



# Undercover Online: An Extension of Traditional Policing in the United States

Melissa J. Tetzlaff-Bemiller<sup>1</sup>

University of Central Florida, USA

## Abstract

*This study examines law enforcement personnel who work undercover chatting investigations in order to catch online sexual predators. Law enforcement efforts in this area are relatively new. This research addresses such questions as what types of training do these law enforcement personnel who try to snag online sexual predators go through and what specifically do their jobs entail. Seventeen law enforcement personnel were interviewed from different parts of the United States. The interview schedule covered six areas: respondents' careers, their home lives, training received that is relevant for their current positions, details about their jobs, the undercover aspects of their jobs, and their demographics. This study is important because it offers a closer look at the individuals who put their time and efforts into neutralizing online sexual predators before they can harm additional children and minors. This knowledge will add to the current literature in this area as well as aid policy developers on issues concerning law enforcement organization and personnel.*

---

Keywords: Sexual predators, internet, crime.

## Introduction

The virtual world has been increasingly impacting all aspects of interpersonal relationships. Computers are highly relevant in nearly all aspects of life and are frequently used to facilitate personal relationships. For example, there are many individuals who now use the internet to join online social networks, and even to establish romantic and/or sexual relationships. This is particularly the case with today's adolescents who use Facebook®, MySpace™, Twitter™, and the wide variety of network communities for socializing with hundreds, if not thousands, of others throughout the world. An estimated 14 million youth, ages 12–17 years, were using social networking sites (SNSs) in 2006 (Mitchell, Finkelhor, Jones, & Wolak, 2010).

The internet offers a world of anonymity which can have both positive and negative consequences. The internet provides individuals the ability to explore possible problems (physical, mental, sexual, and social, etc.) and gain the support of others in the privacy of their own home. In the same way, it also offers individuals the chance to explore interests that may or may not be approved of by society. Therefore, while the virtual social world brings many individuals satisfaction, there can be problematic social encounters. This may

---

<sup>1</sup> Department of Sociology, University of Central Florida, 4000 Central Florida Blvd, Howard Phillips Hall, rm. 403 Orlando, FL 32816, USA. E-mail: melissa@knights.ucf.edu

be especially true concerning youth because even though current preteens and teenagers are sophisticated in the use of technology, they are likely to be fairly unsophisticated when it comes to social relationships and virtual communities. As such, there may be many adolescents who can be easily duped by manipulative adults. These youth can readily be ensnared in a world where they become victims of older predators masquerading as the adolescent's peers (Walsh & Wolak, 2005; Young, 1997).

Increasingly, these individuals have come to the attention of law enforcement agencies that have developed task forces to catch online predators or, at a minimum, make it more difficult for them to prey on young people. These officers often will go online, join SNSs, sit in chat rooms, and pose as young teenagers in order to snag online sexual predators (Mitchell, Wolak, & Finkelhor, 2005a).

The focus of the present study is those individuals (referred to forthwith as law enforcement personnel [LEP]) who work to catch online sexual predators with the goal of examining their views about their jobs, their strategies for catching online predators, and their training. As such, this analysis seeks to describe the job of these LEP who work undercover online to try and make the internet a safer place.

### **Literature Review**

Research has found a link between sexual offending in the "real" world and solicitation for sex in the virtual world. Walsh and Wolak (2005) found that "more than a quarter of the online sexual predators had prior arrests for nonsexual offenses, and nine percent had prior arrests for sexual offenses against minors. Three percent of sexual assault defendants were registered sex offenders at the time of their crimes" (p. 264), and the majority of the defendants had met their victims on the internet.

These internet-initiated crimes followed a common pattern in which offenders met victims in chat rooms and developed relationships, which were often romantic or sexual, lasted a period of a month or longer, and involved communicating via chat rooms, e-mails, and instant messages (Walsh & Wolak, 2005). Grooming is a method that is used by online sexual predators to lure the children they meet. The grooming process has been described as a way of blurring the lines between appropriate and inappropriate behaviors (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006). This process gradually shifts material or contact that a child or adolescent considers inappropriate to something they accept (Young, 1997). The predator attempts to gain the affection, interest, and trust of the victim and is sometimes considered to be a friend or even a mentor to the young person (Conte, Wolf, & Smith, 1989; Young, 1997). Research has suggested that some children and adolescents are likely to find this attention appealing. They have a strong desire to form relationships; to belong; and to gain attention, validation, and acceptance (Baumeister & Leary, 1995), often because they are troubled in the "real" world. Young (1997) suggests that the process of normalizing sexual and inappropriate behaviors means that the victim is less likely to tell anyone, because they see the behavior as normal, and therefore the predator does not have to resort to threats to keep the victim quiet. This allows the predator to keep a friendly/mentoring relationship going. It is important to note that this entire process occurs online, taking advantage of its anonymity.

In order to catch these online predators, LEP must use similar strategies as those adopted by their targets. This means going undercover and using the internet as their investigative location. Undercover work involves a method where an investigator looks for criminal activity by inserting him or herself into the lives of people intent on engaging

in illegal behavior (Girodo, Deck, & Morrison, 2002). The investigator pretends to be someone else by falsifying his or her true identity and developing trust and acceptance by the targeted individual (Mitchell, Finkelhor, & Wolak, 2005b), almost as if they were grooming the predator.

Given the growth in and harm from online sexual victimization of youth, law enforcement agencies have developed special units as ways to try and stop online sexual predation before it reaches unsuspecting youth. Undercover investigations on the internet can be conducted in a variety of ways. These include having investigators pose online as minors, often called proactive investigations because the police may have an opportunity to capture suspects before a youth has been victimized; they may also pose online as mothers of young children who are seeking men to teach their children about sex. Undercover investigations also occur when police find out youth have been solicited by adults. These are often called reactive, or take-over, investigations since investigators go online, taking over the solicited youth's profile or posing as another youth, while still targeting the original suspect (Mitchell et al., 2005b). Another way LEP target offenders is by posing online as child pornography traders or sellers (Mitchell et al., 2005b).

Not much research has examined how these investigations are carried out. However, Mitchell et al. (2005b) found that most investigators posed as female adolescents with the majority posing as age 12 or older. Most investigators met their targets in chat rooms, through Internet Relay Chat, or through instant messages. Nearly half of all the investigations began in sex-oriented chat rooms. Multiple forms of online communication exist between targets and investigators; typically these communications were through chat rooms, instant messages, and e-mail. The length of time the investigator communicated with the targets was typically short, lasting one month or less in more than half of the cases and between one and six months prior to the arrest in about a third of the cases. The number of online interactions between the investigator and the target was usually 10 or less, however, in some cases the target was more demanding or weary, causing online interactions to increase to between 11 and 30 times.

Continuing, Mitchell et al. (2005b) found that proactive investigations typically began in chat rooms or through instant messaging and developed rather quickly. When compared with cases involving juvenile victims, investigators appeared to be using appropriate age identities, as well as both male and female identities. Those proactive investigations conducted through chat rooms tended to be clearly sexually oriented. This raises the possibility that more successful offenders (i.e., those who do not get caught) work outside of sex-oriented chat rooms. It is possible that police are catching naive offenders who have not developed the grooming techniques necessary for pursuing a relationship with a teenager in sex-oriented chat rooms (Mitchell et al., 2005b).

Another way law enforcement has attempted to combat the virtual world of online child solicitation is by using SNSs. Investigators typically had web pages or profiles on SNSs that were used by offenders to get information about the impersonated minors' likes and interests, and whereabouts at a specific time, and look at pictures of the impersonated minor (Mitchell et al., 2010).

## **The Present Study**

Specifically, there is only minimal research that addresses such questions as who are these LEP who try to snag online sexual predators, what kinds of training they go through, and what their jobs entail. Answering these questions is the intent of the present

study. In doing so, this investigation will contribute to the current literature on law enforcement responses to online sex predators by providing insight into how LEP engage in activities with individuals online while deciding whom to target or not. This research will also aid the literature by adding more descriptions and characteristics of the nature of the online job these LEP perform on a daily basis. This could help in formulating a broader picture of the techniques used by online predators, aiding in better training initiatives and on the job procedures.

## **Methodology**

### **Sample**

Telephone interviews were conducted with 17 individuals who are members of the special units that LEP use to catch online sexual predators. The sample comes from several states in the United States (Delaware, Florida, Idaho, Iowa, Kentucky, Maryland, New Mexico, Ohio, Oregon, Texas, Virginia, and Wyoming) and includes LEP from local, state, and federal agencies. Individuals were obtained through snowball sampling and the use of the list of task force agencies provided on the Internet Crimes Against Children (ICAC) Website. The researcher spent time working in a law enforcement environment and maintained contact with some coworkers. One of the previous coworkers supplied the researcher with a contact who was able to give the researcher more possible contacts who fit the criteria for inclusion in this research. The first individual interviewed then referred the researcher to the ICAC website where there is a list of Regional ICAC Task Force Agency Contacts in the United States. The researcher went down the list calling each agency asking to interview an individual who met the criteria for participation; the individual worked (currently) with a sex crime unit and his/her primary realm of enforcement was the virtual world.

### **Data**

The responses of the sample to the interview instrument comprise the data for this project.<sup>1</sup> Specifically, the interview schedule consists of forty questions that focus on six aspects of the LEP's life: individual, home life, training, details about the job, undercover aspects, and demographics.

The first part of the interview contains 12 broad questions with more detailed follow-ups when relevant and focuses on the respondent. During this part of the interview, individuals answered questions concerning their backgrounds, how they became part of their units, their schedules, and the agencies for which they work. The next part of the interview shifts the focus to the LEP's home lives. In this section, questions focus on relationship statuses, children, and social lives. This section contains five broad questions with more detailed follow-ups when relevant. The third section inquires about the LEP's training. In this section, there are two broad questions with more detailed follow-ups, when relevant, that focus on where or from whom they received their training, as well as the content of the training. The fourth section relates to the respondents' jobs. Questions here contain strategies used, sites patrolled, and how the respondents identify with their targets. There are 13 broad questions with more detailed follow-ups when relevant. The fifth section encompasses four broad questions with more detailed follow-ups when relevant about the undercover aspects of the LEP units and job tasks. The questions here solicit respondents' thoughts on whether or not they think their jobs are undercover, how

---

<sup>1</sup> This study was found to be exempt by the University of Central Florida's Internal Review Board.

their jobs relate to other undercover jobs, and if they consider their job to be risky. The interview concludes by asking demographic questions about their age, race/ethnicity, and gender.

### ***Data Analysis***

The interviews were conducted via telephone. Interviews were transcribed so as to better search, review, and highlight the respondents' answers. The researcher typed the answers the respondents gave during the interview and then cleaned up the typing afterwards. The interviews were then printed and read through, compared, and analyzed while looking for patterns and exceptions. The researcher highlighted responses to be used in this research and compiled the statistics manually. Also, the researcher made an Excel file that contains all of the respondents' answers to each question. As such, data analysis was qualitative, as patterns in responses were identified, highlighted, and discussed. In order to underscore some of the stronger or more important findings as well as to provide summary descriptions, the researcher used measures of central tendency and frequencies. For the purpose of this paper, the researcher is only focusing on three areas of the interview: the individuals training, details about the job, and demographics.

### **Findings**

The results of all the interviews provided some in-depth and highly interesting information about the jobs of LEP who go undercover in the virtual world in order to preemptively catch online sexual predators. The interviewed individuals were between the ages of 31 and 58. The average age of respondents was 43 years old. Fifteen were male and two were female. Sixteen respondents were Caucasian and one was Hispanic. Forthwith, when discussion notes, "all respondents," this means 100% of the respondents.

All of the individuals interviewed were part of units that employed proactive undercover chatting (UC) with sexual predators. However, they came to those positions from different sized agencies and backgrounds. All had some college education. The most commonly held degree was a Bachelor's degree (7); followed by a Master's degree (5). Even so, three did not complete a degree and two had an Associate's degree. All of the respondents had worked in law enforcement prior to their current assignment. The range of total years worked in law enforcement was from five to 29 with an average of 18.65 years in law enforcement. Ten of the respondents had volunteered for their current positions with the UC units. Among the seven respondents who did not volunteer, six were placed or promoted to that position and one accidentally fell into the position by being involved in a narcotics investigation that evolved into a sexual predator investigation.<sup>2</sup>

Fifteen of the individuals interviewed were married, but the length of the marriage varied from 3 months to 34 years, with the average length of marriage being 13.78 years. Two respondents were in relationships. Concerning other members of the respondents' families, all but one individual had children. The ages of the respondents' children varied from 19 months to 32 years old. And, respondents had from zero to five children, with

---

<sup>2</sup> His unit caught a dope dealer on Myspace™. He had been watching the television show, *To Catch a Predator*, and decided to make a profile of a 13 year old girl. It did not take long before he started catching people and decided to take it to the Attorney General. The Attorney General helped develop his new unit dedicated to catching sexual predators.

the average being 1.76 children. Table 1 provides information about each of the respondents.

Table 1. Characteristics of Respondents

Pseudonym	Gender	Age	Ethnicity	Education	Married	Years Married	Number Children	Children Ages (in years)	Years in Law Enforcement	How on Unit	State
John	Male	42	Caucasian	Masters	Yes	3	1	1.75	20	Promoted	ID
Sean	Male	44	Caucasian	Associates	Yes	.25	2	23 and 17	23	Accident	NM
Sally	Female	41	Caucasian	Bachelors	Yes	10	2	9 and 5	14	Volunteered	NM
Danny	Male	51	Caucasian	Bachelors	Yes	27	1	22	29	Volunteered	TX
Stephen	Male	51	Caucasian	Bachelors	No		2	14 and 11	29	Promoted	DE
Dean	Male	36	Caucasian	Some College	Yes	13	2	6 and 3	16	Volunteered	MD
Timothy	Male	35	Caucasian	Bachelors	Yes	12	2	8 and 6	12	Promoted	OH
Fred	Male	48	Caucasian	Masters	No		1	22	23	Promoted	FL
Chris	Male	53	Caucasian	Some College	Yes	10	5	32, 30, 26, 24 and 22	27	Volunteered	OR
Matt	Male	58	Caucasian	Masters	Yes	30	0		31	Volunteered	WY
Patrick	Male	33	Caucasian	Bachelors	Yes	3.5	1	2.5	7	Promoted	KY
Frank	Male	53	Caucasian	Some College	Yes	34	3	25, 17, and 11	23	Placed	VA
Chad	Male	31	Caucasian	Masters	Yes	4	1	2	5	Volunteered	KY
Tony	Male	36	Hispanic	Masters	Yes	18	1	5	16	Volunteered	FL
Susie	Female	42	Caucasian	Associates	Yes	11	3	8, 6, and 4	12	Volunteered	IA
Jim	Male	37	Caucasian	Bachelors	Yes	8	1	3	10	Volunteered	FL
Scott	Male	45	Caucasian	Bachelors	Yes	23	2	7 and 12	20	Volunteered	TX
Mean		43.29				13.78	1.86		18.65		

### Training

All respondents agreed that training was offered for this type of position; however, respondents felt that the training was weak in some areas and very expansive in others. Additionally, most training was a part of ICAC and offered in sessions at yearly conferences and throughout the year. To elaborate, respondents noted that ICAC offers training in many different areas, but there is more emphasis for some of these areas than others. For example, at the annual conference, there were numerous sessions on child pornography but not many on UC.

In all, respondents received many different types of training in conjunction with their assignments in the sex crimes units. The types of training that respondents received included: undercover chatting, techniques used by online sexual predators, strategies law enforcement can use to be more effective, internet sites, cyber investigation, undercover machines, forensics, search and seizures, interviews and interrogations, evidence, search warrants, guidelines, legalities, information technology, internet protocol (IP) addresses, operating systems, computer hardware, file structure, data recovery, and many more. Regarding the form that their training took, all of the respondents agreed that the training is face-to-face instruction. Further, within the face-to-face sessions, many (like undercover chatting) offer hands-on learning so the participants can see exactly how to log into different chat rooms or set up multiple profiles.

The length of time their training courses lasted varied. Some of the training sessions lasted a day, while other sessions lasted three or four days. The annual ICAC conference lasts a week or more. At the annual conference, there are training sessions on everything related to internet crimes against children and not just one specialized area like the two-day-long trainings. All respondents also mentioned that in addition to the ICAC training,

they learn on-the-job. Many of the respondents also kept up with technology and youth by training on their own. Nine respondents read court cases, research articles, past chats, and studies. Media was another area of focus. This is how LEP keep current on children's interest. One respondent mentioned that his unit has subscriptions to teen and preteen magazines.

The amount of training officers received was highly varied, with nine individuals agreeing that they attended some form of training monthly or bimonthly for an annual total of perhaps 100 hours. One, however, logged over 300 hours of training each year. Also, one respondent indicated that he had never had any formal training for chatting. This individual does go to the ICAC conferences and has received training on various topics related to the job, but has never received any training on chatting. The rest of the respondents stated that they received training ranging from "as needed" to "all the time."<sup>3</sup> All the individuals agreed that the training was helpful. Nevertheless, three respondents said that they found some aspects of training to be a hindrance. "Being away from home for as long as some (training) takes is the only hindrance," explained Patrick.<sup>4</sup> Stephen also mentioned that sometimes it can be too technical or the speakers don't teach enough. Other things mentioned were glitches in the systems when the teachers are teaching and that not everything goes according to plan.

### ***Details about the Job***

All of the individuals interviewed did more than just chatting. They all performed peer to peer (P2P)<sup>5</sup> investigations. Respondents were also involved in traveling cases—which is when the target travels to meet the undercover officer, thinking s/he is a child. Other job duties noted by all respondents involved investigating tips forwarded to them from the cyber tip line, and conducting reactive investigations—which is when they get a complaint, from a parent for example, that a person who is acting inappropriately has contacted a child. This type of investigation involves the undercover officer taking over the child's instant messaging name and talking to the suspect to learn that person's intentions. Child exploitation cases involving the internet in anyway are also part of the job. And, of course, all respondents noted that they had to complete hours of paperwork.

One respondent told a story about an online website. He said, "Two young girls had been reported for running away. One was fifteen and one was thirteen. The parents seemed very concerned and wanted to get them back. As the case developed, he found out that one of the girls was pregnant. This led to some investigation which is when they found that the father had been using the internet to pimp them out. She was impregnated from one of those guys that the dad made her have sex with. The parents wanted their daughters back so they could keep using them for income." P2P cases involve file sharing sites like Limewire®. One respondent said he gets thousands of images a day. Once somebody has these files and shares them, one can see what they have. He also claimed, "These people don't accidentally download child porn. If you go onto LimeWire and type in child porn, you are not going to get many hits. The subculture has acronyms they use

---

<sup>3</sup> The numbers of respondents answering each question may not always total 17. This is because some respondents answered single questions in multiple ways, and some respondents answered questions in unique ways that did not fit the pattern noted and discussed.

<sup>4</sup> All names have been changed.

<sup>5</sup> Peer to peer investigation is a type of investigation used to find individuals who are investing in child pornography.

and you won't know these acronyms unless you are one of us or one of them!" UC will sometimes lead to a traveling case. This is when the sexual predator will travel a distance to meet with someone they believe is a child. Sally explained that, "We often times use a decoy house, but sometimes we just meet them where they want, but we generally make them come to us. I have had guys travel four hours to meet me before. Often times they try to tell me, when they find out I am not 13, that they were just going to talk!" Another respondent has set up an undercover operation through Yahoo! Groups. He cleverly made a group and gave it a name that, again, only members of the subculture would understand. He made it so the group creator, himself, had to approve or deny entrance into the group. The only way to be allowed in was to send the creator three child pornography images. He claimed, "I had so many emails full of child porn. It was the easiest bust we have ever done because every email has an IP address attached. These guys are not the smartest!"

Concerning reactive cases, LEP will sometimes take over a child's screen name and keep chatting with the predator. Sometimes this is done on SNSs, chat rooms, games, or many other places. Often times, they have to pose as moms and dads trying to solicit their son or daughter out, or as moms or dads who are talking to somebody who is attempting to allow them to have sex with their child. A respondent stated, "You know, I am not always a child. I would say about 30% of the time I am posing as an adult. It kind of makes it easier, but it is more aggravating. Children are naïve; adults generally know what they are doing!"

Nevertheless, one of the aspects of the respondents' jobs entailed online chatting to search out potential sexual predators. The most common strategies for UC was entering a chat room and waiting for someone to instant message them and maintaining a large online presence through multiple internet sites. Since all respondents were assuming the identity(ies) of adolescents, keeping their covers believable and intact required the use of technology as well as knowledge of the current youth culture. They all used pictures to keep their online images real. Since these pictures had to be from individuals who worked in law enforcement, they could only use pictures that had been age regressed or pictures from the officer's youth. They all used chat acronyms (lol-laugh out loud, rofl-rolling on the floor laughing, brb-be right back, etc.), misspelled words, and incorrect grammar (not capitalizing every word that should be capitalized and not using proper punctuation) in order to appear more youthful.

Additionally, due to the fact that most (15) of the respondents were male and portrayed female youth, the majority did not contact sexual predators by the phone, however, when they felt they had to talk to their targets, they used female coworkers to do the actual talking to the sexual predator on the phone. Only two individuals had used webcams to make contact with their suspects. These two were male. One accomplished this by putting duct tape over the lens and telling the person he was chatting with that the feed was showing up on his computer so it must be their computer that had a problem. The other respondent explained that he uses scotch tape over the lens to blur everything out. But, all respondents agreed that they would accept the invitation to watch a webcam. This way they could have a picture which most often makes their case against the perpetrator stronger. An email was also something many wanted because emails come with IP addresses. Although the respondents all agreed that chat rooms were where they spent most of their time, they also patrolled SNSs and other areas on the internet. As examples, one individual set up a group in Yahoo® Groups to catch child pornography traders,

another went into gaming sites like Second Life®, and a third went into Craigslist®. When reactive investigations come up, often times a gaming site (World of Warcraft®) or gaming platform (XBOX™) would be used.

Fourteen respondents agreed that it does not take multiple times of communicating to figure out if the person they are talking to is a sexual predator or not. For example, John said, “They are very direct with what they want.” Chris echoed this, “They will bring up sex within the first few lines or at least in the first 10 minutes.” Chad agreed that, “If they continue to talk with me after they know my age; I need to keep an eye on them and continue chatting.” Two respondents agreed that it depends on the individual. Still, one respondent exclaimed “Sometimes the relationship has to develop a bit so they believe you are real.” How respondents knew they were talking to a sexual predator was more defined, eight said it was how they talked and the questions they asked (a/s/l-age, sex, location; have you ever had sex, did you enjoy it, etc.), and nine expressed that they know they need to keep talking when the guy knows their “age” and keeps talking. Communication was facilitated through multiple methods. The most common (11 respondents) was through chat, followed by email, texting, phone calls, SNSs, and webcams.

While there was a vast disagreement on what strategy was most effective, all but five respondents said the various strategies were all at least somewhat effective. One respondent noted an exception to this, however. His agency attempted an undercover proactive investigation in Second Life®. Second Life® is a virtual environment where people are able to make an avatar—a digital copy of oneself to reflect whatever physical traits one wishes to have—that lives in a world where there are few rules or norms. In this investigation, officers made avatars and tried to identify possible sexual predators. The respondent felt that this particular investigation/strategy was ineffective because it took too long, used too many resources, and was not as effective as simply locating online sexual predators via chatting sites. Other strategies given that were not as effective were: portraying a boy is not as effective as portraying a girl, portraying an individual that you are not familiar with (one needs to know information about the individual’s life they are portraying—know the school you tell the person you go to), being too aggressive with the conversation, and using SNSs to catch sexual predators (they are good bolsters that are used to reinforce your identity, but they are not good to use alone in order to catch a predator).

Among all respondents, the average percentage of arrests that were made after individuals became targets was between 90%–95%. This was most likely due to the fact that the target had crossed the line at one point or another during their conversation with an undercover law enforcement officer. This, then, permitted law enforcement to start a more official investigation to find out more on the individual via subpoenas and/or background checks. In order to be this successful in their investigations, all respondents agreed that they had to adhere to the guidelines set forth by ICAC. All respondents also mentioned that they must, at all costs, avoid entrapment and enticement.

The legalities of investigations are crucial to the way that law enforcement officers were able to work online undercover. Officers are not allowed to initiate the first conversation with any person, but they are allowed to initiate any subsequent conversations (thus avoiding entrapment). Law enforcement officers are also not allowed to initiate any sexual talk or relationship talk, but they are allowed to respond to it if the person they are chatting with brings it up first (thus avoiding enticement). There are also state laws that

the LEP must follow, as well as ICAC guidelines. A general rule that was mentioned from eight respondents is that one cannot portray a child negatively. Regarding general strategies then, all respondents agreed that they did not target anyone in particular in their investigations; rather they waited for online individuals to engage them. When this happened, the officers paid attention to any signs that an individual showed of potential sexual predation. Here, only at the point the officers began chatting with individuals that they suspected may be sexual predators did those persons become targets. When they had strong evidence that any particular target was indeed a sexual predator, they generally ended up arresting that person. However, in some cases the target avoided arrest because they stopped communication and “virtually” disappeared.

Regarding the amount of time it took to catch a sexual predator, all respondents explained that it was completely dependent upon the individual predator. Patrick explained, “It depends on how quickly they feel like they can trust that you are not a cop.” Stephen agreed with, “It depends on the individual and how you click with him.” While the most common response given by eight respondents was one day (one day was used in conjunction with another time period, giving a time period that it might take to catch an online sexual predator), the time ranged from four hours to two years. Danny stated, “There is no good answer for how long it takes to catch one of these guys, it takes as long or as short as it takes. A case is built upon obtaining evidence within the guidelines of the law and it can happen within a day or weeks.”

Most of the respondents (14) explained that the grooming process can be relatively short or nonexistent. Most often, if there is a grooming process at all, it lasts for only a short time (5 minutes or so). If the case is leaning more towards traveling, the chatting usually lasts over a longer time period, and the grooming process is a bit more substantial, but even then there was not much of a grooming method employed. The number of predators caught by each unit was also completely divergent. The respondents all gave various answers that ranged from one to two predators per month to 15 to 20 predators a month. Others respondent gave rates for the year and said four predators per year all the way up to 150+ predators per year.

In the end, the respondents all agreed that online sexual predators are all over the internet; wherever children are, they are. They also all said they wish they had more resources and could catch all of them that they do not have time to go after or find.

## **Discussion and Conclusion**

These interviews provided a wealth of information about the LEP who go undercover in the virtual world and try to snag sexual predators before they can harm children. These respondents were LEP who at the time of the interview were part of a unit that went online to catch sexual predators. They discussed many issues relating to their jobs, what types of training they went through, and what job characteristics help to make them more successful at catching sexual predators online.

Concerning training, it was agreed by all respondents that ICAC offers many training opportunities throughout the year, as well as at its annual conference. In general, this training is helpful, but the amount of training any individual officer received varied. Not only did the amount vary, but also the type of training the LEP received varied. Many types of training sessions were offered for the LEP, but they were not required to attend all of these. It is interesting and practical that many LEP did day-to-day training on the job by keeping current on the latest youth trends.

Law enforcement officers also provided some details about their jobs and offered certain strategies that they typically employed in their efforts. They emphasized the speed at which they realized they were communicating with a potential sexual predator and gave the impression that grooming may not be as common as some previous research has found. This finding is particularly interesting since previous literature has discussed the process of grooming from the perspective of the undercover officer as well as the sexual predator. Here, these respondents basically said that grooming really does not happen, or, if it does, it is very short. It may be that there is a difference in grooming strategy based on whether or not the sexual offender knows his target. Many of these officers were investigating sexual predators using a more proactive strategy. In these cases, then, they would be more likely to catch predators who were strangers to their victims. Previous literature (Young, 1997) has noted that predators that are family members or acquaintances to their victims are likely to use grooming as a way to make their actions seem more appropriate, thereby minimizing the possibility that their victims will tell another adult.

All LEP agreed that UC was not their only job and that they had to perform many other tasks. There was not a clear cut time frame for how long it took to catch an online sexual predator, but all agreed that it involved collecting the evidence and following the guidelines. The number of sexual predators caught was highly varied among respondents.

### **Implications**

This research has shown that the training for LEP targeting sexual predators is not consistent across all units or agencies regarding the content or frequency. It may be beneficial if there were requirements in place that required individuals to receive a certain amount of training over the same content per year. That way, all agents could be up to date on any legal changes or precedents, predators' techniques, computer technology, and knowledge of youth culture. For example, agents could learn new ways to use webcams and to avoid enticement. One respondent mentioned that he will often times use his webcam by placing scotch tape over the lens to make the image come across blurred. Once, when he did this, the perpetrator asked him to place the webcam between his legs and touch himself. The officer moved the webcam to show his fingers, which to the perpetrator resembled a pair of legs. He then moved the webcam and his fingers to make it look like there was movement. This may or may not be misconstrued as enticement if a case such as this goes to court and it would be less risky (for the successful prosecution of a case) if all agents received training about which actions they can legally take and which they cannot. Also, of course, youth culture is ever changing, and with the continual advent of new technology, agents could receive annual training in the newest fads and "computer speak" that has emerged in youth culture.

### **Limitations**

This study was conducted with interviews of 17 individuals from across the United States. Seventeen individuals are by no means representative of the LEP who work on internet sex crimes units. Also, the demographics appear to be unrepresentative of law enforcement in general i.e., there were 15 males and 16 Caucasians out of 17 individuals in this study. The sample is clearly non representative on both gender and race/ethnicity. The individuals also were all associated with ICAC. It is not known to the researcher if there are LEP operating these types of investigations outside of ICAC, but since ICAC offers the training and has guidelines, the sample tended to have similar responses in some

areas. Similar responses could also be a product of snowball sampling (people who know each other tend to have similar situations and views). Also, the interview ended up being quite lengthy, often times taking two or more hours. This may have caused law enforcement to not answer questions as thoroughly by the end of the interview as they did at the beginning. A lot of the questions the researcher wanted to focus on were towards the back-end of the interview, causing the researcher to constantly have to probe for more answers, where at the beginning of the interview the LEP would just talk about a question for a lengthy amount of time and give very thorough responses.

### **Future Research**

Future researchers on this topic need to obtain more representative and larger sample from law enforcement agencies and possibly go outside of ICAC. It would be beneficial to focus on the grooming process that previous research has discussed but that the current research found to be nonexistent or much briefer in duration. Lastly, training would be another area of focus for future researchers, as clearly there is a wide range in the amount of training received as well as the content covered. Nonetheless, this study has provided a fruitful description of the world of the virtual undercover law enforcement agent targeting sexual predators.

### **Acknowledgement**

*I would like to acknowledge and thank Dr. Elizabeth Mustaine, Dr. Jay Corzine, and Dr. Jana Jasinski for their comments on earlier drafts of this article.*

### **References**

- Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin*, *117*, 497-529.
- Conte, J. R., Wolf, S., & Smith, T. (1989). What sexual offenders tell us about prevention strategies. *Child Abuse & Neglect*, *13*, 293-301.
- Fleming, M. J., Greentree S., Cocotti-Muller, D., Elias, K. A. & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth Society*, *38*, 135-155.
- Girodo, M., Deck, T., & Morrison, M. (2002). Dissociative-type identity disturbances in undercover agents: Socio-cognitive factors behind false-identity appearances and reenactments. *Social Behavior and Personality*, *30*, 631-644.
- Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Use of social networking sites in online sex crimes against minors: An examination of national incidence and, means of utilization. *Journal of Adolescent Health*, 1-8.
- Mitchell, K. J., Finkelhor, D. & Wolak, J. (2005a). The internet and family and acquaintance sexual abuse. *Child Maltreat*, *10*, 49- 60.
- Mitchell, K. J., Wolak, J.& Finkelhor, D. (2005b). Police posing as juveniles online to catch sex offenders: Is it working? *Sex Abuse*, *17*, 241-267.
- Walsh, W. A. & Wolak J. (2005). Nonforcible internet-related sex crimes with adolescent victims: Prosecution issues and outcomes. *Child Maltreat*, *10*, 260-271.
- Young, S. (1997). The use of normalization as a strategy in the sexual exploitation of children by adult offenders. *The Canadian Journal of Human Sexuality*, *6*, 285-296.