March 2003
Volume 72
Number 3

**United States
Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001**

**Robert S. Mueller III
Director**

Contributors' opinions and statements should not be considered an endorsement by the FBI for any policy, program, or service.

The attorney general has determined that the publication of this periodical is necessary in the transaction of the public business required by law. Use of funds for printing this periodical has been approved by the director of the Office of Management and Budget.

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535-0001. Periodicals postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

Editor
John E. Ott

Associate Editors
Cynthia L. Lewis
David W. MacWha
Bunny S. Morris

Art Director
Denise Bennett Smith

Assistant Art Director
Stephanie L. Lowe

Staff Assistant
Linda W. Szumilo

This publication is produced by members of the Law Enforcement Communication Unit, Training Division.

Internet Address
leb@fbiacademy.edu

Send article submissions to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

FBI Law Enforcement Bulletin

Features

The Seven-Stage Hate Model
By John R. Schafer, M.A. and Joe Navarro, M.A.
1
Investigators must understand the hate process to deal successfully with hate groups.

A Study on Cyberstalking
By Robert D'Ovidio, M.S. and James Doyle
10
To successfully investigate cyberstalking cases, law enforcement must understand how offenders use the Internet to stalk victims.

Best Practices of a Hate/Bias Crime Investigation
By Walter Bouman
21
Rendering hate/bias crimes the special attention they deserve will help law enforcement agencies treat victims, relate to communities, and prosecute offenders.

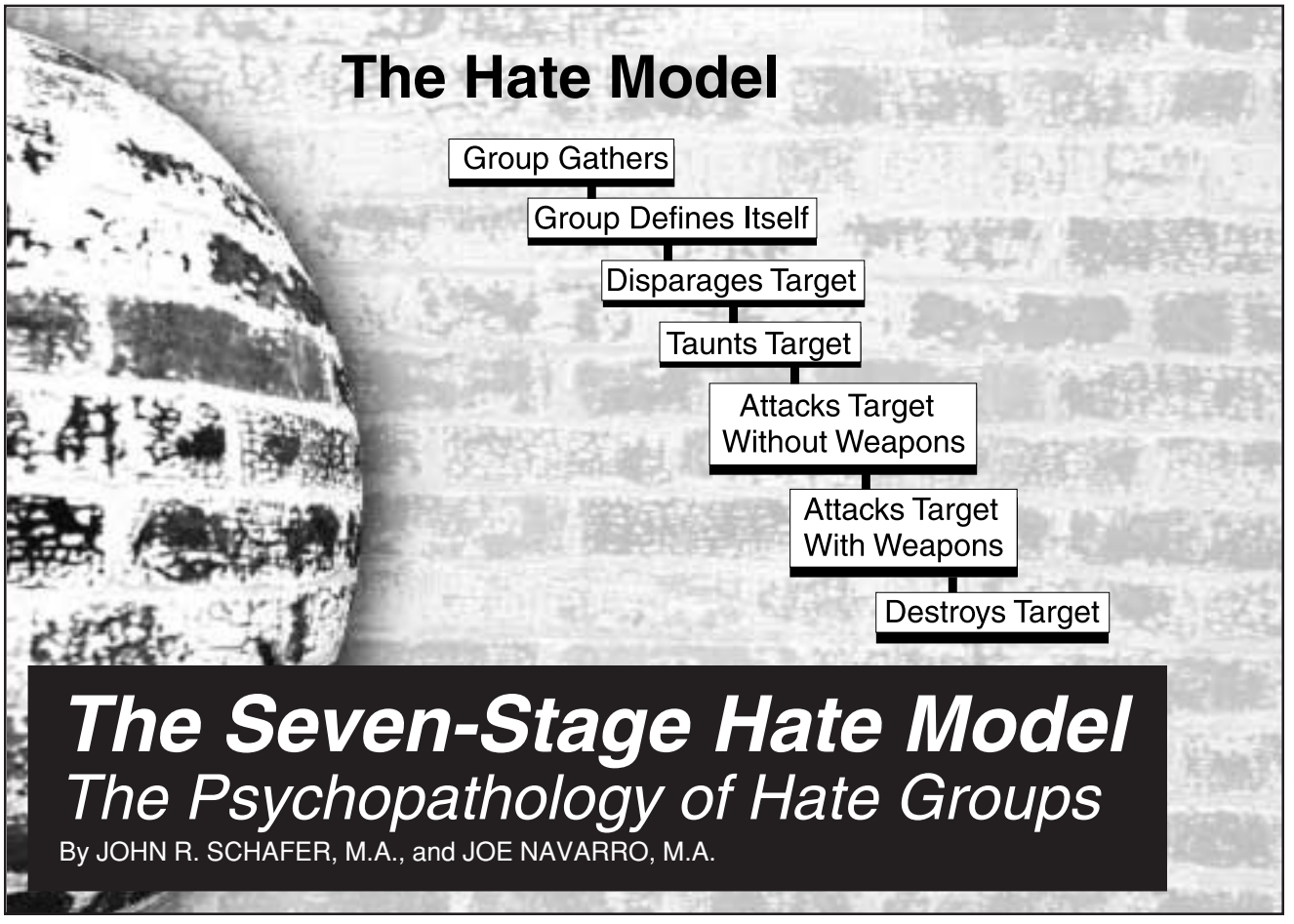
Obtaining Written Consent to Search
By Jayme Walker Holcomb, J.D.
26
Courts analyze a number of significant issues regarding written consent searches.

Departments

9 **Bulletin Reports**
Web-Based Resources
Law Enforcement

18 **Police Practice**
Recruitment Strategies

ISSN 0014-5688 USPS 383-310



The Seven-Stage Hate Model

The Psychopathology of Hate Groups

By JOHN R. SCHAFER, M.A., and JOE NAVARRO, M.A.

The manifestations of hate are legion, but the hate process itself remains elusive. Limited research in this field precluded the development of a comprehensive hate model. Understanding hate groups is essential for the development and implementation of successful intervention strategies, which depend on an understanding of the hate process. The proposed hate model consists of seven stages, including how hate groups define themselves, how hate groups target their victims and taunt them with verbal insults and offensive gestures, and how hate groups attack their victims with or without weapons.[1]

DEFINITION OF HATE

Hate, a complex subject, divides into two general categories: rational and irrational. Unjust acts inspire rational hate. Hatred of a person based on race, religion, sexual orientation, ethnicity, or national origin constitutes irrational hate.

Both rational and irrational hate mask personal insecurities. Everyone experiences personal insecurities in varying degrees throughout their lives. The more insecure a person feels, the larger the hate mask. Most people concentrate on the important issues in life, such as earning a living, rearing a family, and achieving personal goals. These pursuits give meaning and value to life.[2] Nonetheless, irrational hate bleeds through day-to-day activities in the form of racial barbs and ethnic humor. Not all insecure people are haters, but all haters are insecure people.

With respect to rational hate, haters do not focus as much on the wrong done to them or others, but, rather, on their own helplessness, guilt, or inability to effect change. The object of rational hate often is despised or pitied.[3] In the same way, irrational hate elevates the hater above the hated.[4] Many insecure people feel a sense of self-worth by relegating a person or group of people to a lower status.[5]

Special Agent Schafer is assigned to the FBI's Lancaster, California, resident office and also serves as a member of the FBI's National Security Division's Behavioral Analysis Program.

Special Agent Navarro serves in the FBI's Tampa, Florida, office and also is a member of the FBI's National Security Division's Behavioral Analysis Program.

SKINHEAD GROUPS

During a 7-year FBI investigation of skinhead groups in Southern California between 1992 and 1999, specific patterns emerged. Skinhead groups typically consist of uneducated, young, white males between the ages of 13 and 24 who have no long-term prospects for success. Although many come from single-parent, dysfunctional families, some exceptions exist. For example, members of the Western Hammerskins in Hemet, California, had high school educations and came from two-parent, middle-class families. Further examination revealed that both parents made long, daily commutes to work in Los Angeles and left their teenage children unsupervised. The lack of parental supervision and guidance spawned personal insecurities similar to those found in skinheads who come from dysfunctional, single-parent environments.

Fortunately, most skinhead groups are not well organized and lack the leadership structure found in the majority of street gangs engaged in "for-profit" criminal activities. However, the Western Hammerskins group has a stronger leadership hierarchy than most skinhead groups, and it boasts a very active recruitment program. Potential members receive a recruitment package, which includes a swastika armband, a T-shirt with white supremacist slogans, white supremacist literature and band stickers, and other supremacist materials. Recruiters also pass out business cards embossed with the Western Hammerskins' logo and the recruiter's name and telephone number. The group's higher educational level may explain the sophistication of its recruitment techniques.

Skinhead groups subdivide into two categories: criminally motivated and hate motivated. Criminally motivated skinhead groups spend most of their time engaged in for-profit criminal activities, such as drug sales and burglaries. Incidental to their criminal activity, they commit hate crimes. The San Fernando Valley Peckerwoods (SVP) in California was a criminally motivated skinhead group. SVP members primarily sold methamphetamines and committed residential burglaries. Periodically, SVP members attacked minorities with weapons and, on one occasion, placed packages resembling bombs near an apartment complex where African-Americans lived. Members intended for the fake bombs to frighten current residents to relocate and to discourage other African-American families from moving into the complex.

Conversely, hate-motivated skinhead groups dedicate the majority of their time to hate crimes.[6] Incidental to hate crimes, these hard-core skinheads commit petty thefts or sell small amounts of narcotics to support daily needs, such as food, cigarettes, and alcohol and other drugs. The Nazi Low Riders (NLR) skinhead group located in Lancaster, California, exemplifies a hate-motivated skinhead group. At one time, NLR members spent their time prowling the streets of Lancaster looking for minorities to attack. The NLR matured to the point where their members routinely beat and stabbed minorities, and, in one instance, murdered an African-American.

Haters cannot stop hating without exposing their personal insecurities. For example, at the onset of the FBI investigation, FBI authorities told hard-core members of the NLR that they would arrest them if their hate violence continued; yet, the hate violence persisted. The FBI

similarly warned the members of the SVP who, however, stopped or were more surreptitious concerning criminal activities, and their hate violence ceased. The reaction of the SVP members comported with general criminal deterrence literature.[7] The reaction of the NLR members did not, however, because hate, not criminal acts, was their primary motive.

Interviews of both criminally motivated and hate-motivated skinheads may explain this phenomenon. Criminally motivated skinheads identified themselves as criminals first and haters second. They also expressed a degree of personal security in their status as criminals. The criminally motivated skinheads possess a certain sense of self-worth; hence, they have fewer insecurities. However, this was not the case with hate-motivated skinheads. The explanation by one 15-year-old NLR member typified the thought process of hate-motivated skinheads. He said, in effect, "I dropped out of school in the eighth grade, but I stopped learning midway through the sixth grade. I covered my body with hate tattoos. I couldn't get a good job if I wanted to. No one would hire me. Once, I tried to get a job at a fast food restaurant, but the manager refused to hire me because the restaurant served multiracial customers. If I quit being a skinhead, I have nothing. I am nothing. I have no choice but to be a skinhead. I expect to die a young, violent death."

Skinheads converge, get drunk, take drugs, and, at some point, spontaneously seek out hate targets to attack. They conduct little, if any, planning before committing hate crimes. One hate-motivated skinhead put it best when he stated, "We don't look for trouble but somehow trouble always finds us, and we're ready to deal with it when it comes."

THE HATE MODEL

Several academic authorities on hate crimes in America identified three types of bias crime offenders: the thrill seeker, the reactive offender, and the hard-core offender.[8] They described the reactive offender as one "who grounds his attack on a perceived transgression, such as an insult, interracial dating, or a neighborhood integration."[9] The authors' model incorporates the thrill seeker and the hard-core offender, but redefines the concept of the reactive offender. This phenomenon can be described as secondary justification; skinheads routinely use this technique to instigate attacks. For example, a group of skinheads encounter a mixed-race couple and shout racial slurs. If the couple reacts in a manner other than a submissive one, the skinheads perceive that behavior as an act of aggression. The skinheads later tell the police they merely defended themselves against aggressors. The skinheads, of course, leave out the fact that they acted as the instigators. Secondary justification is difficult to detect because skinheads can interpret a simple glance as aggressive behavior.

> ***Skinhead groups subdivide into two categories....***

Secondary justification also exists on a larger scale. When a community reacts to a hate crime, skinheads perceive that reaction as aggressive, which reinforces the notion that skinheads must defend themselves against a common enemy. Secondary justification places the skinheads in a victim status and rationalizes continued violence. To further illustrate this principle, a skinhead, with a swastika tattooed on his cheek, walked into a jewelry store to buy a ring for his girlfriend. The skinhead became incensed when the Jewish clerk treated him poorly. The skinhead later commented that if Jews treated him with more respect he would not hate them so much. The skinhead clearly saw himself as a victim, although he openly displayed a provocative symbol of hate on his face.

Empirical observations show that hate groups go through seven stages in the hate process. Haters, if unimpeded, pass through these seven successive stages without skipping a stage. In the first four stages, haters vocalize their beliefs. In the last three stages, haters act on their beliefs. A transition period exists between vocalization and acting out. In this transition period, violence separates hard-core haters from rhetorical haters.

Stage 1: The Haters Gather

Irrational haters seldom hate alone.[10] They feel compelled, almost driven, to entreat others to hate as they do. Peer validation

bolsters a sense of self-worth and, at the same time, prevents introspection, which reveals personal insecurities.[11] Further, individuals otherwise ineffective become empowered when they join groups, which also provide anonymity and diminished accountability.

Stage 2: The Hate Group Defines Itself

Hate groups form identities through symbols, rituals, and mythologies, which enhance the members' status and, at the same time, degrade the object of their hate. For example, skinhead groups may adopt the swastika, the iron cross, the Confederate flag, and other supremacist symbols. Group-specific symbols or clothing often differentiate hate groups. Group rituals, such as hand signals and secret greetings, further fortify members. Hate groups, especially skinhead groups, usually incorporate some form of self-sacrifice, which allows haters to willingly jeopardize their well-being for the greater good of the cause. Giving one's life to a cause provides the ultimate sense of value and worth to life.[12] Skinheads often see themselves as soldiers in a race war.

Stage 3: The Hate Group Disparages the Target

Hate is the glue that binds haters to one another and to a common cause.[13] By verbally debasing the object of their hate, haters enhance their self-image, as well as their group status. In skinhead groups, racist song lyrics and hate literature provide an environment wherein hate flourishes. In fact, researchers have found that the life span of aggressive impulses increases with ideation.[14] In other words, the more often a person thinks about aggression, the greater the chance for aggressive behavior to occur. Thus, after constant verbal denigration, haters progress to the next more acrimonious stage.

Stage 4: The Hate Group Taunts the Target

Hate, by its nature, changes incrementally. Time cools the fire of hate, thus forcing the hater to look inward. To avoid introspection, haters use ever-increasing degrees of rhetoric and violence to maintain high levels of agitation. Taunts and offensive gestures serve this purpose. In this stage, skinheads typically shout racial slurs from moving cars or from afar. Nazi salutes and other hand signals often accompany racial epithets. Racist graffiti also begins to appear in areas where skinheads loiter. Most skinhead groups claim turf proximate to the neighborhoods in which they live. One study indicated that a majority of hate crimes occur when the hate target migrates through the hate group's turf.[15]

> ***"Empirical observations show that hate groups go through seven stages in the hate process."***

Stage 5: The Hate Group Attacks the Target Without Weapons

This stage is critical because it differentiates vocally abusive haters from physically abusive ones. In this stage, hate groups become more aggressive, prowling their turf seeking vulnerable targets. Violence coalesces hate groups and further isolates them from mainstream society. Skinheads, almost without exception, attack in groups and target single victims. Research has shown that bias crimes are twice as likely to cause injury and four times as likely to result in hospitalization as compared to nonbias crimes.[16]

In addition to physical violence, the element of thrill seeking is introduced in Stage 5. Two experts found that 60 percent of hate offenders were "thrill seekers."[17] The adrenaline "high" intoxicates the attackers. The initial adrenaline surge lasts for several minutes; however, the effects of adrenaline keep the body in a state of heightened alert for up to several days.[18] Each successive anger-provoking thought or action builds on residual adrenaline and triggers a more violent response than the one that originally initiated the sequence.[19] Anger builds on anger. The adrenaline high combined with hate becomes a deadly combination. Hard-core skinheads keep themselves at a level where the slightest provocation triggers aggression.

Stage 6: The Hate Group Attacks the Target with Weapons

Several studies confirm that a large number of bias attacks involve weapons.[20] Some attackers

use firearms to commit hate crimes, but skinheads prefer weapons, such as broken bottles, baseball bats, blunt objects, screwdrivers, and belt buckles. These types of weapons require the attacker to be close to the victim, which further demonstrates the depth of personal anger. Attackers can discharge firearms at a distance, thus precluding personal contact. Close-in onslaughts require the assailants to see their victims eye-to-eye and to become bloodied during the assault. Hands-on violence allows skinheads to express their hate in a way a gun cannot. Personal contact empowers and fulfills a deep-seated need to have dominance over others.

Stage 7: The Hate Group Destroys the Target

The ultimate goal of haters is to destroy the object of their hate. Mastery over life and death imbues the hater with godlike power and omnipotence, which, in turn, facilitate further acts of violence. With this power comes a great sense of self-worth and value, the very qualities haters lack. However, in reality, hate physically and psychologically destroys both the hater and the hated.

Model Application

Anecdotal evidence suggests that this hate model has a wider application. For example, when a coworker becomes a hate target for reasons other than race, sex, or national origin, the hater immediately seeks out others in the office who dislike, or can be persuaded to dislike, the hated coworker (Stage 1). The group establishes an identity using symbols and behaviors. They use a lifted eyebrow, a code word to exclude the hated coworker from a lunch invitation, or any number of other actions to demean and isolate. The haters even may adopt a name for their group (Stage 2). At this point, the haters only disparage the hated coworker within their group (Stage 3). As time passes, the haters openly insult the hated coworker either directly or indirectly by allowing disparaging remarks to be overheard from afar (Stage 4). One morning, the hated coworker discovers his desk rearranged and

© Corbis

offensive images pasted over a picture depicting his wife and children (Stage 5). From the sophomoric to the terroristic, acts of hate have the same effect. Eventually, the haters sabotage the hated coworker's projects and attempt to ruin the individual's reputation through rumors and innuendoes (Stage 6). In so doing, the haters make the work environment intolerable for the hate target (Stage 7). Scenarios like this occur every day across America and, indeed, around the world. The targets of hate may change, but the hate process remains constant.

ASSESSMENT

Assessing and analyzing skinhead groups can help investigators tailor intervention strategies to each hate group, thus increasing the probability of successful intervention and rehabilitation. Law enforcement can assess a skinhead group by first determining if the group is hate motivated or criminally motivated. The best method to establish motivation is through one-on-one interviews, although reviewing police reports and criminal histories prove adequate determining factors as well.

Second, investigators should measure the maturity of the group, which is not determined by the chronological age of the group's members but by the collective actions of the group. Violence constitutes an important maturation indicator. Comparing the group's activities to the stages in the hate model can determine the maturity of a skinhead group. Mature groups commit more violent acts than immature groups.

An additional step in the assessment process involves gauging the strength of the group's mythology. Immature groups have simple mythologies, whereas mature groups have more complex and stubborn mythologies. Studying group mythologies proves difficult because they represent the aggregate of a group's common beliefs, experiences, symbols, and rituals.

SYMBOLS, RITUALS, AND MYTHOLOGY

Fully understanding hate groups involves identifying and defining their unique symbols, rituals, and mythologies. Symbols give

greater meaning to irrational hate. Haters use symbols for self-identification and to form common bonds with other group members. Additionally, they often swear allegiance to these symbols. For example, the swastika, a simple symbol, served as a powerful rallying point for the Nazi movement and helped mobilize an entire country.[21]

Each hate group adopts its own symbols or borrows them from others. Symbolic words and nonverbal behaviors reflect individual disdain and serve as advertisements to attract fellow sympathizers. Offensive language is the most common expression of dislike for others. Hate groups also display contempt by using nonverbal gestures, such as a Nazi salute. Clothes, short haircuts, military boots, tattoos, and bumper stickers also represent symbols that can effectively communicate hate.

Symbols, however, are not enough to unify a group; therefore, more organized hate groups incorporate rituals, which serve two functions. First, they relieve individual group members from deep thought and self-examination. Second, rituals reinforce beliefs and fortify group unity.

The hate group's experiences, beliefs, and use of symbols and rituals combine to create group mythologies. Mythologies unify disparate thoughts and act as filters through which group members interpret reality.[22] Group mythologies can have profound effects on its members.[23] A group with a powerful mythology results in one resistant to ideological challenges, and, therefore, it is more dangerous. Mythologies nurtured, reinforced, and protected from outside ideas provide a forum where group members can escape individual responsibility. "When we lose our individual independence in the corporateness of a mass movement we find a new freedom–freedom to hate."[24]

> ***An accurate assessment of skinhead groups is critical to developing intervention strategies.***

INTERVIEWING TECHNIQUES

Ironically, skinheads, especially hate-motivated skinheads, talk to anyone who will listen, including law enforcement officers. One investigator who knew little about white-supremacist ideology simply asked skinheads why they hated, what their tattoos meant, and how skinhead groups were organized. Numerous interviews and observations substantiated the initial information obtained by the investigator. On the other hand, criminally motivated skinheads are less likely to talk because they act more like criminals. Investigators should determine the motivation of skinheads when planning interview strategies.

Hate-motivated skinheads have well-rehearsed answers for questions, such as "Why do you hate?" "Can't you see what you're doing is wrong?" "How would you like it if someone picked on you because of your race?" Skinheads answer smugly; they feel secure as skinheads. Because hate masks personal insecurities, interviewers should temporarily forego questions about why skinheads hate and strive to identify the skinheads' personal insecurities. Interviewers should begin this probe by asking skinheads about their family relationships, which probably represent the source of the skinhead's insecurities because a sense of who people are and where they fit in society typically develops within the family structure. Interviewers also should explore skinheads' future plans, educational goals, and desired employment. This forces skinheads to see themselves as they really are. If forced to look at themselves, skinheads become vulnerable, less resistant to rehabilitation, and, in law enforcement settings, more likely to confess. This process could take several hours or many months depending on the resistance level of the skinhead.

This strategy proves less effective when interviewing criminally motivated skinheads because they view themselves as criminals who hate, rather than haters who commit criminal acts. More traditional interviewing strategies have proven successful with criminally motivated skinheads.

INTERVENTION STRATEGIES

An accurate assessment of skinhead groups is critical to developing intervention strategies.

Dismantling immature skinhead groups proves easier than breaking down sophisticated skinhead groups. Skinheads not solidly committed to supremacist ideology more likely will respond to rehabilitation attempts than hard-core skinheads.[25] Skinheads who have not passed from Stage 4 (rhetoric) to Stage 5 (violence) will prove more receptive to rehabilitation strategies than those skinheads who commit violence.

Investigators should approach criminally motivated skinhead groups by using tactics similar to those used against criminal street gangs. Disrupting the activities of mature, hate-motivated skinhead groups requires time and more elaborate interdiction strategies because such groups are more unified and committed to their beliefs. Conversely, aggressive prosecution constitutes an efficient means to disrupt immature, hate-motivated skinhead groups.

Law enforcement used this technique to dismantle Peer Pride, an immature, hate-motivated skinhead group in Palmdale, California. The FBI learned about Peer Pride when the group hung a noose from a tree in front of the home of an African-American family. Five Peer Pride members taunted the family with racial slurs and demanded that they move out of the neighborhood. Local law enforcement initially treated this incident as a prank because hanging the noose was the only reported hate activity by the group. However, a neighborhood canvass determined that Peer Pride members periodically sat in front of a local fast food restaurant and shouted racial slurs at the African-American patrons. Instead of leniency for the first-time offenders, the Los Angeles County District Attorney's Hate Crimes Unit recommended harsh sanctions, including jail sentences. The effect was immediate. The group disbanded and no other similar problems occurred in the neighborhood. The incident, in and of itself, could have been interpreted as a prank, but, in reality, the group was passing from Stage 3 to Stage 4 in the hate model.

In contrast, the Lancaster NLR group was a mature, hate-motivated skinhead group. Four NLR members beat an African-American transient to death to earn the right to wear lightning-bolt tattoos. According to the group's ritual, members only can earn lightning-bolt tattoos by killing minorities. A review of police reports related to NLR criminal activities clearly showed the NLR group progressing through the seven stages of the hate model.

School administrators and teachers can use the hate model to informally assess hate group activities on campus. Identifying the stage in which a hate group is operating provides valuable information to determine how dangerous the group is and what type of intervention strategies to employ. Early intervention increases the probability of success, especially before the transition period from rhetoric (Stage 4) to violence (Stage 5). These strategies can range from informal sensitivity instruction to more formal programs, such as the Juvenile Offenders Learning Tolerance (JOLT) program administrated by the Los Angeles County District Attorney's Office Hate Crimes Unit. JOLT is a model intervention program intended for first-time, low-level offenders who face potential criminal prosecution and school disciplinary action.

CONCLUSION

To develop and implement successful intervention strategies to deal with hate groups, law enforcement personnel first must understand the hate process. The hate model identifies the multiple stages of the hate process. Investigators can use this model to identify haters who have not yet transitioned from hate rhetoric to hate violence and target them with intervention programs, which have a higher probability of success. Likewise, law enforcement personnel can identify and target hard-core haters with appropriate interdiction strategies. Knowing how the hate process works helps interviewers penetrate the hate mask and address the hater's underlying personal insecurities. If investigators can attenuate these personal insecurities, haters will become more receptive to rehabilitation. Identifying and understanding the stages of the hate

process constitute the first steps in controlling hate violence. ✦

Endnotes

[1] The authors based this article on their observations and interviews of several hundred self-described skinheads, defined as "usually white males belonging to any of various, sometimes violent, youth gangs whose members have close-shaven hair and often espouse white-supremacist beliefs," *Merriam Webster's Collegiate Dictionary*, 10th ed. (1996), s.v. "skinhead."

[2] See Eric Hoffer, *The True Believer: Thoughts on the Nature of Mass Movements* (New York, NY: Harper and Row, 1989).

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Statistics, however, reveal that most hate crimes are not committed by hate groups. See U.S. Department of Justice, Federal Bureau of Investigation, Uniform Crime Reporting Program, *Hate Crime Statistics 2000* (Washington, DC, 2001). For more information on collecting hate crime, see U.S. Department of Justice, Federal Bureau of Investigation, Uniform Crime Reporting Program, *Training Guide for Hate Crime Data Collection* (Washington, DC, 1997).

[7] Raymond Paternoster and Alex Piquero, "Reconceptualizing Deterrence: An Empirical Test of Personal and Vicarious Experiences," *Journal of Research in Crime and Delinquency* 32 (August 1995): 251-286.

[8] See Brian Levin, "A Dream Deferred: The Social and Legal Implications of Hate Crimes in the 1990s," *The Journal of Intergroup Relations* 20, no. 3 (Fall 1993): 10, citing Jack Levin and Jack McDevitt, *Hate Crimes: The Rising Tide of Bigotry and Bloodshed* (New York, NY: Plenum Press, 1993).

[9] Ibid.

[10] Supra note 2, 93-94.

[11] Supra note 2, 93-94.

[12] Supra note 2, 99.

[13] Supra note 2, 92.

[14] Charles W. Turner and John F. Layton, "Verbal Imagery and Connotation as Memory Induced Mediators of Aggressive Behavior," *Journal of Personality and Social Psychology* 33 (1976): 755-763.

[15] Supra note 8, 10.

[16] Supra note 8, 9.

[17] Supra note 8, 10.

[18] Dolf Zillerman's research is described in Daniel Goleman, *Emotional Intelligence* (New York, NY: Bantam Press, 1997), 60-62.

[19] Ibid.

[20] Supra note 8, 8.

[21] William L. Shirer, *The Rise and Fall of the Third Reich: A History of Nazi Germany* (New York, NY: Fawcett Crest, 1960), 71.

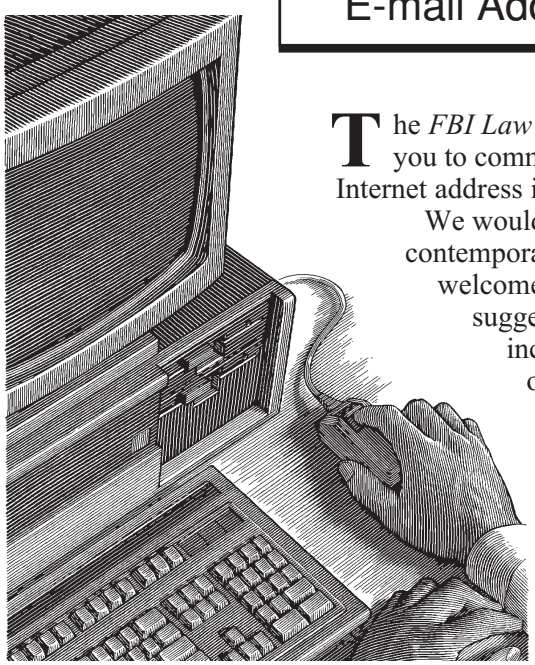
[22] Daniel C. Maguire and A. Nicholas Farnoli, *On Moral Grounds: The Art, Science of Ethics* (New York, NY: The Crossroads Publishing Co., 1991), 164-167.

[23] Joseph Campbell and Bill Moyers, *The Power of Myth* (New York, NY: Doubleday, 1988), 31.

[24] Supra note 2, 100.

[25] Supra note 8, 10.

The *Bulletin's* E-mail Address



The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our Internet address is *leb@fbiacademy.edu*.

We would like to know your thoughts on contemporary law enforcement issues. We welcome your comments, questions, and suggestions about the magazine. Please include your name, title, and agency on all e-mail messages.

Also, the *Bulletin* is available for viewing or downloading on a number of computer services, as well as the FBI's home page. The home page address is *http://www.fbi.gov*.

Bulletin Reports

Web-Based Resources

Biometrics Catalog On-line

The Biometrics Catalog, a federally funded database, is a service of the National Institute of Justice for the biometrics community and potential users of biometric technology. The catalog is designed to provide multiple search options so that browsers can find information quickly and easily. This catalog can be accessed at *http://www.biometricscatalog.org*.

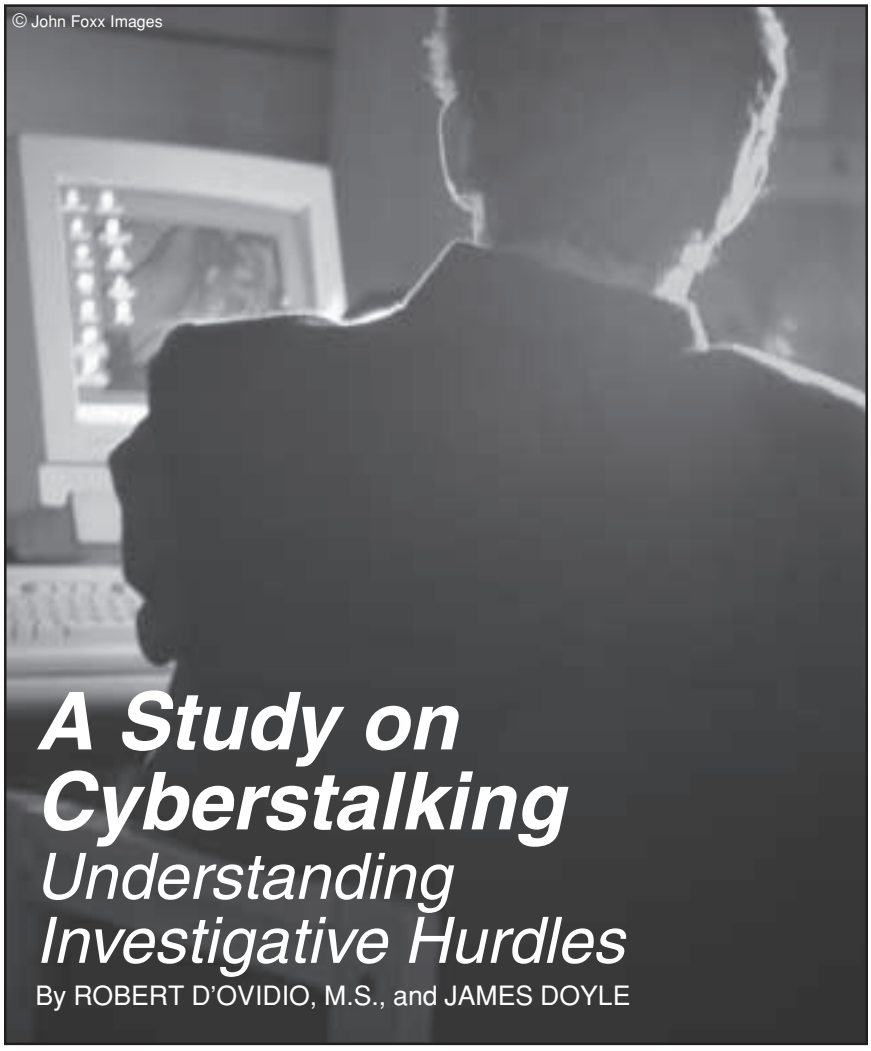
Crime Mapping Research Center (CMRC)

The CMRC Web site is the primary source of information from the National Institute of Justice's (NIJ) Crime Mapping Research Center. It serves as an international clearinghouse for information about the development of crime mapping and spatial analysis. It includes a list of CMRC staff, NIJ-funded grants that pertain to crime mapping, descriptions of upcoming conferences, a list of mapping-related software, a bibliography of crime-mapping resources, and descriptions of CMRC's current initiatives. CRIMEMAP, CMRC's listserv, is one of the center's main information dissemination tools. CRIMEMAP facilitates communication among crime analysts, researchers, geographers, and other interested parties about justice-related computerized mapping technologies. CMRC can be accessed at *http://www.ojp.usdoj.gov/nij/maps*.

Law Enforcement

The National Institute of Justice (NIJ) and the Office of Community Oriented Policing Services (COPS) sponsored a study on the combined effects of pepper spray exposure and positional restraint on respiratory functions. *Pepper Spray's Effects on a Suspect's Ability to Breathe* presents the results of this study. This NIJ Research in Brief (NCJ 188069) summarizes the issues that gave rise to the study, the study's major findings, and their implications for law enforcement. Findings suggest that inhalation of pepper spray does not pose a significant risk to subjects in terms of respiratory and pulmonary functions, even when it occurs with positional restraint. However, pepper spray exposure did result in a small but statistically significant increase in blood pressure, the origins and implications of which remain unclear. This report is available electronically at *http://www.ojp.usdoj.gov/nij/pubs-sum/188069.htm* or by contacting the National Criminal Justice Reference Service at 800-851-3420.

Bulletin Reports is an edited collection of criminal justice studies, reports, and project findings. Send your material for consideration to: *FBI Law Enforcement Bulletin*, Room 209, Madison Building, FBI Academy, Quantico, VA 22135. (NOTE: The material in this section is intended to be strictly an information source and should not be considered an endorsement by the FBI for any product or service.)



A Study on Cyberstalking

Understanding Investigative Hurdles

By ROBERT D'OVIDIO, M.S., and JAMES DOYLE

By enabling human interaction without the constraints of physical barriers and with the perception of anonymity, the Internet has become the ideal instrument for individuals who wish to intimidate, threaten, and harass others. A stalker can use the Internet to send alarming messages anywhere, within a matter of moments, under the guise of a fictitious screen name or pseudonym. Understanding how offenders use the Internet to stalk victims in cyberspace can provide law enforcement officers with solutions when they encounter impediments investigating these types of cases.

DEFINITION OF CYBERSTALKING

As the Internet becomes the communication device of choice for millions of people worldwide, news headlines, such as "Killer Keeps Web Pages on Victim, Stalks Her Through Internet"[1] and "Penn Opens Hate E-mail Inquiry,"[2] have begun to appear more frequently. These headlines depict stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person. The term *cyberstalking* has emerged to describe the use of such technology to harass or stalk.[3] Cyberstalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.

All 50 states and the federal government have enacted statutes aimed at protecting the victims of stalking. Many of these statutes have existed for a long time, while others have originated recently. Some of the older statutes were broad enough to cover any type of stalking behavior, including cyberstalking; others had to be amended to do so. In some jurisdictions, new laws specifically addressing the problem of cyberstalking have been enacted. In adapting general stalking and harassment statutes to cover instances of cyberstalking, legislators have expanded the means by which offenders commit this crime to include electronic communication devices.

Several states currently include specific protections against threatening electronically transmitted communications in their stalking or harassment statutes.[4] Additionally, Title 18, Section 875, U.S. Code, criminalizes threatening messages transmitted electronically in interstate or foreign commerce. The use of federal legislation to prosecute cases of cyberstalking, however, is limited, by law, to

instances where the harassing messages are transmitted across state lines or outside the United States. Despite the existence of Title 18, Section 875, the federal government historically has limited its involvement in prosecuting cases related to electronically transmitted threatening messages to cases involving special circumstances, such as threats made against the president of the United States. As with stalking that does not involve the Internet, local authorities investigate and prosecute most cyberstalking cases in either the jurisdiction where the victim resides or in the jurisdiction where the messages originated.

With the rapid pace of technological advancement that exists in today's society, legislation should take an evolutionary approach toward defining electronic communication devices and systems of transmission. Legislation that limits electronic devices and transmission systems to specific technologies, such as telephones and land-based wires, risk becoming antiquated with the emergence of new technologies, such as computers and wireless transmission systems.

THE STUDY

Background

Anticipating the significant role computers would play in the commission of crimes in the future, the New York City Police Department (NYPD) developed the Computer Investigation & Technology Unit (CITU) in 1995. CITU investigates cases where offenders use a computer or the Internet as an instrument to commit a crime or where a computer represents the target of a crime or constitutes a source of evidence relating to a crime. The unit also performs outreach services to business and community groups to educate people on computer ethics, safe Internet practices, and data security issues related to the most current practices of computer hackers. Additionally, CITU provides training and technical assistance to local, state, and federal law enforcement and prosecutorial agencies.

Methodology

The authors used official police records from NYPD's CITU to capture data on the extent and nature of cyberstalking for this study. Specifically, the data for this study were drawn from information contained within standardized forms filed by the complainant at the time of the initial complaint and standardized investigative forms that detail the progress of the investigation from beginning to end. Data were gathered using all closed cases of aggravated harassment[5] investigated by NYPD from January 1996 through August 2000 in which criminals used a computer or the Internet as the instrument of the offense. In addition to the date of the offense, descriptive information was gathered on the victim, the offender, the outcome of the case, the method used to harass, and whether the victim and suspect resided in the same jurisdiction.

Extent of the Problem

When compared to other cybercrimes, cyberstalking has been the most prevalent crime

Mr. D'Ovidio is a Ph.D. student and instructor at Temple University in Philadelphia, Pennsylvania.

Mr. Doyle serves as president of a private company that trains law enforcement and consults in the area of high-tech crime.

reported to and investigated by CITU since the unit's inception. During the 56-month period from January 1996 through August 2000, 42.8 percent of the cases investigated by CITU involved aggravated harassment by means of a computer or the Internet. Additional CITU investigations during this period involved grand larceny, computer and network trespassing, forgery, petty larceny, criminal impersonation, child pornography, crimes against children, and schemes to defraud. Understanding the distribution of cybercrimes is essential to allocating a computer crime unit's resources in a cost-efficient manner. Training that provides investigators with the technical knowledge and procedural experience needed to successfully investigate cyberstalking should be a priority for a computer crime unit. Agencies should note that the technical training needed to successfully investigate cases of cyberstalking is not entirely crime specific and will prove useful when investigating other types of computer-related crime.

An examination of case outcomes revealed that 192 of the 201 cyberstalking cases investigated by CITU were closed during the 56-month period of this study. Approximately 40 percent of the cases were closed with an arrest, and almost 11 percent of the cases failed to produce evidence that a crime was committed. CITU closed the remaining cases after finding evidence to support the victim's complaint due to a jurisdictional issue, an uncooperative complainant, a case transfer, or exhausting all investigative leads without positively identifying a specific offender.

The Offender

Offender characteristics were examined using the 134 closed cases where a suspect was arrested or where evidence to support an arrest existed but a suspect was not arrested because of an uncooperative complainant or a jurisdictional issue. The results revealed that

> ***"...computer crime investigation units should develop working relationships with their counterparts in other jurisdictions."***

males (approximately 80 percent of the cases) were more likely than females to commit aggravated harassment using a computer or the Internet. Approximately 74 percent of the offenders were white, 13 percent Asian, 8 percent Hispanic, and 5 percent black. The average age of the offender was 24, with the oldest offender being 53 years old and the youngest being 10 years old. Approximately 26 percent of offenders were juveniles, according to New York State law, or under the age of 16.

The Victim

Victim characteristics were examined using the 171 closed cases where investigators determined that a threatening or alarming message[6] was transmitted using a computer or the Internet (excluding cases with unfounded outcomes). Females, the most likely recipients, were victimized in about 52 percent of the cases, whereas males were the victims of aggravated harassment in approximately 35 percent. Educational institutions represented the next most likely target with 8 percent. Offenders chose private corporations in almost 5 percent of the cases. Public-sector agencies were targeted in about 1 percent of the cases.

Approximately 85 percent of victims were white, 6 percent Asian, 5 percent black, and 4 percent Hispanic. The average age of the victims was 32, with the youngest victim being 10 years old and the oldest being 62 years of age.

Technological Methods

In 92 percent of the cases, offenders used only one method to stalk their victims. E-mail was used most often. Offenders used e-mail to harass their victims in approximately 79 percent of the cases. The second method most often used by offenders was the instant messenger. Offenders used instant messengers to harass their victims in about 13 percent of the cases. Chat rooms were used in approximately 8 percent of the cases, while message boards and Web sites were used respectively in 4 percent and 2 percent of the cases. Last, offenders employed newsgroups and false user profiles in approximately 1 percent of the cases.

Cyberstalking Methods

Cyberstalkers have employed various methods of Internet communication to harass their victims. Although not exhaustive, the following list describes some of the methods that cyberstalkers may use:

- E-mail: A method of communication that allows an individual to transfer text, picture, video, and audio files to another person's electronic mailbox. In using e-mail to harass, the cyberstalker creates a text-based, graphic-based, or audio-based message of a threatening, alarming, or otherwise harassing nature and sends it to the e-mail account of the intended victim.
- Newsgroups: A method of communication that amounts to an ongoing discussion about a particular topic. Internet users contribute to the ongoing discussion by posting their opinions, comments, or related experiences about a particular subject. These postings are linked together and can be retrieved by querying a database of newsgroup topics. Cyberstalkers can use these forums to post threatening or defamatory statements directed at a specific individual or group of individuals. In *New York v. Munn* (688 N.Y. S.2d 384; 1999), the court found the defendant guilty of aggravated harassment for posting a message to an Internet newsgroup that instructed people to kill police officers from the NYPD.
- Message boards/guest books: A method of communication similar to a newsgroup in that its contents amount to comments about a particular topic. Internet sites often have guest books where visitors can enter their names and make comments about the site. The visitor's name and comments are subsequently available to be viewed by others visiting the Web site. A person who wants to threaten or harass the owner of a Web page easily can leave alarming messages in a guest book.
- Internet sites: A method of communication that involves posting information to a unique uniform resource locator (URL). Internet users later can retrieve this information by directing their Web browser to the corresponding URL. An Internet site becomes the method of harassment when a cyberstalker posts information on a Web page about an individual that causes them to become alarmed or frightened. For example, a cyberstalker could create an Internet site that advertises sexual services for hire and includes the victim's picture, phone number, and address. Subsequently, the victim is bombarded with telephone calls or personal visits from individuals inquiring about the advertised sexual services.
- Chat rooms: A method of communication that enables real-time text, audio, and video-based group interaction. Chat rooms, or chat channels, usually are organized around specific topics of conversation. Topics include, but are not limited to, such issues as politics, religion, relationships, and sex. When communicating in a chat room, a participant's messages are broadcast to everyone signed into the particular chat room. Several types of chat services have emerged since the development of the Internet. Chat services can be public or private. Public chat services are open to everyone with access to the Internet. For example, Internet relay chat (IRC) and I seek you (ICQ) chat are open to all Internet users. Both IRC and ICQ chat rooms have hundreds of chat channels that cover a diverse range of subjects and enable the transfer of files between active participants. Unlike public chat services, private services limit access to their chat channels and are hosted by specific on-line service providers. Chat rooms provide cyberstalkers with different options to harass their victims. A stalker can send alarming messages directly to the victim while conversing in a chat room. The message is delivered to the intended victim, as well as to all those users who currently are logged into the chat room. In addition, the cyberstalker can pose as the victim in a chat room and provide personal information to participants, thereby resulting in the intended victim being directly contacted in person, by e-mail, or by phone.
- Third-party instant messengers: A method of communication that enables real-time text, audio, and video-based interaction between two individuals over the Internet or a computer network. Users program their instant messenger software to notify them when designated individuals log on to the network. With instant messaging software, users have the ability to engage in real-time dialogue with a designated person as long as both parties are connected to the network. Stalkers with prior knowledge of a victim's screen name can use an instant messenger to send harassing messages in real time when both parties are logged onto the Internet.
- Commercial service user profiles: A method of communication that involves posting descriptive information about oneself to the membership directory of a commercial Internet service. Service subscribers can query this directory so that they may find other members who share similar hobbies, interests, or backgrounds. People who want to harass others may establish a false user profile that will direct unwanted communication toward their victim in the form of repeated telephone calls, e-mails, or in-person contact.

Resources

U.S. Department of Justice Cybercrime Web Site: *http://www.cybercrime.gov*
High Technology Crime Investigation Association: *http://www.htcia.org/*
SEARCH—The National Consortium for Justice Information & Statistics: *http://www.search.org/*
National Center for Missing & Exploited Children: *http://www.ncmec.org/*
International Association of Computer Investigative Specialists: *http://www.cops.org/*
Compuforensics: *http://www.compuforensics.com/*
National Law Enforcement & Corrections Technology Center: *http://www.nlectc.org/*
National White-Collar Crime Center: *http://www.iir.com/nwccc/nwccc.htm*

Knowing the type of Internet technology used most often by cyberstalkers can prove beneficial to law enforcement administrators who must decide how to allocate the training budget for computer crime investigators. Because e-mail constitutes the method most often used by cyberstalkers, unit administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics.

ISSUES FACING LAW ENFORCEMENT AND POTENTIAL SOLUTIONS

Technical features of the Internet and procedural issues with the law present problems for criminal justice agencies when investigating and prosecuting cyberstalking cases. These problems, however, are not crime specific and generally occur when agencies investigate and prosecute cases involving any type of computer crime.

Jurisdiction

The global reach of the Internet and the instantaneous nature of computer-mediated communication present law enforcement with jurisdictional issues that could negatively impact the investigation and the subsequent prosecution of computer crimes.[7] With the Internet, stalkers no longer need physical proximity to have contact with their victims. They just as easily can harass a person in another state or country as they can a person who lives in close proximity.

The majority of CITU's aggravated harassment cases involved investigations where both the offender and victim resided within the jurisdiction of the NYPD. In approximately 72 percent of the cases, the offender and the victim resided within the five boroughs of New York City. In comparison, 26 percent of the cases involved either an offender or a victim who resided outside the jurisdiction of the NYPD but within the United States, while 2 percent of the cases involved an offender from a foreign country.

An offender residing outside the jurisdiction of the investigating agency can negatively impact the outcome of a case. In New York City, the District Attorney's Office is less inclined to prosecute aggravated harassment cases if the arrest of the suspect requires extradition from another jurisdiction. Such policies have prevented the apprehension of offenders by the NYPD in cases where investigations by CITU have produced evidence supporting their arrests. In 20 aggravated harassment cases investigated by CITU, the NYPD did not arrest the suspects, despite supporting evidence, because their arrests would require extradition from another jurisdiction. In these cases, the NYPD made referrals to the police departments that had jurisdiction over the offenders.

Differences in statutory definitions of stalking across states may complicate the investigation and prosecution processes when offenders reside outside the jurisdiction of the investigating agency. Jurisdictions that do not recognize Internet communication as a viable method to stalk or harass may deny or ignore the extradition request, search warrant, or subpoena of a jurisdiction where

such methods do constitute a criminal offense.

To minimize the negative impact jurisdictional issues have on the successful investigation and prosecution of cyberstalking cases, computer crime investigation units should develop working relationships with their counterparts in other jurisdictions. Such relationships can prove essential to securing the arrest of out-of-state or foreign offenders in their home jurisdictions when the victim's jurisdiction will not arrest if extradition is required. In addition, cross-jurisdictional relationships between computer crime investigation units can help secure the execution of out-of-state subpoenas and search warrants and facilitate relationships with out-of-state Internet service providers, computer manufacturers, and software developers. Over the past decade, various professional organizations have formed for those involved with the investigation of computer-related crimes. Participation in these organizations can provide law enforcement with invaluable links to out-of-state resources.

Because of the ease with which cyberstalkers may attack across jurisdictional lines, legislatures should carefully define the venue of the offense. In cases where threatening communication originates from another state or country and the statute of the investigating jurisdiction defines the venue of the offense in terms of where the communication originated, the criminal justice community will not be able to properly serve the victim. When creating legislation to combat cyberstalking or when revising existing stalking legislation to include Internet communication, states should define the venue of the offense in a manner that includes both the place where the communication was received and the place where the communication originated.

> ***...administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics.***

Account and User Information

The unwillingness of some Internet service providers to readily grant law enforcement access to subscriber records further complicates the investigation of a cyberstalking case. Not all Internet service providers agree on what constitutes subscriber records, which are obtainable by subpoena, as opposed to transactional records, which require a search warrant.[8] When compared to obtaining telephone records from a telephone company, obtaining a suspect's Internet account information from a service provider can prove far more complicated and involve an increase in the amount of paperwork and time an investigator spends on a case.

Out-of-date and missing account, subscriber, or user information also presents problems to law enforcement agencies when investigating cases of cyberstalking. Without toll records or transactional data, investigators can have a difficult time establishing an electronic link between the suspect and the victim. The financial and human costs associated with gathering and maintaining account information decreases the possibility that Internet service providers will voluntarily collect and maintain such data for a useful period of time. Missing toll records, transactional data, user information, or account content resulted in a negative case clearance in approximately 18 percent of the cyberstalking cases investigated by CITU. In these cases, the content of the communication contained a threatening message, but no arrest occurred because detectives could not gain access to the electronic evidence to legally support apprehending a specific individual. To ensure that account, subscriber, and user information are collected and saved long enough to help law enforcement, legislation that regulates Internet service providers should include data collection requirements.

Anonymizing Tools

The continued development and increased availability of anonymizing Internet tools (i.e., devices that ensure a person's anonymity when using the Internet) can complicate the investigation of cyberstalking cases. Anonymous

remailers allow individuals to send electronic mail without transmitting any information that would enable others to determine the identity of the author. Remailers strip identifying information from the e-mail header and erase any transactional data from servers that would enable law enforcement to trace the message back to the author. Consequently, cyberstalkers who use an anonymous remailer as the sole means to send threatening or harassing e-mail messages will remain virtually undetectable to the victim and law enforcement. The danger raised by the use of anonymous remailers, as depicted by CITU's caseload, does not stem from the frequency in which these tools are used, but from the effect these tools have on the investigative process. Anonymous remailers were used in only 4, or 2.1 percent, of the 192 cyberstalking cases investigated by CITU. Investigators, however, could not trace the harassing e-mail messages sent through the anonymous remailers back to their authors in all four cases where these tools were used.

Anonymous Web-browsing services also offer cyberstalkers the opportunity to harass or threaten victims while remaining virtually untraceable to law enforcement. Some companies provide users with the ability to surf the Internet, participate in public chat channels, send instant messages, and post messages to newsgroups without transmitting any identifying information. The exclusive use of such services to send harassing messages would prevent investigators from establishing an electronic link between the victim and the offender. An examination of CITU's cyberstalking caseload found no instances where offenders used anonymous Web-browsing services to stalk their victims.

The widespread availability of anonymizing tools can increase the amount of cyberstalking and Internet deviance in general. Theoretically, deviance will result from the use of anonymizing tools because people will feel less restrained when not faced with the fear of detection by their victim or the police. The absence of a legally binding international body to regulate the Internet leaves little hope that the deployment of anonymizing tools will be stopped. Even if a country did succeed in banning the distribution of anonymizing tools, the global reach of the Internet would enable people to seek out such tools in countries that allow their use. Consequently, citizens must learn to survive on an Internet where people can act without accountability. In the absence of a regulatory solution to safeguard Internet users against those who employ anonymizing tools to harass, Internet service providers and related software companies should seek a technological solution aimed at blocking unwanted anonymous communication.

Distribution of Cybercrimes Investigated by the New York City Police Department January 1996 through August 2000

Crime	Number of Cases	Percent of Cases
Aggravated harassment	201	42.8
Grand larceny	102	21.7
Hacking (e.g., computer trespass)	46	9.8
Forgery	23	4.9
Petit larceny	22	4.7
Criminal impersonation	20	4.3
Child pornography	19	4.0
Crimes against children	14	3.0
Scheme to defraud	10	2.1
Other crimes	13	2.8
Total	**470**	**100**

CONCLUSION

Because the Internet allows human interaction without physical barriers and with the perception of anonymity, it has become the ideal instrument for individuals who wish to intimidate, threaten, or harass. Federal and state legislation have emerged to criminalize such behavior. Legislatures aiming to criminalize cyberstalking should

take an evolutionary approach toward defining the means of communication covered by the law to ensure protection against harassing communications sent using newly developed technologies.

An examination of all computer crimes investigated by the New York City Police Department from January 1996 through August 2000 found cyberstalking to be the most prevalent computer crime investigated by the department. Thus, police personnel administrating computer crime units should prioritize staffing and training initiatives that properly equip their units to deal with the cyberstalking problem. Additionally, because cyberstalkers use e-mail as the communication method of choice, computer crime unit administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics.

Out-of-date and missing account, subscriber, and user information, as well as anonymizing tools, presented problems for law enforcement during cyberstalking investigations. Working relationships between computer crime units in all agencies can minimize the negative effects that jurisdictional issues have on the investigation and prosecutorial processes. These relationships can help facilitate the execution of out-of-state subpoenas and search warrants and provide law enforcement with an open door to out-of-state Internet service providers.

Out-of-date and missing account, subscriber, and user information also have prevented law enforcement from establishing an electronic link between the suspect and the victim. To offset this negative effect, legislative action should establish data collection standards for Internet service providers that meet the needs of computer crime investigators.

> ***"All 50 states and the federal government have enacted statutes aimed at protecting the victims of stalking."***

Finally, the infrequent use of anonymous remailers by cyberstalkers should not pull attention from the negative effect that these tools can have on the law enforcement process. The increased availability and continued development of anonymizing Internet tools that are easier to use than previous versions likely will increase the use of these options by criminals. When used, anonymous remailers successfully prevented law enforcement from tracing e-mail messages back to the offender. A technological solution aimed at blocking anonymous communication will offset the threat to users posed by anonymous remailers. ✦

Endnotes

[1] "Killer Keeps Web Pages on Victim, Stalks Her Through Internet," (November 29, 1999), *retrieved June 21, 2001 from http://www.canoe.ca/technews9911/30_killer.html*.

[2] Sudarsan Raghavan, "Penn Opens Hate E-mail Inquiry," *Philadelphia Inquirer* on-line (November 7, 1999), retrieved June 21, 2001, from *http://www.phillynews.com/inquirer/99/Nov/7/front_page*.

[3] U. S. Department of Justice, "1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry," August 1999; retrieved November 6, 2001, from *http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm*.

[4] American Prosecutors Research Institute, *The Status of Cyberstalking in the Context of Violence Against Women* (Arlington, VA: American Prosecutors Research Institute, 1999). For instance, section 240.30 of the New York State Penal Law finds a person guilty of aggravated harassment if the individual purposely intends to harass, annoy, threaten, or alarm another person by means of mechanical, electronic, or written communication. Additionally, New York revised its antistalking statutes in December 1999 to cover electronic communication, such as e-mail, that is likely to cause fear or harm. In defining the actions that constitute stalking, section 646.9 of the California State Penal Code includes verbal, written, or electronic communications that are intended to place individuals in reasonable fear for their safety. In defining electronic communications, California has relied upon the definition used in the U.S. Code for regulating behavior related to communication devices. Specifically, the term electronic communication means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system." According to the California State Penal Code, the devices used to transmit electronic communications include, but are not limited to, telephones, cellular phones, computers, video recorders, fax machines, and pagers.

[5] New York Penal Law § 240.30

[6] As defined by New York Penal Law § 240.30.

[7] Neil Barrett, *Digital Crime: Policing the Cybernation* (London, England: Kogan Page, 1997).

[8] The legal requirements for obtaining such records are contained in the Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. §§ 2701-2711.

Mr. D'Ovidio can be reached via e-mail at dovidio@temple.edu.
Mr. Doyle can be reached via e-mail at jrdoyle@internetcrimes.com.

Recruitment Strategies
A Case Study in Police Recruitment

By Mark A. Spawn

For years, an official advertisement in a local newspaper constituted the only police recruitment efforts of the Fulton, New York, Police Department. The simple announcement usually provided a sufficient number of applicants for screening and hiring purposes. However, the department recently encountered a problem—even though applicants passed the written civil service test, many of them failed the physical agility test.

Background

Fulton, New York, a small city in the central part of the state, employs 35 sworn officers to serve the community. The Fulton Police Department maintains an active police candidate list for at least 2 years and, often, up to 4 years. But, because of an insufficient number of candidates several years ago, the agency offered the civil service test, the first phase of the testing process, for police officers for the second time in 2 years. In 1996, 144 applicants took the written examination for the police officer position, and, of those, 100 individuals passed. When the department offered the police test again in 1999, 47 applicants took the test and 36 (76 percent) passed.

The next stage in the testing process consists of the physical agility test. The department tests candidates for flexibility, the amount of push-ups and sit-ups performed in a certain time frame, and the completion of a 1.5-mile run. In 1999, more than 58 percent of the applicants could not pass the agility test, which left a short list of candidates. After the remaining group completed background investigations and psychological and polygraph testing, seven more applicants were excluded from the list leaving only 12 percent of those who had taken the written test eligible for appointment. The shortage of eligible candidates seriously concerned the department. In particular, candidates did not seem prepared for the agility test. The written examination had not changed significantly in recent years, but neither had the agility standards. To rectify the problem of a seriously short candidate list, the Fulton Police Department announced another written test in 2000 to garner more candidates.

Recruitment

For the written test in 2000, the department embarked on a serious recruitment campaign. The department sent posters to area colleges and press releases to local newspapers and radio and television stations. The department highlighted the recruitment drive, as well as the physical standards, on a special page on its Web site. The department's officers and their families, as well as the department staff, assisted with the production of a television commercial that aired in the region and drew the most attention. It showcased Fulton and its police department by starting with a community theme, then leading to a police officer talking with a citizen, investigating an accident, and examining crime scene evidence. At the end of the commercial, viewers saw a telephone number and heard a voice that asked them, "Are you up to the challenge?" For 2 months, the agency continued a barrage of media releases and aired the television commercial. This proved an unusual recruitment approach in the area, and it drew the attention of all three local network affiliates, which increased publicity even more. During this time, the

Recruitment Strategy

	1999 No Strategy	2000 Aggressive Strategy
Candidates taking written test	47	160
Candidates passing written test	36	111
Top-scoring candidates passing all screenings*	42%	71%

**includes written exam, physical agility test, and background investigation*

department made applications available not only through the civil service office during business hours but also from the police department. All of these efforts proved so successful that the department had to use a high school gymnasium as a testing center.

To help candidates meet the required physical fitness standards, each applicant received a summary of the requirements. Even though the standards constitute a part of the basic application package, the department added emphasis by attaching a simplified chart, which showed applicants what the department would require if they passed the written examination. Candidates received the fitness standards once again prior to agility testing, several weeks before the test. By providing this information to the candidates well in advance, the department hoped that the elimination rate would decrease significantly.

Results

The results of candidate testing showed that the department's efforts paid off. A record 160 candidates took the written examination and 111 (69 percent) passed. A segment of those applicants with a passing score underwent the physical agility testing. Of that group, 71 percent passed, a 29 percent increase from the previous year. Even though a 7 percent greater failure rate existed with the written examination compared to the previous year's exam, the significant increase of those who successfully completed the agility test gave the department a much larger candidate pool. It also validated the recruitment campaign and, particularly, the emphasis on the physical agility component.

During the written examination in 2000, the department surveyed candidates to elicit responses concerning recruitment efforts. It designed the survey to measure best practices for recruitment, availability of application packages, number of police tests taken, and applicants' knowledge of physical agility standards. A summary of the survey results indicated that newspaper advertising proved the most prominent medium from which candidates learned about the police test, followed closely by the television advertising. Candidates suggested that newspaper and television were the best mediums to notify them of future tests. The availability of police test packages was important—45 percent of candidates obtained them from the police station and 33 percent from the personnel office.

The most critical survey question evaluated whether the department delivered the message on agility standards. Surveys asked if candidates knew about the physical agility requirements. An overwhelming 94 percent said that they knew, and 5 percent answered that they "somewhat" knew about them. Only 1 percent answered "no." The best analysis occurred when top-scoring candidates underwent physical agility testing. At that time, the pass rate for the agility test reached 71 percent, a 13 percent increase from the previous year.

In New York, the entrance exam is standardized and given on the same day statewide. This allows

applicants to sit for one test and have their scores filed with other jurisdictions in the state. In 2000, 82 percent of the applicants sitting for the Fulton exam tested only for the Fulton Police Department.

Conclusion

The officer candidate selection process—from the written test to the agility test, to background investigations, psychological evaluations, and polygraph examinations—is intensive and expensive. After many applicants failed the physical agility test in 1999, the Fulton Police Department implemented an aggressive recruitment campaign to attract larger numbers of candidates. The department used a variety of resources to recruit local residents and to advise them of required physical fitness levels. As a result, a record number of candidates took the written examination, and the number of applicants who passed the physical agility test increased dramatically from the previous year.

A recurrent emphasis on fitness throughout the testing process is a message to candidates of the importance of the standards. While some law enforcement administrators might view a high failure rate for physical testing as a problem beyond their control, an intense recruitment program highlighting the minimum requirements is one method to increase results and yield more candidates. ✦

Chief Spawn heads the Fulton, New York, Police Department.

Subscribe Now

United States Government
INFORMATION

Order Processing Code:
* 5902

☐ YES, please send _____ subscriptions to:
FBI Law Enforcement Bulletin

The total cost of my order is $ _____.

Credit card orders are welcome!
Fax orders: (202) 512-2250
Phone orders: (202) 512-1800
Online orders: bookstore.gpo.gov

(FBIEB) at $36 each ($45 foreign) per year.
Price includes regular shipping & handling and is subject to change.

Name or title (Please type or print)

Company name Room, floor, suite

Street address

City State Zip code+4

Daytime phone including area code

Purchase order number (optional)

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐–☐

☐ VISA ☐ MasterCard ☐ Discover

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

Authorizing signature 1/2001

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Important: Please include this completed order form with your remittance. ***Thank you for your order!***

Best Practices of a Hate/Bias Crime Investigation

By WALTER BOUMAN

© Mark C. Ide

On April 23, 1990, the U. S. Congress signed the Hate Crime Statistics Act into law.[1] Previous to this act, hate/bias crimes existed, but were not tracked or focused on as a specific type of crime. For example, Adolf Hitler's attempted genocide in the 1930s and 1940s registers as one of the most heinous acts in history and the abomination that all hate/bias crimes are measured against, but, at the time of its discovery and investigation, no act or specific guideline for investigating and classifying hate/bias crimes existed.

The FBI defines a hate/bias crime as "a criminal offense committed against a person, property, or society which is motivated, in whole or in part, by the offender's bias against a race, religion, disability, sexual orientation, or ethnicity/national origin."[2] Hate/bias crimes destroy communities, as well as hoard resources from law enforcement agencies. Hate/bias crimes tear at the very fabric of American society—a society based on clear and certain truths intended for all citizens and communities and distinctly stated in the Declaration of Independence. "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness."

Law enforcement agencies and officers need to know the issues, guidelines, and action steps that comprise an effective hate/bias crime response and investigation.[3] Law enforcement agencies also should ensure that investigators receive training in such critical elements as understanding the role of the investigator, identifying a hate/bias crime, classifying an offender,

interviewing a victim, relating to a community, and prosecuting an offender. When hate/bias crimes occur, they deserve investigators' timely response, understanding, and vigilance to ensure an accurate and successful investigation. While veteran investigators of hate/bias crimes recognize these basic tenets, they also know the importance of revisiting them periodically to remind law enforcement officers how to handle fragile victims, families, and communities that have been traumatized by the hateful act of a criminal. Furthermore, the events of September 11, 2001, require the law enforcement community to render special attention to these crimes because the hated community was the entire United States and its way of life.

Understanding the Investigator's Role

All investigators responding to or helping in the investigation of a hate/bias crime must be caring and compassionate persons. They must tolerate all races, religions, national origins, sexes, sexual orientations, and disabilities to maintain a nonjudgmental attitude throughout an investigation. Investigators must have comprehensive knowledge of the general elements and motivations behind hate/bias crimes. Investigators also need to recognize the potential of such crimes to affect the primary victim, the victim's family, other members of the victim's group, or the larger community.

When working with the victims of a hate/bias crime, the role of the first responder is critical.[4] In many instances, the investigator is the first contact with law enforcement, the government, or the justice system that the victim may have experienced. Investigators become representatives of their entire agency, and, without a good first impression, the victim may feel driven away. Driving a victim away, even unintentionally, will slow an investigation and cause the victim to feel even more alienated. Responding to a potential hate/bias crime in the correct fashion can open the lines of communication between the victim and the investigator, but it also can ensure that the search for offenders begins in the right direction.

"Investigators become representatives of their entire agency, and, without a good first impression, the victim may feel driven away."

Mr. Bouman currently trains federal officers in California and New Mexico in cooperation with the Federal Law Enforcement Training Center (FLETC) based in Glynco, Georgia.

Identifying Hate/Bias Crimes

A common, but critical, mistake in a hate/bias crime investigation is the misidentification of the crime. Attempting to correct a misidentification with a victim, community, or within a law enforcement agency is time consuming and difficult at best. Officers unsure about identifying a potential hate/bias crime should consult with a supervisor or an expert on the topic. They should use the department chain of command to inform the department of the incident and to update key members throughout the investigation. Questions similar to the following will help investigators identify hate/bias crimes and begin an investigation.

- Was the victim a member of a targeted class?
- Was the victim outnumbered by the perpetrators?
- Did the victim and offender belong to different groups?
- Would the incident have taken place if the victim and offender were of the same group?
- Have other incidents occurred in the same locality or in a similar place?

- Have other incidents happened at similar times?
- Is the time significant to hate-motivated groups?
- Were the victims of these incidents members of a targeted group?
- Was the victim a member of a protected class that is outnumbered by members of another group in the neighborhood?
- Did the offender use biased oral comments, written statements, or gestures?
- Were bias-related objects, items, or symbols used or left at the crime scene?

Classifying Offenders

Equipped with the answers to these questions, investigators should be able to determine if the crime was committed based upon hate or bias and, if so, begin to investigate the motivations of the offender. Hate/bias crimes, offenders, and their motivations all typically fit within five basic classifications.

1) Thrill seeking: Generally groups of young people, these offenders are motivated by the experiences of psychological or social excitement, mere pleasure, or the gain of bragging rights. Their targets often are unknown outside the groups they represent. Hate/bias-based graffiti or verbal or physical assault represent offenses of this classification.

2) Organized: Motivated by the need to express their profound resentment against, for the most part, minority groups, these offenders look for a role model or leader who will organize and encourage them to act. Skinheads and their activities exemplify this classification.

3) Missionary: Usually identifying with a specific leader or higher power, these offenders seek to rid the world of evil by disposing of the members of an identified and despised group. Those led by Hitler typify this classification.

> ***"Hate/bias crimes destroy communities, as well as hoard resources from law enforcement agencies."***

4) Reactive: Typically showing a lack of tolerance for individuals of other groups, these offenders protect and defend what belongs to them (a country, community, neighborhood, school, or church) from outsiders. Average citizens defending their race against another race characterize this classification.

5) Identity conflicted: Motivated by self-hatred or self-protection, these offenders assault targets with whom they share common traits or characteristics. A homosexual person targeting or assaulting other homosexuals epitomizes this classification.

Once a crime has been responded to, recognized as a hate/bias crime, and classified as such, investigators should conduct a timely and comprehensive follow-up investigation. Knowing and understanding the five typical classifications, as well as remaining aware of meaningful calendar and anniversary dates (e.g., Hitler's birthday), key symbols (e.g., tattoos, mantras), or previous patterns of activity significant for these groups and their agendas, can assist in an effective investigation. Investigators must proceed promptly to keep the incident from escalating, apprehend the perpetrator, and diligently process all physical evidence, all while remaining sensitive to the feelings and needs of the victim or surrounding community.

Interviewing Victims

Hate/bias crimes are uniquely violent and traumatic. Victims of these crimes feel degraded, isolated, frightened, suspicious of others, powerless, and depressed. Some victims experience severe trauma and denial about the incident, and some victims and families may feel emotionally disturbed for extended periods of time. This long-term stress can take a substantial toll on a family and the surrounding community. Effective investigators know and understand these elements of hate/bias crimes.

© Peter Hendrie

> Responsive and sensitive investigators also understand how important their communication skills are in these cases and that, in many cases, listening is more important than talking.

When interviewing the victim of a hate/bias crime, investigators must pay attention to the victim's state of mind and do everything in their power to gain useful information while creating a nonstressful environment for the victim. Investigators should interview victims in private. This will help calm victims and remove them from any distractions. Investigators who allow a close friend or family member to join the interview will experience calmer victims. These people will provide support, keep the victims focused, and help them relax. However, official statements cannot be made for victims by friends and family, and investigators should make this clear. Some victims also may require, or be more comfortable with, an interpreter.

Investigators should ask questions slowly and allow the victim plenty of time to think or recall important details. Some questions will be difficult to ask and answer; therefore, investigators never should become impatient or argumentative with the victim. Investigators need to collect critical information about specific acts or words used by the perpetrator, as well as record and compile anything else that can help establish a motivation of hate or bias. Victims also will need time to vent frustration and display emotions. To help facilitate this, investigators should express a genuine sense of care and concern throughout the investigation. Last, investigators must help victims connect to sources of support in the community. The critical information gathered during these interviews will be advantageous to a thorough and expeditious investigation, the apprehension of perpetrators, the prosecution of the crime, the response to other such crimes, and the prevention of hate/bias crimes in the future.

Relating to Communities

Many citizens do not understand hate/bias crime laws, investigation procedures, or the time required to complete a successful investigation. Thus, investigators need to work as liaisons between their agency and the community. Educating victims and others about hate/bias crimes should become a priority and coincide with an investigation. Victims and communities will then better understand probing and inquisition regarding the incident. Moreover, education could become a valuable investment in future prevention or response to such crimes.

Investigators can use many tactics to educate, train, and empower communities to fight hate/bias crimes. Establishing and training Neighborhood Watch groups, encouraging community meetings and community problem-solving activities, and supporting community efforts by involving local law enforcement agencies are just a few of the ways investigators can make a good first impression with the community. Investigators also can train targets and victims of hate/bias crimes as responsive and preventive advocates; engage members of local community organizations to help with the response, investigation, and prevention of hate/bias crimes; and help coordinate critical support services for primary and secondary victims. Vigorously responding to and investigating hate/bias crimes in the local community and using

the media proactively to inform and educate the community also will generate trust for investigators within a community. On a larger scale, using national resources, programs, and models for prevention, response, and healing will help revive communities.

Working with the families, friends, neighbors, and communities that surround a hate/bias incident becomes as important as working with the victim. Secondary victimization induces blame, outrage, or fear in a family, group of friends, or community. These groups may be motivated to act in response to a hate/bias crime and retaliate in their own ways unless they are educated and provided other options for response or healing. Moreover, no better advocates exist in a community than victims of a hate/bias crime. Training victims and communities to cooperate with law enforcement and other community programs takes the control out of the hands of the perpetrator, instills confidence in the victim and community, and prevents future crimes.

Prosecuting Offenders

To instill even more confidence in an affected community, investigators must help with the prosecution of offenders. Keeping the state district attorney's office informed and involved is absolutely necessary for effective prosecution of individuals involved in hate/bias crimes. Federal violations will require the involvement of federal agencies. In these cases, establishing rapport with the federal agency assisting in the investigation and with the U.S. Attorney's Office will constitute the correct avenue for investigators. Also pertinent to investigations is the fact that some states do not have hate/bias crime laws. Departments and investigators in these states must be willing to assist the federal agencies and unite with the U.S. Attorney's Office to ensure the prosecution of suspects. A working relationship with any state or federal attorney's office and its investigators can help develop a joint road map to a successful investigation and prosecution, secure needed search warrants, establish rapport between the victim and the prosecutor, and introduce the victim and community to the inner-workings of the justice system.

> ***...no better advocates exist in a community than victims of a hate/bias crime.***

The goal of an investigation is to bring the criminal to justice. Prosecution of the perpetrator will help the victim and community bring closure to the horrid events and will bring law enforcement and the community more into harmony, thus creating a safer place for people to live and work.

Conclusion

Law enforcement officers who respond to or investigate hate/bias crimes must understand the complexities that define such acts. In turn, they will benefit from informed choices and actions that can help keep or return a community to a safe, secure, and peaceful state. Before the goal of returning a community to normalcy can be achieved, however, investigators have the task of dealing with families, the community, and the local media, in addition to the victim and offender. Furthermore, multiple law enforcement agencies must be included in the investigation to ensure that every logical question is asked and every practical scenario is investigated. Law enforcement agencies and departments that understand the connections between these actions and results will promote the sensitive, timely, and effective response and investigation of hate/bias crimes in their communities.

Endnotes

[1] U.S. Department of Justice, Federal Bureau of Investigation, Uniform Crime Reporting Program, *Hate Crime Statistics 2000* (Washington, DC, 2001). For more information on collecting hate crime, see U.S. Department of Justice, Federal Bureau of Investigation, Uniform Crime Reporting Program, *Training Guide for Hate Crime Data Collection* (Washington, DC, 1997), 60.

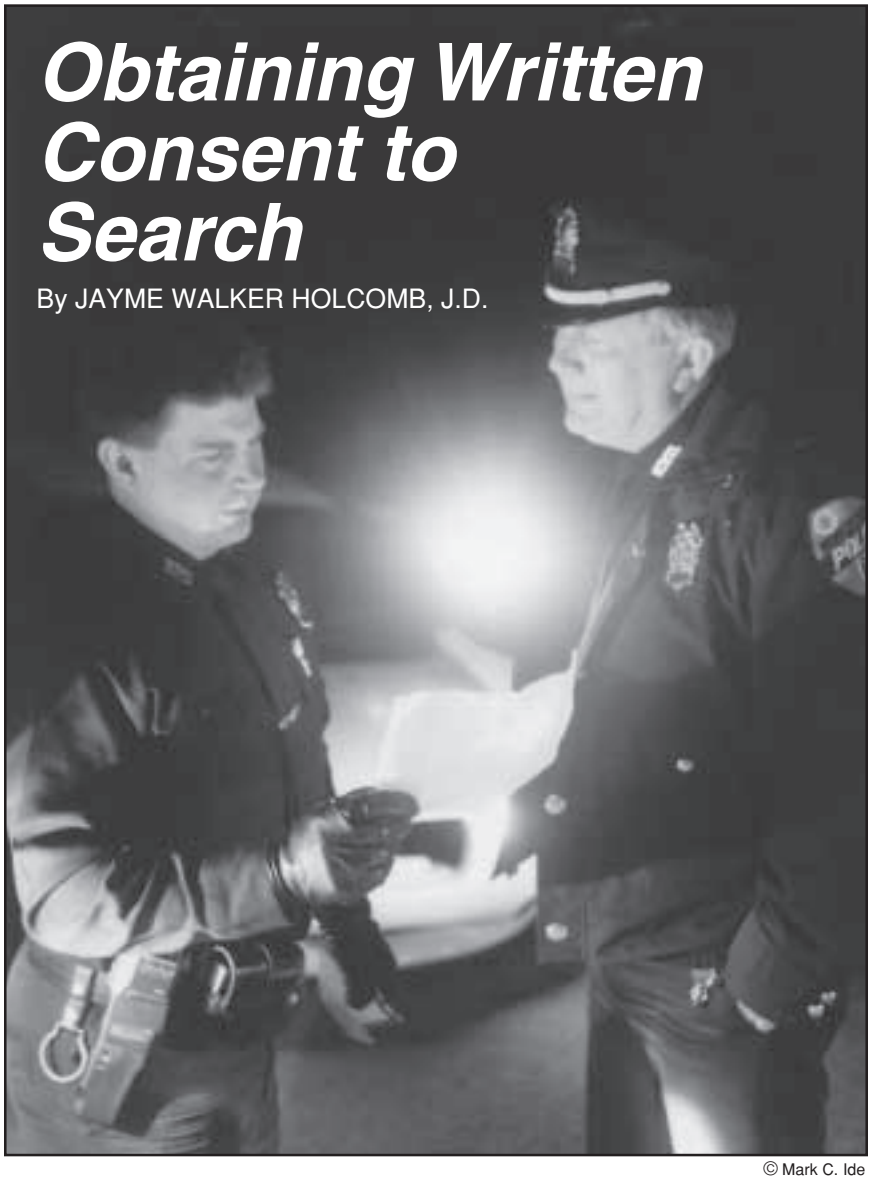
[2] Ibid., *Training Guide for Hate Crime Data Collection,* 59.

[3] The author reached the conclusions in this article by drawing on his 15 years of teaching experience on hate/bias crimes, as well as his 33 years of experience with the Los Angeles County, California, Sheriff's Department.

[4] In some agencies, the first responder is also the lead investigator, while in other agencies the lead investigator is a different officer. For the purpose of this article, the roles of the first responder and the lead investigator are combined and referred to as the investigator.

Obtaining Written Consent to Search

By JAYME WALKER HOLCOMB, J.D.



© Mark C. Ide

The Fourth Amendment preserves the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] It is well settled that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[2] The U.S. Supreme Court has stated that a search conducted pursuant to lawfully given consent is an exception to the warrant and probable cause requirements of the Fourth Amendment.[3]

In *Schenkloth v. Bustamonte*,[4] the U.S. Supreme Court ruled that a court reviewing whether an individual voluntarily consented to a search must consider the totality of the circumstances surrounding the consent. An individual need not provide *written* consent for a search of his or her person or property to a law enforcement officer for a consent search to be valid. Even though a writing is not legally required, law enforcement officers often will ask an individual for written consent to search to provide evidence of voluntariness.

This article considers the particular issues that courts analyze regarding written consent to search. These issues include the evidentiary significance of a written consent to search form, the presentation of a consent to search form to an individual, the impact of a person's refusal to sign a written consent to search, and the content of consent to search forms.

Evidentiary Significance

The government has the burden of proving that an individual voluntarily consented to a search.[5] The presence of a writing reflecting that an individual consented is, therefore, quite significant,[6] and evidence that an individual signed a statement of consent to a search has been found to be a clear indication of voluntariness.[7] The lack of a writing memorializing a consent to search also may be noted by a court,[8] as may the failure of an officer to use an available written consent form.[9] One court has stated, "[o]f course, a written consent to a search is not a legal requirement, but law enforcement officers fail to obtain a written consent when one readily could be obtained at the risk that the government's ability to prove the voluntariness of a consent will be seriously compromised."[10]

The decision by the U.S. Court of Appeals for the Seventh Circuit in *United States v. Duran*[11] is an excellent example of the role a signed written consent can play in a court's analysis. In *Duran*, Cesar Duran's wife, Karen, took a pair of new tennis shoes back to a shoe store to obtain help lacing them. Karen left the shoes with a store employee and went shopping elsewhere in the mall. The store employee discovered three packages of what appeared to be marijuana in the shoes and called the police. The police arrived at the store and determined that the packages did contain marijuana. The police arrested Karen when she returned to the store. The officers also found $3,000, a small amount of cocaine, and drug paraphernalia in her purse. The officers read Karen her *Miranda* warnings and took her to the police station.

At the police station, Karen told the officers where she lived and admitted that her husband sold large quantities of marijuana in the local area. Karen also signed a form consenting to a search of the Duran residence, an old farmhouse on the property, and several outbuildings. The police arrested Cesar after finding 28 pounds of marijuana and a number of weapons during the search.

In considering Cesar's challenge to Karen's consent to search, the *Duran* court specifically pointed to the consent form signed by Karen. The court rejected Cesar's argument that the fact that this was Karen's first arrest should be given weight, noting that the form's language stating that she could refuse to consent and that any evidence discovered could be used against her put her on par with an experienced arrestee in terms of what she needed to know. The court stated, "[t]hat the form contained these warnings, in fact, weighs heavily toward finding that her consent was voluntary."[12]

Signing the Form

Circumstances surrounding the signing of a written consent will be analyzed carefully by a court. Even though an individual signed a consent to search form, the consent to search still may be found invalid. Factors that courts will consider in determining if the consent was voluntary include the characteristics of the subject giving the consent, the environment in which the consent is given, the actions taken or statements made by the subject giving the consent,[13] and the actions taken or statements made by law enforcement officers during the course of asking for consent to search.[14]

The extent to which law enforcement officers maintain a noncoercive environment in which a written consent to search is obtained also is significant.[15] For example, what is said if the individual asks questions or makes statements about the form or while signing it[16] and how many law enforcement officers are present when the form is signed will be factors considered by a court.[17] Moreover, courts also have examined the following factors when deciding if a person has given voluntary written consent: whether the officer ascertained the ability of the individual to read,[18] whether the officer saw the individual read the form,[19] whether the officer read the form out loud to the individual,[20] whether the officer explained the content of the form to the individual,[21] whether there was adequate light in which to read the form,[22] whether there was enough time to read the form,[23] whether the officer accurately translated the form while reading it out loud,[24]

"Officers who obtain written consent to search from an individual should document in detail the facts and circumstances under which the consent was given."

Ms. Holcomb serves as the chief of the Legal Instruction Section, DEA Training Academy.

whether the form adequately indicated that the individual is consenting to the search if it is in another language,[25] whether the individual was allowed to change the language of the form,[26] whether the individual made a phone call prior to signing the form,[27] and whether the form was signed before or after the search occurred.[28]

The 1995 decision of the U.S. Court of Appeals for the Eleventh Circuit in *United States v. Tovar-Rico*[29] is an example of a case in which an individual signed a consent to search form where the search was found invalid. In *Tovar-Rico*, officers followed two persons who had just obtained a substantial amount of cocaine from two undercover officers. The individuals entered an apartment building without carrying anything and were seen leaving apartment 901 a short time later. Neither person carried anything. The individuals returned to the apartment and left 10 to 15 minutes later with a third person.

One individual then removed a large amount of cocaine from the trunk of a car parked at the building and took it inside. An officer observed that individual exit unit 901. Officers arrested all of the individuals involved in the transaction who were around the apartment building and then proceeded to unit 901.

Five officers knocked on the door to unit 901, announced their identity, and requested permission to enter. When Tovar answered the door, the officers quickly entered with weapons drawn and conducted a protective sweep. The officers entered each room of the apartment while Tovar sat at the dining room table. One of the officers asked Tovar for permission to search the entire apartment. The officer told Tovar that she did not have to allow the search, but that if she did not, they would come back with a search warrant. Tovar agreed to the search and signed a written consent form.

The court rejected the argument that there were exigent circumstances that would permit a warrantless entry. The court also cited another case stating that the government does not carry its burden of

© Mark C. Ide

proving that a consent is voluntary by showing that someone merely submitted to a claim of lawful authority. The court found Tovar's consent was involuntary and stated that, "Tovar had already observed officers explore every room in the apartment and could not reasonably have known that she could still refuse a search....We entertain no doubt that Tovar opened the door in response to a 'show of official authority' and cannot be deemed to have consented to the agents' entry or to have voluntarily consented to the search."[30]

In the 1999 case of *United States v. Rodriguez*,[31] the court held that the defendant did not voluntarily consent to a search of his car. Agents in *Rodriguez* obtained a search warrant to search the defendant's residence. Between 10 and 15 agents participated in the execution of the warrant, but no evidence was found during the 3-hour search. At the end of the search, an agent asked the defendant about a car parked in front of the house, which the defendant denied owning. He remained silent even when shown a bill of sale for the vehicle with his name on it.

The agent presented a written consent form printed in English for the defendant to sign. The defendant did not speak English, and, therefore, the form had to be translated into Spanish. The agent then proceeded to literally translate the form as he read it to the defendant. Notably, the agent never had obtained a person's consent to search in Spanish before, and there were Spanish-speaking officers present at the home who may have done a better job in translating. The defendant agreed to sign the consent form. As the agent filled out the form and the defendant was about to sign it, the "defendant asked [the agent] 'whether they [agents] were going to search the vehicle anyway,' to which the latter responded affirmatively."[32] The defendant signed the form. The agents found weapons in the car, which the defendant sought to suppress.

In determining whether the defendant voluntarily consented to the search, the court considered the defendant's age and criminal

history and noted that there was no information in the record regarding the defendant's education, experience, intelligence, or whether he was mentally deficient. The defendant argued that he was not told that he could refuse consent, while the government stated that the consent to search form signed by the defendant advised him of his right to refuse. The court stated that whether the defendant is informed of the right to refuse consent to search is one factor to be taken into account in determining voluntariness, but indicated that the critical issue to be addressed in this case was the agent's ability to accurately translate the consent form.

The court concluded that the defendant had not voluntarily consented to the search of the vehicle. The court stated that the environment created by the agents in the home at the time the defendant's consent was obtained was implicitly coercive. More particularly, the court found it significant that when the agents obtained consent, the defendant was handcuffed, unlawfully seized, separated from the rest of his family while his crying 3-year-old daughter was left alone with one of the 10 to 15 agents in the house, and it was strongly implied that the car would be searched even if he did not consent. At the suppression hearing, the agent was asked to translate the consent form into Spanish as he had on the day in question. The court stated the following with regard to the agent's translation:

> Assuming that the former translation replicated the latter, we find that defendant was ill-advised of his constitutional rights.... The translation was literal and clumsy, almost awkward sounding. While under more relaxed circumstances it would not be implausible to find that [the agent's] translation sufficiently informed defendant about some basic concepts (e.g., his right to refuse consent, his right to consult an attorney), the implicitly coercive environment created by...agents at defendant's home precludes such a finding.[33]

> ***"...officers should be extremely careful in making sure that the language in the form accurately describes what will be searched."***

Refusal to Sign Form

In many cases, an individual will be willing to verbally consent to a search but will refuse to sign a consent to search form. In such cases, as long as the consent to search is voluntary, the verbal consent will be sufficient to allow the search.[34] Significantly, it has been held that "the refusal to execute a written consent form subsequent to a voluntary oral consent does not act as an effective withdrawal of the prior oral consent."[35] In one case, a court held that the prior verbal consent of a suspect was sufficient even though the individual failed to read, but signed, a consent form that had been incorrectly translated into Spanish.[36]

Officers who encounter individuals who refuse to consent to a search in writing but who consent verbally should document their refusal to provide written consent. Additionally, as with any verbal consent to search, officers should carefully document exactly what the person said to the officers to indicate his or her consent. For example, in *United States v. Boukater,*[37] the U.S. Court of Appeals for the Fifth Circuit found that Boukater voluntarily consented to a search of his briefcase. After being advised of his constitutional rights and being told that he was free to leave, Boukater stated that he wanted to know what was going on. The agents advised Boukater that he was suspected of carrying counterfeit bills and was asked if he would consent to a search. Boukater then stated, "It looks like you got me. You can search my bags." After refusing to give written consent, he was asked if he was withdrawing his consent. At that point, one agent stated that Boukater said, "No, go ahead," and the other agent stated that he said, "Well, go ahead. You got me. It's in there."[38]

Form Content

There is no prescribed language that federal courts have held that must be placed into a consent to search form. A written consent to search may be handwritten[39] or be

on a preprinted form. While there is no specific language that must be included in a written consent, the language that is used is extremely important. For example, there is a vast difference between a writing stating, "I have been asked to permit special agents...to search..."[40] and "it has been required of me that I give my consent to a search...."[41] The first of these statements indicates that the individual had a choice in whether to agree to a search, while the latter implies that there was none.

In most situations, officers use a preprinted form when obtaining a written consent. The officer will fill in the particular details on the form relating to the item or location to be searched and the individual consenting to the search. The use of a preprinted form may prevent an officer from inadvertently using potentially coercive language, but using such forms may lead to contested issues related to descriptions of items or property due to a failure to change boilerplate language.[42]

There are a number of standard items included in valid written consent to search forms. First, the form will indicate to whom the individual is giving consent to search, for example, Officer Smith of the Highway Patrol or agents of the Drug Enforcement Administration.[43] Second, the form will identify the item or location that the individual is consenting to be searched, for example, a 1986 blue Ford pickup truck, VA license 123 ABC.[44] Third, the form will state that the individual is voluntarily consenting to the search, for example, "I freely consent to this search"[45] or "I have given this authorization...voluntarily and without threats, promises, pressures, or coercion of any kind."[46] Even though it is well settled that an individual does not have to be informed by an officer of the right to refuse to consent to a search,[47] because courts will consider this as a factor in determining the voluntariness of the consent, many forms include such a statement.[48]

> ***"...the critical issue to be addressed in this case was the agent's ability to accurately translate the consent form."***

Most of the challenges made to the language found in written consent forms concern the scope of the search[49] permitted by the language in the form.[50] For example, in the U.S. Court of Appeals for the Eleventh Circuit decision *United States v. Kapperman,*[51] officers stopped Cervantes' car based upon a reasonable suspicion that the passenger in his car was fugitive Kapperman. After determining that the passenger was Kapperman, the officers asked Cervantes for consent to search his car. Cervantes provided both oral and written consent to search. The police arrested Cervantes after finding cocaine in a suitcase in the trunk.

Appellant Kapperman argued that the consent form signed by Cervantes did not authorize opening the suitcase in the trunk. The consent form authorized officers to search the car and remove "whatever documents or items of property whatsoever, which they deem pertinent to the investigation."[52] The *Kapperman* court found that this language permitted searching within containers in the car, as it would be unlikely that papers and other items would be loosely strewn about the inside of a vehicle. The court also noted that the U.S. Court of Appeals for the Seventh Circuit rejected an identical challenge in *United States v. Covello*[53] and stated that in *Covello*

> [t]he Seventh Circuit rejected a challenge identical to the one presented here. Reviewing a district court opinion that held that an individual's consent to search his car did not include authorization to search luggage found inside of the car, the court reversed, noting that the interpretation of the signed consent form was crucial to the case. The form authorized the agents "to conduct a complete search" of the car, and permitted the searching agents to remove from the vehicle any property contained therein. Thus, the court concluded, the signed consent form authorized the questioned conduct. To bolster its decision, the court evaluated the circumstances surrounding the property owner's decision to consent, concluding that they were consistent

with a complete search of the vehicle.[54]

Challenges by defendants to the language in standardized consent forms are usually unsuccessful. Nonetheless, officers should be extremely careful in making sure that the language in the form accurately describes what will be searched.

Conclusion

Obtaining an individual's consent to search in writing provides substantial evidence that an individual voluntarily consented. However, even though an individual consents to a search in writing, courts still will scrutinize all of the facts surrounding the signing of the consent form when deciding whether, under the totality of the circumstances, the consent was voluntary.

Officers who obtain written consent to search from an individual should document in detail the facts and circumstances under which the consent was given. Officers should pay particular attention to actions and statements made by both the officer and the individual when the form is signed. Similarly, in situations where an individual refuses to sign a written consent to search but verbally consents to a search, officers should document meticulously both what the officer said when asking for consent and what the individual said when giving consent.

Officers also should be familiar with the content of any preprinted consent forms used by their department and any departmental policies related to obtaining consent to search and the use of written consent to search forms. Consent to search forms should be reviewed by department counsel for legal sufficiency, and foreign language consent forms should be reviewed by certified or otherwise qualified interpreters prior to use.[55] Careful attention to the details associated with the use of written consent to search forms will help ensure that the use of the form provides valuable proof of voluntariness, instead of providing a source for defense counsel challenge. ✦

Endnotes

[1] U.S. CONST. Amend. IV.

[2] *Katz v. United States,* 389 U.S. 347, 357 (1967).

[3] *Id.*

[4] 412 U.S. 218 (1973).

[5] *Bumper v. North Carolina,* 391 U.S. 543 (1968).

[6] *United States v. Moreno,* 280 F.3d 898, 901 (8th Cir. 2002).

[7] *United States v. Navarro,* 90 F.3d 1245, 1257 (7th Cir. 1996).

[8] *See United States v. Marc,* 1997 W.L. 129324 (D. Del. 1997).

[9] *United States v. Forbes,* 181 F.3d 1, 8 (1st Cir. 1999).

[10] *United States v. Rodriguez-Diaz,* 161 F. Supp. 2d 627, 631 n.7 (D. Md. 2001).

[11] 957 F.2d 499 (7th Cir. 1992).

[12] *Id.* at 502.

[13] For example, actions, such as signing a consent to search form, volunteering the possession of an apartment key, and showing officers how the key worked, are important. *United States v. Genao*, 281 F.3d 305, 310 (1st Cir. 2002).

[14] *See* J.W. Holcomb, "Consent Searches: Factors Courts Consider in Determining Voluntariness," *FBI Law Enforcement Bulletin*, May 2002, 25-32.

[15] *United States v. Ramirez,* 963 F.2d 693, 704 (5th Cir. 1992); *United States v. Twomey*, 884 F.2d 46, 51 (1st Cir. 1989).

[16] *See, e.g., United States v. Moreno,* 280 F.3d 898, 900 (8th Cir. 2002); *United States v. Saadeh,* 61 F.3d 510, 517 (7th Cir. 1995).

[17] *See, e.g., United States v. Rodriguez,* 68 F. Supp. 2d 104 (D. Puerto Rico 1999).

[18] *See, e.g., United States v. Fryer,* 974 F.2d 813, 820 (7th Cir. 1992).

[19] *See, e.g., United States v. Santurio,* 29 F.2d 550, 558 (10th Cir. 1994)*; United States v. Fryer,* 974 F.2d 813, 820 (7th Cir. 1992).

[20] *See, e.g., United States v. Botello,* 991 F.2d 189, 194 (5th Cir. 1993); *United States v. Fryer,* 974 F.2d 813, 820 (7th Cir. 1992); *United States v. Ramirez,* 963 F.2d 693, 704 (5th Cir. 1992).

[21] *See, e.g., United States v. Murillo,* 255 F.3d 1169, 1172 (9th Cir. 2001); *United States v. Garza,* 118 F.3d 278 (5th Cir. 1997); *United States v. Ramirez,* 963 F.2d 693, 704 (5th Cir. 1992); *United States v. Tibbs,* 49 F. Supp. 2d 47, 54 (D. Mass. 1999).

[22] *See, e.g., United States v. Fryer,* 974 F.2d 813, 820 (7th Cir. 1992).

[23] *See, e.g., United States v. Chaidez,* 906 F.2d 377, 379 (8th Cir. 1990).

[24] *See, e.g., United States v. Iribe,* 11 F.3d 1553, 1555 (10th Cir. 1993); *United States v. Rodriguez,* 68 F. Supp. 2d 104 (D. Puerto Rico 1999).

[25] *See, e.g., United States v. Perez,* 37 F.3d 510, 515 (9th Cir. 1994); *United States v. Jamarillo*, 841 F. Supp. 490 (E.D.N.Y. 1994).

[26] *See, e.g., United States v. Twomey,* 884 F.2d 46 (1st Cir. 1989).

[27] *See, e.g., United States v. Fryer,* 974 F.2d 813, 820 (7th Cir. 1992).

[28] *See, e.g., United States v. Tibbs,* 49 F. Supp. 2d 47, 54 (D. Mass. 1999).

[29] 61 F.3d 1529 (11th Cir. 1995).

[30] *Id.* at 1536.

[31] 68 F. Supp. 2d 104 (D. Puerto Rico 1999).

[32] *Id.* at 108.

[33] *Id.* at 112.

[34] *See, e.g., United States v. Pereira-Munoz*, 59 F.3d 788 (8th Cir. 1995); *United States v. Thompson,* 876 F.2d 1381 (8th Cir. 1989).

[35] *See United States v. Lattimore,* 87 F.3d 647, 650 (4th Cir. 1996)(citing *United States v. Thompson,* 876 F.2d 1381, 1384 (8th Cir. 1989)); *United States v. Castillo,* 866 F.2d 1071, 1081-82 (9th Cir. 1988); *United States v. Boukater*, 409 F.2d 537, 539 (5th Cir. 1969).

[36] *United States v. Garza,* 118 F.3d 278 (5th Cir. 1997).

[37] 409 F.2d 537 (5th Cir. 1969).

[38] *Id.* at 538.

[39] *See, e.g., United States v. Twomey,* 884 F.2d 46 (1st Cir. 1989).

[40] *United States v. Saadeh,* 61 F.3d 510, 517 (7th Cir. 1995).

[41] *United States v. Jamarillo*, 841 F. Supp. 490, 491 (E.D.N.Y. 1994).

[42] *See, e.g., United States v. Ramirez,* 963 F.2d 693, 704 (5th Cir. 1992).

[43] *See, e.g., United States v. Saadeh,* 61 F.3d 510, 517 (7th Cir. 1995).

[44] *See, e.g., United States v. Torres,* 32 F.3d 225, 228 (7th Cir. 1994).

[45] *United States v. Saadeh,* 61 F.3d 510, 517 (7th Cir. 1995).

[46] *United States v. Reeves,* 6 F.3d 660, 661 (9th Cir. 1993).

[47] *See United States v. Drayton,* 536 U.S. 194 (2002).

[48] *See, e.g., United States v. Torres,* 32 F.3d 225 (7th Cir. 1994); *United States v. Reeves,* 6 F.3d 660 (9th Cir. 1993).

[49] For additional information regarding the scope of a suspect's consent to search, *see Florida v. Jimeno,* 500 U.S. 248, 251 (1991), in which the Court stated that "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness–what would the typical reasonable person have understood by the exchange between the officer and the suspect?"

[50] *See, e.g., United States v. Stribling,* 94 F.3d 321 (7th Cir. 1996); *United States v. Torres,* 32 F.3d 225 (7th Cir. 1994); *United States v. Reeves,* 6 F.3d 660 (9th Cir. 1993); *United States v. Covello,* 657 F.2d 151 (7th Cir. 1981).

[51] 764 F.2d 786 (11th Cir. 1985).

[52] *Id.* at 794.

[53] 657 F.2d 151 (7th Cir. 1981).

[54] *United States v. Kapperman,* 764 F.2d 786, 794 (11th Cir. 1985).

[55] *See generally United States v Jamarillo*, 841 F. Supp. 490 (E.D.N.Y. 1994); 28 U.S.C. § 1827 (2002).

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

Wanted: Notable Speeches

The *FBI Law Enforcement Bulletin* seeks transcripts of presentations made by criminal justice professionals for its Notable Speech department. Anyone who has delivered a speech recently and would like to share the information with a wider audience may submit a transcript of the presentation to the *Bulletin* for consideration.

As with article submissions, the *Bulletin* staff will edit the speech for length and clarity, but, realizing that the information was presented orally, maintain as much of the original flavor as possible. Presenters should submit their transcripts typed and double-spaced on 8½- by 11-inch white paper with all pages numbered. When possible, an electronic version of the transcript saved on computer disk should accompany the document. Send the material to:

Editor, *FBI Law Enforcement Bulletin*
FBI Academy
Madison Building,
Room 209
Quantico, VA 22135
telephone: 703-632-1952,
e-mail: leb@fbiacademy.edu

The Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. The *Bulletin* also wants to recognize those situations that transcend the normal rigors of the law enforcement profession.

Deputy Ramage

Deputy Warner

Deputies Devant Ramage and David Warner of the Graves County, Kentucky, Sheriff's Department received a call of an unconscious man in a rural part of Graves County whose breathing had ceased. Due to the large size of the county, the deputies were dispatched because they could respond more quickly than an emergency medical services (EMS) team. Upon arrival, the deputies found an elderly man on the floor of his home. The man was unconscious, not breathing, and lacked a pulse. Deputies Ramage and Warner immediately began CPR. They were able to resuscitate the man prior to the arrival of EMS personnel, who stated that the man probably would not have survived had it not been for the quick response and judgment of the deputies.

Sergeant Tatum

Officer Carter

Responding to a call about a drowned individual, Sergeant Chris Tatum and Officer Debbie Carter of the Waycross, Georgia, Police Department found a small child at the bottom of a pool. Officer Carter entered the pool and retrieved the child. Sergeant Tatum also noticed a male adult at the bottom of the pool and immediately dove in to retrieve the individual who happened to be the child's father. With the assistance of an emergency medical technician, the father was removed from the pool and CPR was started on both individuals. The child was revived and recovered completely. Unfortunately, the child's father could not be revived. The skill and prompt action of Sergeant Tatum and Officer Carter saved the life of the young child and brought a blessing out of a terrible tragedy.

Nominations for the ***Bulletin Notes*** should be based on either the rescue of one or more citizens or arrest(s) made at unusual risk to an officer's safety. Submissions should include a short write-up (maximum of 250 words), a separate photograph of each nominee, and a letter from the department's ranking officer endorsing the nomination. Submissions should be sent to the Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

U.S. Department of Justice
Federal Bureau of Investigation
FBI Law Enforcement Bulletin
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Official Business
Penalty for Private Use $300

Periodicals
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Patch Call

The mission of the University of Vermont Police Services, established as a full-time police agency with statewide authority in 1991, is represented by its patch. The green mountains, overlooking Lake Champlain, speak to the natural beauty and rugged individualism of Vermont and are the namesake for the university. The Latin words represent three keys to the agency's success: excellence, integrity, and service.

The patch of the North Salt Lake, Utah, Police Department depicts the year that Utah became a state. The center of the patch features a beehive, which is the state symbol for industry. The city of North Salt Lake was incorporated in 1946. It has a population of 8,500 and currently is served by 11 sworn police officers.