicitation crimes advocate strong enforcement efforts. Under the foregoing rationale, non-offending pedophiles who engage in fantasy role play on the Internet are distinguishable from their offending counterpart by the absence of any solicitation activity. Generally, perhaps this is true.

Consider, however, the non offending pedophile, whose fantasy role playing involves a clandestine meeting with a thirteen-year-old. In “playing out” this fantasy on the Internet during an on-line chat session, the pedophile discusses the particulars of the meeting, including the various sexual acts that the child would be expected to perform. We can assume, arguendo, that the pedophile is non offending and has no real intention of carrying out the meeting or sexual contact. In this scenario, the offender may be guilty of a crime under some laws even though his conduct extended no further than mere guilty thoughts. In this unusual but plausible scenario, the non offending pedophile’s fantasy mechanism produces results nearly identical to those of the offending pedophile who arranges for a meeting but simply fails to show. Both are liable under the language of the law; however, only one ever intended to engage in the underlying conduct we truly wish to prevent.


IV. THE LAW

A. Fear Spurs Action

It is clear from the collected data that pedophiles are present on the Internet in and out of chat rooms. The media has reported this Internet presence frequently and zealously. These harbingers prophesize about a time when no child will be safe in cyberspace from the evil that lurks behind every chat room door. This media onslaught is not new, but legislators bent on singlehandedly making our "cyberstreets" safe once again are watching very closely. The Alabama Senate Judiciary Committee passed a bill based upon the perceived threat to children from Internet pedophiles. Republican Bill Armistead referred to recent newspaper articles in support of his call for the new legislation. In Boston, Massachusetts Attorney General Scott Harshbarger pleaded for stronger legislation making solicitation of children online a criminal act in itself. Fear of online predators has led to more than one state's passage of legislation criminalizing the Internet solicitation of children. This public fear of online sexual predators influenced the passage, and subsequent amendment of a computer pornography statute in Florida.

B. Florida Statute 847.0135

Florida law enforcement officials prosecute most Internet activities of this nature under section 847.0135 — the Computer Pornography and Child Exploitation Prevention Act of 1986. In particular, subsection three prohibits the use of computer online services for the purpose of soliciting a child to commit a sexual act. This section has prompted police to pursue cases of Internet solicitation. The popularity of these cases has become so great that the Florida Department of Law Enforcement (FDLE) now has specific investigative agents assigned to conduct these type of investigations.

The legislature passed this statute in 1986 as part of Florida's anti-computer pornography and child exploitation effort; however, it went largely unnoticed until 1996. The original statute was not drafted with the language necessary to address the solicitation cases now routinely

57. See Bill Seeks to Crack Down on Child Sex Solicitations on Internet, ASSOCIATED PRESS, Mar. 27, 1997, available in 1997 WL 2512012.
58. See id.
60. See FLA. STAT. § 847.0135 (1997).
61. See FLA. STAT. § 847.0135(3).
prosecuted under the statute. In 1996, the Florida legislature amended the statute to criminalize the mere solicitation of a child for sexual contact through on-line services. Deterrence of the perceived threat of lecherous "dirty-old-men" prowling the Internet in search of prey motivated legislators to add section three of the statute. The most substantial changes to the law occurred with the addition of sections three through five. Section three contains the substantive language upon which most, if not all, Internet solicitation cases are predicated.

Section three provides: "Any person who knowingly utilizes a computer on-line service, Internet service, or local bulletin board service to seduce, solicit, lure, or entice, or attempt to seduce, solicit, lure, or entice, a child or another person believed by the person to be a child" into any sexual act, whether sexual battery, lewdness or indecent exposure, is guilty of a third degree felony. The sweeping breadth of the language alone causes concern about the scope of this law's power.

As a parent, laws that provide assistance in protecting our children will always be well received. Popular laws, however, are not always just laws. Looking critically at the statute, two interrelated problems emerge. The section contains essentially three distinct elements: (1) the conduct element of using the computer to solicit; (2) the attendant circumstance that the person solicited is a child; and (3) the acts to be committed are one of several related sexual activities. These elements contain language making them broad and powerful tools, but in some circumstances they may overextend the ability of law enforcement to bring citizens into the purview of the courts.

V. The Problems

A. Double-Inchoate Crimes

The conduct element requires the actus reus of solicitation. "[T]he solicitation is complete the instant the actor communicates the solicitation. . . ." No further overt acts are necessary. While the efficacy of punishment for such inchoate crimes is open to debate, the punishment of solicitations is a legitimate exercise of legislative power.

The second clause of section three compounds the inherent problems of liability for inchoate offenses. Strict grammatical analysis of the sentence reveals that the word "attempt" modifies the phrase "to

64. See 1996 Fla. Laws ch. 96-338, sec. 70 §3 (Amending Fla. Stat. 847.0135 (1986)).
65. See 1996 Fla. Laws ch. 96-338, sec. 70 §§ 3-5.
seduce, solicit, lure, or entice . . . ”68 This language makes it not only a crime to solicit, but also a crime to attempt to solicit—a double inchoate crime.

The crime of solicitation itself is a specific intent crime.69 “A person cannot be guilty of solicitation unless he intentionally commits the actus reus of the” solicitation offense and intends the result for which he solicited participation.70 Here the actus reus is the knowing use of a computer on-line service to entice or encourage a child to commit one of the enumerated acts.

The premise underlying the punishment of inchoate crimes like solicitation and conspiracy is that special dangers of group criminality exist where two people unite to commit an offense. The whole is more dangerous than its individual components.71 Under this theory, the point at which criminality attaches to conduct moves further back in time. It is well established in American law that “[t]he reach of the criminal law has long been limited by the principle that no one is punishable for his thoughts.”72 Since the ability to know what another human being is thinking is so limited, one cannot accurately reconstruct the thoughts of another to prove any criminality.73 Closely allied with this concept is the concern that there is no way to determine where fantasy or daydreams end and desires of fixed intention that pose a real danger to society begin.74 Society hesitates to punish mere guilty thoughts because the use of our criminal law should be reserved for those instances where society is truly threatened with harm.75 The individual liberties of our citizens are valuable; we must carefully tread upon them, limiting our encroachment only to conduct, not thoughts.76 Placing thoughts at the far left edge of the criminality spectrum and voluntary criminal acts, or the actus reus of a substantive offense, at the far right, society can construct a model with which to think. This model illustrates the difficulty posed as criminality of conduct shifts.

In the case of conspiracy, illegality is positioned only slightly to the left of the right edge of the spectrum. This shift to the left, away from acts and toward thoughts, clearly encroaches into the area of “guilty thoughts.” Society accepts this position, but out of fear that concert of

68. FLA. STAT. § 847.0135(3) (1997).
69. See DRESSLER, supra note 67, at §28.01[A][2].
70. Id.
71. See id. at §29.03[B].
72. United States v. Muzii, 676 F.2d 919, 920 (2d Cir. 1982).
73. See DRESSLER, supra note 67, at §9.01[B].
74. See id.
75. See id.
76. See id.
action will create greater risk to society. The gist of the conspiracy charge is the agreement to act; hence, we recognize the purported danger of an increased likelihood of success of the criminal endeavor. We are willing to make this sacrifice because, as discussed earlier, injury is seriously threatened.

Solicitation is the next step to the left on the spectrum. The inchoate crime of solicitation has occasionally been defined as an attempted conspiracy. By criminalizing conduct at this position on the spectrum, we have moved one large step to the left — away from the actus reus requirement and toward the mere thoughts category. Historically, the punishment of solicitation as a crime has been the subject of heated academic debates. A strong argument must be made that by criminalizing solicitation, the leftward shift on our spectrum moves so close to punishing guilty thoughts that it is contrary to our principles of justice. According to Glanville Williams, however, this leftward shift is necessary in order to allow police to prevent crimes — a legitimate goal of society. The obvious antithesis to this view is that as the conduct we are trying to punish moves closer to the left edge of the spectrum, we must ask whether the defendant’s acts are sufficiently dangerous to warrant judicial intervention. While society accepts the hypothesis that a real danger to our children exists, we position the threshold of punishment much farther to the left and allow police intervention at a much earlier point. Instead of awaiting the inevitable conclusion of the criminal conspiracy, we allow the termination of the enterprise upon its inception.

With this statute, however, the threshold of criminality has been moved back even farther. Analysis shows that punishment is legislatively created when the actor merely attempts to solicit the child. Referring back to our model of criminal conduct, the threshold created in solicitation cases is dangerously close to the left edge — guilty thoughts. Here, the legislature has encroached even more upon thoughts.

Under Florida law, the crime of attempted solicitation does not exist; however, there is nothing to preclude the creation of such an offense by the legislature. Here, that is what the legislature has done. Through the creation of the attempt to solicit, it has created a statutory double-inchoate crime.

This codified form of double-inchoate crimes is, in logical terms,

77. See id. at § 29.04[A].
78. See id. at § 28.01[D].
79. See id. (quoting GLANVILLE WILLIAMS, CRIMINAL LAW: THE GENERAL PART 609 (2d ed. 1961)).
80. See Brown v. State, 550 So.2d 142, 144 (Fla. 1st D.C.A. 1989).
an attempt at an attempt to conspire.\textsuperscript{81} All the concerns which have been raised by the prospect of punishment for attempted conspiracy immediately become magnified because the acts of the defendant have not changed, but encroachment of liberty has.

The rationale for punishment of inchoate crimes still applies, but the farther society moves criminality toward the “thought” end of the spectrum, the greater the danger to society. Under the unity of purpose, or strength in numbers analysis commonly done in conspiracy situations, it is asserted that the mere revelation to another of the criminal scheme extends the conduct far beyond the realm of preparation and into that of attempt.\textsuperscript{82} Following that line of reasoning in attempts to attempt to conspire, there should be an increased danger of completion of the substantive crime before allowing such drastic motion to the left on our spectrum.

In reality, this double-inchoate crime problem is rarely expected to arise. Instead the greater concern is the inchoate crime of solicitation itself. As discussed earlier, the logic behind the recognition of these crimes is sound; however, when these reasons are superimposed against the unusual circumstances presented by on-line activities, heavy-handed enforcement may create greater concerns. Because there is a tremendous propensity for fantasy on the Internet, overzealous enforcement of the solicitation statute can easily overstep principles militating against the punishment of guilty thoughts.

The second element, the attendant circumstance that the actor believes the person solicited is a child, also presents a concern in the on-line context. As a law enforcement officer engaged in this ongoing computer battle, I welcomed the addition of language that enables undercover operatives to assume identities on-line, posing as children and covertly conduct investigations. The difficulty encountered is establishing that the target has a founded belief that the person with whom they speak, the undercover officer, is in fact a child. This issue is, therefore, one of proof, not of ineffective legal drafting. As long as the officer can demonstrate through evidence and testimony that the offender “believed” the officer was a child, there is marginal room for attack. Under conventional forms of covert investigations, this element is relatively straightforward. If an undercover officer approaches a target with property claimed by the undercover officer to be stolen and the target, in turn, purchases the “stolen” goods, it is relatively simple to prove belief. The officer must simply testify that he told the target the goods were stolen. In the context of on-line communications, specifi-

\textsuperscript{82} See id. at 31.
cally the purview of chat rooms and role-playing, it may be much more difficult to argue successfully that the offender had an actual belief. It is easy to foresee the defendant claiming that he felt he was merely "role-playing" and that he believed that the person with whom he was conversing was doing the same. The nature of the on-line environment adds to the difficulty of proof in these cases.

B. The "Guilty Thoughts" Problem to the nth Power

To further complicate matters, virtual communities exist within the computer world. These communities, called MUDs, MOOs, MUSHs and a variety of other odd sounding names, exist totally within cyberspace, populated only by Internet users. Originally the product of role-playing enthusiasts, they have evolved into much more complex and interactive spaces well suited for role play and fantasy.

Professor Sherry Turkle, of MIT, has conducted research in this area, and she has confirmed what most Internet users have known all along: there is very little "reality" in virtual reality. The communities she studied consist of cross-gendered beings that are fictional characters often bearing no relation to the real identity of the participant. These participants routinely engaged in explicit sexual relations, including virtual rapes and multi-partner sexual trysts. Additionally, accounts of murders are depicted on-line and thefts of other characters' "virtual" personal belongings. These behaviors do not encompass any type of criminal liability, but do raise interesting questions about fantasy and role play related to our pedophile discussion.

This world of virtual reality is populated with a limitless array of characters, all posing as someone other than whom they really are. From a prosecutorial standpoint, how does one establish that the offending pedophile had a real belief in the age of his on-line partner. In a world so overwhelmingly fictional, such as the Internet, it is reasonable to assume that every on-line user has a very good idea that anyone he speaks with, in the context of chat-rooms and MUDS, is using mostly fictional information. In fact, in areas such as IRC, specific rooms dedicate themselves to explicit sexual role play. Virtually any type of sexual

84. See generally William Gibson, Neuromancer (1984) (coining the term cyberspace which has gained widespread acceptance as a term referring generally to the virtual world).
85. See Turkle, supra note 83, at 11-15.
86. See id.
87. See id.
88. See id.
89. See id.
fantasy may be witnessed (or participated in), including explicit rapes and violent encounters. In this environment, where all members of the room are using assumed identities, there is no ability to determine the race, sex, or age of the occupants.

This premise may be extended to situations where pedophiles engage in fantasy role play in their own private channel. Given the aforementioned information, is it impossible to imagine that the participants in a pedophile-oriented chat room truly believe, as the statute requires, that the persons with whom they discuss sexual acts are children?

Again, the problem lies not in the fact that belief cannot be proven, but that the unique characteristics of cyberspace create uncommon impediments to establishing the mental elements of inchoate crimes. When a computer user on-line knows that every person with whom he is chatting is assuming some alter ego, there is no plausible way to determine at what point he becomes convinced that his partner is really the person he says he is.

While chatting, I may become the President of the United States of America. Everyone I chat with knows that everyone else is assuming an identity unrelated to, or at least suppressed by, the real world. When is it possible to say that someone really believes that they are talking with the President? In other words, we all know that on-line we are not who we say we are. Knowing that, we cannot truly expect to be able to say, beyond a reasonable doubt that discussions of meeting for sex are not mere “big talk” and braggadocio.

One potential solution, instituted on a procedural level, is through the adjunct use of traditional undercover operations. By corroborating the target’s belief through controlled telephone calls and awaiting his actual arrival at a predetermined meeting place, it may be possible to establish the reality of the target’s belief. While this solution seems to work, it is one that must be instituted on a procedural level, and is not necessarily called for by the language of the statute.

For example, a target, call him John, engages in an on-line conversation with Jill, an undercover officer posing as a thirteen-year-old child. After several weeks chatting, e-mails, and picture exchanges, John suggests that he and Jill should meet. John also suggests that when they meet, Jill should perform fellatio on him.

Clearly, under the definition of section 800.04, Florida Statutes, the performance of fellatio by a thirteen-year-old girl is a felony of the second degree.\textsuperscript{90} Under section 847.0135(3), solicitation to commit any

\textsuperscript{90} See Fla. Stat. § 800.04 (1997).
illegal act described in chapter 800 relating to lewdness is a felony of the third degree. Therefore, because John has solicited Jill to commit this lewd act, he can be charged under section 847.0135(3). Conviction is another matter. Of course, the prosecution must meet the constitutional level of proof necessary for conviction. Depending upon the ability of the undercover officer to testify, and the explicitness with which the offender discussed the details of the meeting, conviction may or may not be attainable.

The third element of the crime specifically delineates those offenses where solicitation will incur liability. In essence, these enumerated crimes are those crimes society views as the real danger. Based upon the enumerated crimes, it is clear that the legislature desires to protect children from sexual contact. It may therefore be inferred that the purpose of this statute is to prevent children from being victimized sexually through the use of computers — a noble goal. The enumerated crimes are irrefutably harmful to society — particularly to children. They are generally well established as legitimately proscribed conduct, and they are quite beyond question in regard to enforceability.

The amendment of section 847.0135 is clearly the result of increased public awareness of the use by sexual predators of the computer for victim selection and contact. Is this a rational response to a genuine threat, or is this a knee-jerk reaction to a perceived danger?

Further critical analysis of the methodology currently used by law enforcement agencies is required. This analysis must be superimposed against the questions about the statute itself, and the intricacies of the computer world already discussed.

C. Entrapment

1. OVERVIEW OF ENTRAPMENT AS THE DEFENSE

One of the most difficult situations encountered by any undercover officer during covert operations is the problem of entrapment. This problem is no trivial matter. Normally, the added difficulties of cyberspace only intensify the problem. Cyberspace produces greater issues regarding proof of predisposition when targeting defendants. A proper analysis must start with a careful examination of the defense itself, then progress into the application of that defense to the current problem.

Entrapment is an affirmative defense that exonerates a defendant from conviction for otherwise criminal conduct because of law enforcement tactics. Although the defense was characterized during early years

as a defense of limited use, one may speculate that the heightened war on drugs and the explosion of drug related crime during the 1980s stretched police enforcement efforts to the very limits of legal acceptability. In conjunction with the explosion of drug trafficking in the 1980s, law enforcement faced a unique problem. Methods of enforcement lacked effectiveness. The traditional, reactive style of policing, so well suited to burglary, grand theft, or murder investigation, became nearly useless in the context of narcotics smuggling and sales. The shackling of law enforcement effectiveness necessarily led to innovative methods through which to attack the problem.

These innovations, while obviously not entirely new, were employed on a grand scale. Tactics such as undercover operations and street level interdiction operations became not the exception, but standard operating practice. That is not to say that the technique of undercover operation was never before used. The nuance here, however, was the methods and scale with which agencies employed the tactic. A method reserved heretofore for specific, targeted operations, such as stolen property rings, prostitution organizations, and gambling was now employed in the mass market of criminal conduct.

The process, which I euphemistically refer to as “Darwinism in the hood,” transposes Darwin’s evolutionary theory into the highly accelerated world of competitive criminal life. While human characteristics and genetic codes do not necessarily adapt more rapidly, their abilities to transform themselves and their environment does. This is seen no more readily than in the adaptability of criminals to new methods of enforcement.

As criminals metamorphose into beings of superior criminal intellect, their methods of criminal accomplishment distill into better and more powerful tools, and law enforcement does what it has done for years — it plays catch up. True to its nature, the slow moving, slothful creature that is government, evolves in this ever more competitive biocenosis at a somewhat slower pace. It does, however, evolve. Contrary to popular thought, the police must adapt or they will be overcome. In the 1980s, the problem was drugs, most particularly, street-level drugs. Today, it is the Internet criminal. Tomorrow — who knows?

In the 1980s and early 1990s, law enforcement redirected its response to the drug war in novel ways. One of the most novel was the manufacture of crack cocaine by the Broward County, Florida Sheriff’s Office for resale to potential defendants. This adaptive response is an inevitable reaction to changing patterns in criminal conduct. Not sur-

93. See State v. Williams, 623 So.2d 462 (Fla. 1993).
prisingly, when law enforcement assumes a more aggressive enforcement prerogative, issues arise surrounding the exact extent to which police may encourage criminals to commit crimes.

Based on historical lessons learned through the fight against drugs law enforcement has become slightly more agile. When the eventual, some say predictable, happened, and criminals began to capitalize on the resources of computer technology, most police agencies clamored to recruit and train computer literate officers. With this we again see the aggressive, proactive use of undercover techniques, this time applied to virtual reality.

Law enforcement embraces cyberspace as a new venue from which to conduct covert operations for the same reasons that criminals are drawn to the Internet. Gone are the days of the U/C line. Today’s’ U/C line is a hotmail, E-mail account and an Internet connection. The benefits are obvious. Little cost is involved, especially compared with the relatively large expenditure necessary to establish a conventional cover, and many targets may be worked simultaneously in a short period of time. Officers are no longer limited by the awkward burdens of time and space. Most importantly, an undercover officer can assume any identity, age, or gender required by the intelligence data.

Over time, this new area of attack will necessarily attract its share of entrapment defense claims. Even under the best conditions, the undercover officers, involves herself in the encouragement of the offender to commit the crime. Eventually a defendant will present himself in a manner more conducive to the ability to raise the entrapment defense if the “child” with whom he is discussing oral sex is a law enforcement official.

2. FEDERAL ENTRAPMENT — THE EXEGESIS OF THE DEFENSE

In 1932, the United States Supreme Court recognized the affirmative defense of entrapment for the first time in the seminal case of Sorrells v. United States. From this humble beginning, the defense has undergone a divergent path of interpretation fraught with strong debate between scholars and judges. Along one path there lies the “subjective” definition of entrapment which is first announced in Sorrells. The other is the “objective” test, best established by Justice Roberts’ concurrence.

94. Law enforcement parlance for a dedicated telephone line, usually listed in a fictional non-existent name, from which telephone calls could be placed or received during undercover sting operations.

95. Hotmail, a product of Microsoft®, offers free E-mail accounts without verification of identity. Criminals and cops alike can assume as many personae through E-mail addresses as they wish.

96. 287 U.S. 435 (1932).
in the same case. While these two paths have similar characteristics, they are predicated upon slightly different lines of legal reasoning.

i. The Subjective Standard

The subjective test established by *Sorrells* views the question from the defendant’s standpoint. If the defendant had no criminal predisposition, and was induced by governmentally-sponsored deception, then he cannot be held liable for the crime. Writing for the majority, Chief Justice Hughes relied heavily on the principle that criminal conduct and punishment for actions must stem from culpability. This criminal intent must originate with the defendant, not the government. Where the criminal intent is based upon the governments’ provocation, there is really no criminal intent on the part of the defendant and he should not be punished.

ii. The Objective Standard

As stated earlier, Justice Roberts’ concurrence opinion in *Sorrells* established the objective test for entrapment. In this matter, Justice Roberts relied heavily on the government agents’ entreaty conduct. Much later, in *Sherman v. United States*, Justice Frankfurter said that the objective approach “shifts attention . . . to the conduct of the police and the likelihood, objectively considered, that it would entrap only those ready and willing to commit crime.” In essence, the questions asked under the objective test look more critically at the nature of the police conduct employed to ensnare the target. While the distinctions between the two analyses may be slight, the intrinsic versus extrinsic perspectives make a world of difference.

The subjective theory requires the finder of fact to determine the question of entrapment. Conversely, Justices Roberts’ and Frankfurter’s objective approach asks whether the police conduct is a proper use of governmental power. Justices Roberts and Frankfurter focus the analysis on the conduct of police, theorizing that the defense of entrapment is oriented toward curtailing abusive police practices.

---

99. See id. at 188.
100. See *Sorrells*, 287 U.S. at 452.
101. See id. at 459.
102. See id.
104. Id. at 384 (Frankfurter, J., concurring).
105. See id. at 382 (Frankfurter, J., concurring).
Subsequent decisions by the Supreme Court have entrenched the subjective approach. In United States v. Russell,\textsuperscript{106} the court addressed a second issue tied to the entrapment defense. The defendant in Russell alleged that the police conduct was so egregious as to violate the Due Process Clause.\textsuperscript{107} The court reasoned that, in theory, the possibility exists that distasteful police conduct can rise to the level of a due process issue, but it did not do so in this case.\textsuperscript{108} Rather, the court focused on the predisposition of the defendant.

Taking this line of reasoning one step further, in United States v. Hampton,\textsuperscript{109} the Court conflated the tests for entrapment and due process, and it ruled that proof of a defendant’s predisposition precludes use of either as a defense.\textsuperscript{110} In so holding, Justice Rehnquist relied heavily upon the decisions in both Russell and Sherman, reiterating that entrapment arises only when “the Government’s deception actually implants the criminal design in the mind of the defendant. . . .”\textsuperscript{111} Because the Court found the defendant predisposed to commit the crime he was unable to raise the defense. Although the United States Supreme Court categorically rejected the “objective” standard of due process, the Supreme Court of Florida has, on occasion, considered its adoption.

3. THE FLORIDA STANDARD

i. The Cruz Test

In 1985, the Florida Supreme Court accepted the objective test for entrapment in Cruz v. State.\textsuperscript{112} In Cruz, a police officer posed as a drunken indigent displaying $150 dangling from his rear pocket. The defendant, took the money and was arrested. Justice Erhlich, writing for the majority, outlined the evolution of the entrapment defense, through Sorrells, Sherman and eventually Hampton. Justice Erhlich departs from United States Supreme Court precedent and posits that a subjective test and an objective test can coexist in Florida’s jurisprudence.\textsuperscript{113} To bolster this postulate, Justice Erhlich cites a New Jersey Supreme Court decision that, in his opinion, supports the proposition.\textsuperscript{114}

\textsuperscript{106} 411 U.S. 423 (1973).
\textsuperscript{107} See id. at 430.
\textsuperscript{108} See id.
\textsuperscript{109} 425 U.S. 484 (1976).
\textsuperscript{110} See id. at 488.
\textsuperscript{111} Id. at 489 (quoting Russell, 411 U.S. at 436).
\textsuperscript{112} 465 So.2d 516, cert. denied, 473 U.S. 905 (1985) (superseded by FLA. STAT. § 777.201);
\textsuperscript{113} cf. Gonzalez v. State, 571 So.2d 1346 (Fla. 3d D.C.A. 1990).
\textsuperscript{114} See Cruz, 465 So.2d at 521.
The Molnar court viewed the defense of entrapment from the standpoint that police conduct, not the predisposition of the defendant, is the key. It accepted the subjective test of Sorrells. Further, the Molnar court stated that even when the defendant is shown to be predisposed, certain law enforcement practices may nevertheless preclude conviction of the defendant. In the court’s opinion, the egregiousness of the conduct controlled more than the mere predisposition of the defendant.\textsuperscript{115}

The net result of the Cruz decision is to create a two-prong test to gauge entrapment. The Cruz test, establishes an objective threshold of entrapment. Once the objective threshold is passed, the second prong becomes “whether the criminal design originates with the officials of the government. . . .”\textsuperscript{116} In essence, the second prong is a test for predisposition in slightly different terms.

The Cruz court established a specific guide for trial courts, and it announced exactly what must be the subject of inquiry in such a case.\textsuperscript{117} To pass the Cruz test, police conduct must “(1) have as its end the interruption of a specific ongoing criminal activity; and (2) utilize means reasonably tailored to apprehend those involved in the ongoing criminal activity.”\textsuperscript{118} Applying this test to the facts of Cruz, the court reasoned that the state’s conduct was entrapment as a matter of law.

ii. The Legislative Answer to Cruz and the Court’s Response: In Through the backdoor

This Cruz test for entrapment was short-lived. In 1987, perhaps in response to the Florida Supreme Court’s flirtation with the objective test issue, the Florida Legislature adopted section 777.201.\textsuperscript{119} This legislation clearly established that entrapment in Florida was to be decided by a subjective standard. Not until Gonzalez v. State,\textsuperscript{120} however, was it was clear that the statutory entrapment test replaced the Cruz test. While Gonzalez was the first case to reconcile the two standards, it was not the most influential. For that one must examine Munoz v. State.\textsuperscript{121}

In Munoz, Justice Overton, writing for the majority, clarified rather succinctly that the legislature eliminated the objective test of Cruz.\textsuperscript{122} The court, however, retained the ability to examine the entrapment issue

\begin{enumerate}
\item See id.
\item Cruz, 465 So.2d at 521 (quoting to Sorrells, 287 U.S. at 442) (internal quotation marks omitted).
\item Cruz, 465 So.2d at 521-22.
\item Id. at 522.
\item 571 So.2d 1346 (Fla. 3d D.C.A. 1990).
\item 629 So.2d 90 (Fla. 1993).
\item See id. at 91.
\end{enumerate}
under a state constitutional Due Process analysis. Specifically, the Munoz court recognized the legislature’s ability to abolish judicially established principles of decision making. It cannot, however, remove freedoms guaranteed under the Florida Constitution. Through this rationale, the court established that entrapment in Florida may still be determined in a pseudo-objective manner under the guise of due process analysis. By implicating the Florida Constitution and predicating the due process analysis upon it, the Court adeptly removed the issue from the purview of the United States Supreme Court. The Munoz decision established a Cruz-type standard under a refurbished countenance.

The new test under Florida law, post-Munoz, is again a two-part test. If the conduct of law enforcement is so egregious that it shocks the conscience of the court, then entrapment, as a matter of law, may be based upon the principle of due process. Absent egregious conduct, the test rests solely upon the subjective standard established by the Supreme Court in Jacobson v. United States. Under the logic of Munoz, the legislature withdrew the objective standard test from the state supreme court. The Florida Supreme Court, however, reincarnated it under the guise of state constitutional analysis, making some form of the “objective test” for entrapment a continued viable affirmative defense. In fact, Justice Kogan, in concurrence, spoke of this implication: “Thus, the majority appears to toss ‘objective entrapment’ out the front door but then readmits essentially the same concept into Florida law via the rear entrance, with some minor tinkering as to analysis.”

Under Munoz, the defense of subjective entrapment is evaluated in three stages. First, the defendant must show, by a preponderance of the evidence, that the government agent induced his criminal conduct. The second issue examines the defendant’s predisposition to commit the charged offense. On this issue, the burden again lies with the defendant. As indicated in Munoz, however, the defendant’s burden is minimal. Once this threshold has been met the burden of proof shifts to the prosecution. To rebut the defendant’s evidence of lack of predisposition, the prosecution must establish its case beyond a reasonable doubt. The third and final question raised is who is the proper deci-

123. See id. at 98-99.
124. See id. at 99.
126. Munoz, 629 So.2d at 102 (Kogan, J., concurring).
127. See id. at 99; see also Fla. Stat. § 777.201 (1997).
128. See Munoz, 629 So.2d at 99.
129. See id. (stating that “as soon as the defendant produces evidence of no predisposition, the burden of proof shifts to the prosecution”).
130. See id.
sion maker for the issue of subjective entrapment.

Under the statute, it is clear that the decision shall be made by the trier of fact.\textsuperscript{131} The court however, takes the analysis further. If the defendant presents evidence of lack of predisposition where the factual circumstances are not in dispute and the government cannot reach the level of proof required to prove predisposition, then the trial judge may rule on the issue as a matter of law.\textsuperscript{132} In the remaining cases, the issue of subjective entrapment must go to the jury.

D. Application of the Principle to the Problem

We can superimpose Florida’s affirmative defense of entrapment against police conduct allegedly rife with potential for abuse. The court’s dictum in \textit{Munoz} points heavily toward a preference for, and reluctance to depart from, a two-step analysis of the entrapment defense. It is, therefore, essential that we examine the due process issue first.\textsuperscript{133}

1. DUE PROCESS VIOLATIONS

To provide a map of conduct constituting a due process violation under the \textit{Munoz} standard, it is beneficial to examine conduct previously considered as such. In \textit{State v. Glosson},\textsuperscript{134} the state provided a substantial monetary incentive for an informant to arrange a drug deal, secure an arrest, testify, and obtain a conviction. Upon the completion of these conditions, the informant would receive ten percent of all forfeiture proceedings. Based upon these facts, the Supreme Court of Florida found that entrapment had occurred as a matter of law.\textsuperscript{135} Although this case predates \textit{Munoz}, the opinion is quite beneficial to our discussion because it rests upon due process violations, not upon the \textit{Cruz} test.

In \textit{Glosson}, the court rejects the notion that \textit{Hampton v. United States}\textsuperscript{136} forecloses the use of a due process defense by a defendant who is predisposed under the entrapment analysis.\textsuperscript{137} By rejecting the very limited use of due process in the federal courts, the state supreme court effectively shifted the focus from the defendants’ predisposition to the government’s conduct. This fact, as stated earlier, creates a hole in post-

\textsuperscript{131} See FLA. STAT. § 777.2012; see also \textit{Munoz}, 629 So.2d at 100.

\textsuperscript{132} See \textit{Munoz}, 629 So.2d at 100.

\textsuperscript{133} See \textit{id.} at 99. The wording of the opinion, “in the absence of egregious law enforcement conduct,” makes it syntactically clear that this must be determined first. One cannot determine the presence or absence of a condition without first addressing the elements surrounding and comprising that condition.

\textsuperscript{134} 462 So.2d 1082 (Fla. 1985).

\textsuperscript{135} See \textit{id.} at 1085.

\textsuperscript{136} 425 U.S. 484 (1976).

\textsuperscript{137} See \textit{Glosson}, 462 So.2d at 1084.
Munoz entrapment jurisprudence. Glosson, however, fails to establish much more than a broad proposition, offering little guidance as to what constitutes a violation of due process.

In State v. Williams, the Glosson analysis again became pivotal. The Williams court overturned a criminal conviction citing due process violations and using the same reasoning as in Glosson. The Williams Court admitted that "[d]efining the limits of due process is difficult because 'due process,' unlike some legal rules, is not a technical conception with a fixed content unrelated to time, place and circumstances." The Court, expounding upon this, stated that "due process is a general principle of law that prohibits the government from obtaining convictions brought about by methods that offend a sense of justice." Applying these precepts, the Williams court specifically addressed the use of undercover "reverse-sting operations" and found them to be unequivocally permissible. The court accepted the proposition that the police may provide the defendant with controlled substances as part of the undercover operation.

Under the particular facts of Williams, however, the court found that the reverse-sting operation in question violated due process. The cogent condition seems to be the manufacture of the crack cocaine by the Broward Sheriff's Office. Absent this factor, it is likely the court would have held the police undercover-reverse-sting operation permissible. The salient premise that emerges is that police engaged in a criminal act cannot profit from their misconduct.

The Court's heavy reliance on the "canons of decency and fairness which express the notions of justice," combined with the analysis in Glosson, might provide guidance in future cases raised under due process theory in the context of online investigations.

As in most jurisprudential analysis into uncharted territory, one

---

138. 623 So.2d 462 (Fla. 1993).
139. Id. at 465. (quoting Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 162 (1951))(Frankfurter, J., concurring) (internal quotation marks omitted).
140. Williams, 623 So.2d at 465 (quoting Rochin v. California, 342 U.S. 165, 173 (1952) (internal quotation marks omitted).
141. See Williams, 623 So.2d at 465.
142. See id.
143. See id. at 466.
144. See id. at 464. The Court spent considerable time and effort in addressing the dangerous nature of crack cocaine, and that the Broward Sheriff's Office admittedly failed to recover all the crack in the reverse stings.
145. Id. at 465.
146. See Glosson, 462 So.2d at 1085. (The underlying principle seems to be the tremendous incentive to the informant to commit perjury and distort the true nature of the justice system. The nature of his conduct created an unacceptable risk that criminal activity would be created in the innocent, not intercepted in the predisposed. The court was unwilling to accept this.).
must apply existing canons of law to new, untested factual situations. Internet investigative police activity is most closely analogous to undercover police sting operations. The modality of these operations is indistinguishable from a narcotics sales operation or a prostitution sweep. Particularly, the street level approaches to both crimes, narcotics sales and prostitution, lends itself well to the analysis. From an objectivity point of view, therefore, the use of the virtual "street-corner" becomes simply another police sting operation. As clearly pointed out in Williams, police undercover operations do not shock the sense of justice. In cases arising from informant-based tips, the analysis follows the same reasoning as Glosson as it pertains to the due process issue. Provided the informant's conduct is not so ripe for the possibility of the creation of criminal conduct where none formerly existed, there seems to be a nominal opportunity for success in this posture.

One could, however, imagine a situation in which a defendant, involved in an organized ring of pedophiles and child pornography collectors becomes ensnared by police operations. Subsequently, he agrees to cooperate by providing introductions to co-conspirators, and arranges for an exchange of child pornography. In that scenario, the Glosson caveat must apply in a form no different from that addressed by narcotics investigators for years.

In the final analysis of the due process prong, it is foreseeable that a situation analogous to Williams may arise. During many investigations of child pornography and Internet solicitation the defendant asks for photos of the child with whom he believes he is conversing. The situation then presents itself much like the Williams polemic. While it is not disputed that the transmission of child pornography is illegal, there is a clear comparison between that activity and the provision, by law enforcement, of narcotics during undercover reverse-sting operations. The courts are clear. "[F]urnishing of a controlled substance by government agents in a reverse-sting operation [does] not constitute outrageous conduct. . . ."148

Unlike the child pornography statute, Florida Statutes section 893.13 (5)(c) excludes from prosecution law enforcement officials who deliver a controlled substance during the course of a bona fide law enforcement activity.149 The lack of a law enforcement exclusion in the child pornography statutes arguably makes the practice illegal.150 While this issue has yet to come before the Supreme Court of Florida, it seems

147. See Williams, 623 So.2d at 465.
148. Id.
149. See Fla. Stat. § 893.13(5)(c) (1997); see also Williams, 623 So.2d at 466.
150. See generally Fla. Stat. § 847.0135; see also Fla. Stat. § 847; Fla.Stat. § 827.
clear that the Williams reasoning may prevail. The inherent dangers of this conduct outweigh the ends to be reached.151 If a police undercover officer engaged in an on-line criminal investigation furnishes a defendant with some form of child pornography, he has crossed the boundary of egregious conduct established by Williams.152 Like Williams, he violated the due process clause of Florida's Constitution. Under current law, it is unclear whether criminal prosecution would be pursued in this case. If it were, it is fairly well established that under the foregoing analysis the court would find entrapment as a matter of law.

2. THE SUBJECTIVE APPROACH

From our analysis, it is not difficult to determine that the challenge to police "Internet solicitation" cases will rarely come under the due process theory of entrapment. Instead, the Munoz standard of subjective entrapment will likely be the approach taken by criminal defense attorneys seeking to attack the police operation. This subjective analysis becomes more difficult with the interjection of the inherent nuances of cyberspace conduct.

As indicated earlier, the Munoz court established a three-step test for subjective entrapment.153 Each step must be considered independently. The first issue is inducement.154 The typical scenario involves on-line contact between the undercover officer and the accused. The accused often initiates the contact based upon the suggestiveness of the officer's screen name or another alluring factor. In Munoz, a law enforcement agent initiated the contact.155 Clearly, Munoz bolsters the hypothesis that inducement is present where law enforcement initiates the contact. Likewise, in Jacobson, the government contacted the accused regarding his interest in pornography.156 A number of Florida appellate cases support this proposition.157

Disparity exists among the Florida District Courts of Appeal as to what constitutes inducement where the initial contact is not explicitly made by law enforcement. On one hand, the Third District failed to find

151. See generally 623 So.2d 462.
152. See Williams 623 So.2d at 467.
153. See Munoz v. State, 629 So.2d 90, 99-100.
154. See id. at 99 ("The first question to be addressed under the subjective test is whether an agent of the government induced the accused to commit the offense charged").
155. See id. at 101 (juvenile entered the video store and attempted to rent an X-rated video tape).
157. See Nadeau v. State, 683 So.2d 504 (Fla. 4th D.C.A. 1995) (informant contacted accused over 12 times to convince him to get involved); State v. Ramos, 632 So.2d 1078 (Fla. Dist. Ct. App. 1994) (informant contacted accused approximately 15 times to convince him to get involved).
inducement where police set up a decoy sting operation. On the other hand, the Second District found that police induced the accused by advertising the availability of pornography in the newspaper. The similarity of these cases is clear.

In Dawson, the police were aware of a problem with luggage thefts from the airport and established a decoy operation that provided circumstances conducive to lure a thief into action. In Beattie, the police established a decoy operation designed to lure a child pornographer into action. The only difference — the type of bait. In both scenarios the police clearly fished for defendants of a particular nature. Dawson was a thief, Beattie, a pedophile. Same game, different lures. The inapposite results cause consternation.

A powerful argument can be made that an undercover police officer's mere presence in a chat room of sexually explicit orientation constitutes no more than the mere opportunity to commit a crime. Notwithstanding, the analogy to Beattie, the mere presence of an undercover operative in a chat room feels unlike creative activity and more like mere opportunity.

Occasionally, police create their own chat room. Generally, this room bears a suggestive title and topic designed to attract persons predisposed to criminal activity of the nature advertised by the topic. In this situation, the analogy to Beattie becomes much more powerful. The distinction between mere opportunity and inducement becomes much more blurred.

In reality, this question poses few problems for law enforcement. The major question addressed in most entrapment arguments is that of predisposition. This defense may rise in significance with the increase in difficulty of proving predisposition in cyberspace. Given law enforcement's use of this investigative technique, the argument may be shifted, by the state, from that of having to prove predisposition, to proving that police investigative techniques did induce the defendant's conduct. If the state's conduct merely presents the opportunity, the defense of entrapment may be precluded without further need to show predisposition.

158. See State v. Dawson, 681 So.2d 1206 (Fla. 3d D.C.A. 1996) (holding that police placing a piece of luggage near pay phone, defendant picking it up and walking away is not inducement).
159. See Beattie v. State, 636 So.2d 744 (Fla. 2d D.C.A. 1993) (finding that police placement of newspaper advertisement constitutes inducement).
160. See Dawson, 681 So.2d at 1207.
161. See Beattie, 636 So.2d at 745.
162. See generally id.
164. See Munoz v. State, 629 So.2d 90, 99 (Fla. 1993).
If, however, the police conduct does connote inducement, then the second issue, and arguably the most controversial, is evaluated.\textsuperscript{165} Pre-disposition has been the object of controversy for years, even before the introduction of the new variable of cyberspace. In federal jurisprudence, the controlling case is \textit{Jacobson v. United States}.\textsuperscript{166} \textit{Jacobson} has become a key factor in Florida’s analysis through reference in the controlling decision of \textit{Munoz}. \textit{Munoz} established predisposition as the second stage of the three stage analysis in entrapment defenses.\textsuperscript{167} This stage places a large burden upon the prosecution to show that the defendant was predisposed to commit the crime.\textsuperscript{168} After a minimal initial showing of the lack of predisposition by the defendant, the state must rebut this negative beyond a reasonable doubt.\textsuperscript{169} This rebuttal stage poses the most threat to the state’s case.

Several authors addressing this question have called for stricter regulation of police conduct. For example, one author perceives the nature of police on-line conduct as “repeated inducement of online undercover agents.”\textsuperscript{170} While the author’s characterization of police conduct is clearly entrapment under \textit{Jacobson},\textsuperscript{171} it is the exception to the rule when dealing with most police investigation of this nature. Most investigations proceed along a path of prioritization. From initial contact through arrest, the investigating officer must constantly assess the probability of a successful meeting with the target. The expenditure of valuable resources to cajole a single target into committing an act of solicitation is poor management.

The more appropriate examination, under the predisposition test of \textit{Jacobson}, is what police conduct constitutes an appropriate use of resources. In \textit{Jacobson}, law enforcement directly targeted its conduct at Keith Jacobson.\textsuperscript{172} The police directly and repeatedly solicited him into the commission of the crime. Clearly, Jacobson had been targeted from the initial outset of the investigation based upon the appearance of his name on a mailing list.\textsuperscript{173} The Court relied on the premise that the government cannot “originate a criminal design, implant in an innocent person’s mind the disposition to commit a criminal act and then induce

\begin{itemize}
\item \textsuperscript{165} See id.
\item \textsuperscript{166} 503 U.S. 540 (1992).
\item \textsuperscript{167} See \textit{Munoz}, 629 So. 2d at 99.
\item \textsuperscript{168} See id.
\item \textsuperscript{169} See id.
\item \textsuperscript{170} Jennifer Gregg, \textit{Caught in the Web: Entrapment in Cyberspace}, 19 \textit{HASTINGS COMM. & ENT. L.J.} 157, 188 (1996).
\item \textsuperscript{171} See \textit{Jacobson}, 503 U.S. at 541 (repeated requests that defendant purchase child pornography held to be entrapment).
\item \textsuperscript{172} See id.
\item \textsuperscript{173} See id.
\end{itemize}
commission of the crime so that the Government may prosecute."\textsuperscript{174}

Justice White, writing for the majority, specifically condoned the provision, by police, of the opportunity to commit a criminal act.\textsuperscript{175} Pivotal in this argument is Justice White's statement that "the entrapment defense is of little use because the ready commission of the criminal act amply demonstrates the defendant's predisposition."\textsuperscript{176} The Florida Supreme Court copied and imbedded the premise and text of this argument in the \textit{Munoz} decision.\textsuperscript{177} It is quite clear that the predominant factor in establishing the entrapment defense under both lines of cases is the untoward solicitations by the government agents.

E. Application of Entrapment to Cyberspace

From here, we start our dissection of the Internet cases. By way of analogy, we must locate police investigative practices that closely resemble those which we wish to examine. As discussed earlier, the nature of the crime and the method used to detect it are similar to both narcotics and prostitution stings. Within these broad categories of police investigation exist more specific subcategories. Both types of crime are often the target of a police tactic known as a "reverse sting."\textsuperscript{178} Police direct these operations at the interdiction of street-level criminal activity. They are distinguished from other forms of narcotics and prostitution operations in that they have no specific target as the ultimate goal. The goal is, in effect, to reduce the ongoing criminal conduct occurring in specific areas. A police agency routinely institutes a sting operation upon receipt of complaints of specific criminal activity in a given locality.

Under this modality, the police establish decoy officers posing as either drug dealers or prostitutes awaiting customer traffic in the sweep area. These methods of operation, often criticized for putting legally seized narcotics back onto the street,\textsuperscript{179} frequently come under judicial scrutiny particularly on entrapment grounds.

Although this issue remains untested at the United States Supreme Court level, it has arisen at the appellate level of several states. Most closely analogous is \textit{State v. James}.\textsuperscript{180} In \textit{James}, the police set up a reverse-sting in a neighborhood known for criminal narcotics activity,

\begin{footnotes}

\textsuperscript{174} \textit{Id.} at 548 (quoting \textit{Sorrells v. United States}, 287 U.S. 435, 442 (1932)).
\textsuperscript{175} \textit{Id.} at 549-50.
\textsuperscript{176} \textit{Id.} at 550.
\textsuperscript{177} See \textit{Munoz}, 629 So.2d at 99-100.
\textsuperscript{180} 484 N.W.2d 799 (Minn. Ct. App. 1992).
\end{footnotes}
and sold cocaine through an undercover officer to defendant James. On appeal, the court addressed two issues: violation of due process by reverse-sting operations, and the predisposition of James. Like the situation in on-line chat rooms, where officers establish suggestive-sounding names and frequent explicitly named chat rooms, the officer in James assumed a role conducive to attracting persons predispose to commit the offense. He posed in an area and in a manner consistent with a genuine street level dealer. Likewise, in People v. Wesley, the undercover officer posed as a street-level drug dealer in an area known for high volume drug sales. In both situations unsolicited customers eventually approached the undercover officers and engaged in a narcotics transaction.

In addition to the due process analysis, the James court found that under Minnesota’s “subjective” test for entrapment the state could prove the defendant’s predisposition by his “active solicitation to commit the crime.” Pivotal in the court’s analysis was the fact that the defendant approached the undercover officer in an area known for cocaine sales, negotiated with the officer, and used appropriate jargon of the drug trade. Similarly, the Wesley, court found the defendant, predisposed based on his conduct during the initial officer contact, notwithstanding that the defendant was not the specific target of a criminal investigation.

From these cases it is clear that predisposition may be established circumstantially through the defendant’s conduct. Reading these cases in conjunction with Jacobson, it is possible to surmise that a distinction must be drawn between specific undercover activities directed at specific targets, and those directed at specific activities. As established in Jacobson, “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 defendant’s predisposition.” Clearly, if law enforcement has identified a specific area of criminal activity — in James, a house known for high volume drug sales — then reverse-sting activities are permissible uses of

181. See id. at 800.
182. See id. at 801-03.
184. See id. at 327 (officer carried a stereo prop and placed the cocaine rocks in a ziplock baggie).
185. See id. at 1136; see also James 484 N.W.2d at 800.
186. James, 484 N.W.2d at 803 (quoting State v. Grilli, 230 N.W.2d 445, 453 (Minn. 1975)).
187. See James, 484 N.W.2d at 803.
188. See Wesley, 274 Cal. Rptr. at 333. In Wesley the defendant also approached the undercover and made the initial solicitation.
police authority. Additionally, the conduct of the defendant immediately prior to initial contact, the manner of the contact, and the linguistics of the exchange are all factors considered to establish the predisposition of the accused to commit the crime. On-line solicitation cases must be examined like street-level reverse-stings because of their similarity in method of operation. Under this premise, it is clear that within the strict parameters referred above, activities such as entering a chat room under a suggestive name and awaiting contact by a potential molester are no different from the activities of the Minneapolis Police Department in James.

Unlike street-level narcotic sales, the on-line transaction is not an immediate one leading to instantaneous arrest. Rather, it is a more drawn out exchange, a cat and mouse type of seduction. Invariably, however, the first few moments of the exchange between the target and the undercover transpire in almost identical fashion. The target establishes the age of the undercover officer by asking for the age, sex, and location from which the officer is chatting. Thereafter, the conversation proceeds within the framework of any normal solicitation exchange, operating much as a solicitation for prostitution. By incorporating the decision in Jacobson, it is clear that the transaction or criminal solicitation need not be an immediate consequence of the target's initial approach. As Justice White stated, this premise could be applied to "a more elaborate 'sting' operation involving government-sponsored fencing . . . ."190 This statement clearly encompasses the context of a drawn out negotiation between the police and the accused where the accused makes the initial offer of sexual contact only after some extended small talk.

As stated earlier, there are critics of the use of undercover techniques to investigate these on-line solicitations. As part of the argument in support of stronger standards for Internet police conduct, one author postulates a scenario as follows.

For example, consider the situation where a suspected pedophile is engaging in "racy" but lawful speech and is approached by an undercover agent using a suggestive user name and profile. The agent makes "indecent" (illegal under the CDA) comments which induce the user to respond in kind, with the exchange culminating in a request for illegal material.191

While the existence of this of type exchange has undoubtedly been documented, it is a misperception of the true nature of police conduct on-line. I agree with the author that the above referenced exchange, if it

190. Id.
191. Gregg, supra note 170, at 188.
were to have occurred, would probably rise to the level of entrapment as a matter of law under Jacobson. The agent makes initial contact. It is a mistake to assume that police agents conduct themselves in a manner substantially different when on-line than when in person. If an undercover officer approaches a specific defendant and repeatedly solicits him for criminal activity, most police and prosecutors agree that the conduct is probably within the purview of Jacobson. Most real life cases simply do not unfold this way. In reality, the on-line cases are quite similar in inception to most street-level drug cases, with the added twist of anonymity.

The setting of cyberspace lends an added dimension to police undercover activities. Perhaps, given the difficulties inherent in this medium, the judicial system should reconsider the way in which we examine predisposition. I believe, unlike some, that predisposition still may be established through Internet contacts.

The nature of the human psyche is such that predisposition is not an on and off concept. A person's predisposition is most closely illustrated not by a light switch, with two positions — on and off — but by a continuum. On the left edge of the continuum there exists no predisposition to commit deviant sexual behavior. On the far right edge there exists an overwhelming predisposition to commit the deviant act. It is Dr. Marshall's theory that the mere presence in an on-line chat room, clearly orientated toward sexually explicit talk about sex with children, evidences a shift from the far left edge of the continuum toward the right. It is postulated that by the mere presence in that situation, those engaging in the on-line conduct have exhibited some predisposition toward the commission of those deviant acts. It naturally follows then that the further the subject involves himself, the greater his predisposition becomes.

For example, if the subject begins to participate in conversations with others who are engaged in pedophilic-type fantasy and role play, it can naturally be assumed that his predisposition to commit this type of offense has increased. While the offender's disposition may still be nothing more than fantasy in the abstract, it must be recognized that persons with no tendency toward deviant behavior would not find themselves in this position in the first place. The further the subject becomes enmeshed in this fantasy and experimentation, and the more overt the advances toward a child on-line become, the further to the right

193. See id.
on the continuum of predisposition the offender moves. At the far right of the continuum is the actual meeting between the offender and his victim. While it is not asserted that an offender’s criminal predisposition is directly equivalent to psychological predisposition toward deviant behavior, it is illustrative of the fact that the mere presence in a child-sex oriented chat room lends credibility to the standard in James, which considers the offender’s presence in a known crime area.

In Dr. Marshall’s experience, a person does not become pedophilic based upon child pornography fantasy and role play. A psychological predisposition within the subject generates this behavior. The unique nature of this crime must be distinguished from narcotics offenses and other types of crimes. Other types of crimes may be committed by anyone, given the proper inducement. Unlike other crimes, a deviant attraction to children precedes the action of soliciting a child on-line. From that logical assertion, it naturally follows that absent this deviant attraction a person could not be induced to solicit a child. In other crimes, such as theft, there need not be a deviant attraction for inducement sufficient to spur action. Sexually related crimes, however, by the nature of their deviant characteristics, theoretically will only be committed by persons of a deviant predisposition.

It therefore logically follows, that unless the subject is psychologically predisposed to commit this specific type of sex offense, the leap from on-line fantasy to in-person meetings is impossible. From a psychological standpoint, a person engaged in experimentation and fantasy would not generally be expected to carry out the deviant sexual act without the existence of the pedophilic disorder. The concerns expressed over the danger that innocent experimenters and role players will therefore become ensnared by police conduct become greatly reduced under that theory.

As recognized before, there is a difference between psychological predisposition and criminal predisposition. It is entirely possible, and even probable, that a person suffering from pedophilia may be fully psychologically predisposed to commit deviant acts on a child. It does not necessarily follow that he will allow this predisposition to override his desire to remain within the law. In drawing the above analogy, I am not advancing the argument that psychological predisposition should satisfy the criminal predisposition standard. Instead, the argument illustrates that by this type of examination, the concern over the fantasy and “big

194. See id.

195. But see generally Part I supra (concerning the current structure of § 847.0135 and the implications of punishing guilty thoughts).
talk" can be dealt with through a requirement for an overt act in the "real world."

As clearly outlined above, this analysis results in the recognition that police conduct on-line, if done in conjunction with proper "real world" police investigative techniques not unlike any other vice operation, can establish legal predisposition.

F. The Proposed Solution

Concern remains over the interaction between section 847.0135 (3), Florida Statute Stat. and those persons who are predisposed to deviant behavior but not predisposed to deviant criminal behavior. The creation under the Florida statute of "double-inchoate crimes" moves the point of criminal conduct well into the area of thoughts antecedent action. The legislature must repeal section 847.0135(3) Florida Statute and subsequently amend sections 800, 794, and 827, Florida Statutes, as they relate to sexual conduct with a child. If the desired result is enhanced punishment of sexual offenders who victimize children, the same net effect could be achieved through the addition of an enhancement provision within the substantive sections of the law.

Without argument, the legislation currently in effect protects children from sexual molestation. The characteristic that sets this statute apart from the substantive section is the modality with which it accomplishes this goal. It recognizes that a new frontier is being used to perpetrate these evils upon our children. The underlying crime, however, is no different: Sexual exploitation of a child, the crime has not changed, merely the modality. The creation of a new statute is not the most efficient or jurisprudentially the most effective means to achieve our goal.

This type of response to new perceptions of threat is not new. In 1979, the Florida Legislature passed the Florida Drug Abuse Prevention Act. In 1993, however, in response to the perceived, although real, danger to children from the sale of drugs in their proximity, it passed an amendment to the chapter. This amendment, did not create a brand new offense, it merely upgraded the already illegal conduct of drug sales to a higher grade felony when the sales occurred within proximity to a school.

In Internet cases, the government must prove an attempt of either

196. Gregg, supra note 170, at 187.
197. See discussion supra Section V (B) (concerning inappropriateness in Anglo-American law of punishing the equivalent of guilty thoughts).
199. 1993 FLA. LAWS § 93-406.
200. See id.
sexual battery upon a child, or attempted lewd acts with a child, or one of the other enumerated offenses. This being the case, the state can no longer rely solely upon the conduct on the Internet. It must wait for further "substantial steps." Clearly, this removes the danger of punishing guilty thoughts.

Under the proposed change, the state must await the defendant's overt act. For example, the defendant must arrive at the predetermined meeting place or another "substantial step" toward the commission of the crime. Making proof of the crime more removed from the planning stage, and more closely related to criminal conduct, assuages concerns expressed previously over the inability to abandon the crime once the first solicitation has been made.

In accordance with this proposed new format, the jury would presumably be instructed under the standard instructions concerning solicitation where the actor solicited the child, or person whom he believed to be a child, to commit some sexual act. In this case, the actor may still avail himself of the defense of abandonment. Conversely, the crime, as currently written, is the mere solicitation itself which connotes that once the words, or text, have been uttered, the crime is completed, and may be charged.

This jury instruction allows the defense if the actor otherwise prevented commission of the offense. Failure of the defendant to meet with the undercover agent constitutes just such a prevention.

Alternatively, section 847.0135 could be amended to require a specific overt act in furtherance of the crime. While some argue that the mere transmission of E-mail communications is an overt act, it does not have the same conceptual connotation as its real-world equivalent. Clearly, an actor who sends a telegram or letter to a co-conspirator imploring them to commit a substantive act takes an overt step necessary to create the fear that the crime will be further perpetrated. It is not altogether as clear, for the reasons stated earlier, that the cyberspace equivalent does the same thing. The addition, therefore, of the penultimate overt act of meeting with the child, or some equivalently "substantial step," assures that guilty thoughts remain unpunished and that guilty acts receive the full force and effect of our criminal laws.

VI. Conclusion

Colleagues often ask “Should we expend valuable, finite resources on this problem that is essentially the creation of crime where none existed?” The answer is most assuredly in the affirmative, but not without controversy. Society is determined to protect children. It recognizes, as evidenced by the plethora of legislation in that area, that children are unprepared, or ill-equipped, to protect themselves. When it becomes apparent, as it does from the literature on pedophilia and sexual abuse of children, that the danger is real and not perceived, then society must aggressively, punish those persons who perpetrate offenses against the helpless. This crime, sexual abuse of children, is such that prevention is the only efficacious solution. The mere reactive approach, a standard response to crimes of violence and theft, is inadequate and immoral in this framework. Inadequate in the fact that research is clear that numerous cases of child sexual abuse remain unreported, and immoral in that our duty as protectors of children militates an aggressive response to shield them from harmful, life-altering contacts.

The aggressive attack of Internet child sexual predation remains the antithesis of the aggressive attack on prostitution sometimes criticized as “legislation of morality.” Prostitution, while illegal, is unquestionably the commission of an act otherwise legal, and in some societies morally acceptable, with the interjection of a monetary exchange. Two consenting parties enter a business transaction. The abuse of a child by sexual contact, notwithstanding the arguments of pedophiles, cannot aspire to consensual behavior. It must be crushed at the very dawn of its existence, in this case, the solicitation of a child under the fortuitous occasion that it transpires in cyberspace.

The often articulated argument that police in this situation merely create crimes where none previously existed, has been attempted under all circumstances where aggressive, proactive police conduct ensnares unsuspecting criminals. It does not necessarily follow that because the police create the opportunity for an otherwise predisposed criminal to commit his crime that this is “creation” of crime.

In the case of child sexual abuse, this could not be more conspicuous. Both statistical and empirical data reflect the overwhelming fact that child sex offenders will offend. This cannot reasonably be disputed. It must then logically follow that police, posing as victims, will intercept the focus of this behavior before a child is victimized. In essence, for every police officer the child molester meets, there is one less real victim to be counseled. Because of the insidious nature of the offender and the cloak of secrecy within which he operates, there remains no alterna-
tive but the aggressive preemptive strike that is so effective when admin-
istered sensibly and within the confines of society's sense of justice.

Admittedly, the interjection of cyberspace into this equation adds a
facet of complexity not previously seen. This new frontier, however, is
not the bane of society. Problems exist. One such problem is addressed
here. The ethereal intangibility of the Internet creates a disconjunction
between what people perceive as actions and what they perceive as
thoughts. This disconjunction raises a multitude of questions with
which lawyers, scholars, and judges must inevitably struggle as technol-
gy speeds along with jurisprudential thought at its heels. It is simulta-
neously a treasure and a treachery. We must, however, reflect on
previous technological advances. Most were received amid the antitheti-
cal cries of obsequious sycophants and iconoclastic doomsayers. The
truth, however, often lay somewhere in the middle. As in the case of all
eyear technology, the Internet and cyberspace will suffer growing pains.
The growing pains bring with them a cacophony of criticism. As legal
frontiersmen in this vast ether of nothingness, we must balance our fear
of the unknown with our objective sense of right and wrong.

The issues addressed here are a mere splinter of the greater issues
to be addressed. The solution is imperfect. The coexistence of common-
sense and protection of our children, however, is not an unattainable
goal.

If we apply real world principles, such as overt acts and the ability
to abandon an attempt, to crimes occurring somewhere between the
realm of fantasy and action, we can intelligently apply precedent. The
pivotal question becomes at what point in cyberspace do thoughts and
actions merge. Is it the innocuous depression of the "send" button? Is it
that point in which our cyberactions are converted into real actions by
the voluntary execution of a physical act? I find the former much more
troubling than the latter. The combination of the former, Internet com-
munications such as E-mail and chat conversations, with a small amount
of the latter, an overt act done entirely in the real world, can rise to the
level of a "substantial step" and should be the overriding standard by
which our Internet activities are judged.

MICHAEL W. SHEETZ