August 2001
Volume 70
Number 8

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

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.

Internet Address
leb@fbiacademy.edu

Cover Photo
© Adobe Image Library

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

FBI Law Enforcement Bulletin

Features

Departments

ISSN 0014-5688 USPS 383-310

Subtle Skills for Building Rapport

Using Neuro-Linguistic Programming in the Interview Room

By VINCENT A. SANDOVAL, M.A., and SUSAN H. ADAMS, M.A.

Mark Hamilton, a seasoned detective, slowly opens the door to the interview room. The witness to the drive-by shooting sits leaning forward in a chair with her head in her hands. Normally, Mark bellows out his introduction to establish immediate control, but not this time. He enters the room without speaking, pulls a chair close to the witness, leans forward, and, in a barely audible voice, slowly begins, "I'm Detective Mark Hamilton...."

Detective Hamilton is using techniques from Neuro-Linguistic Programming, a communication model with a name he might not even recognize. Yet, his years of interviewing have taught him the techniques. To establish rapport with this witness, Detective Hamilton knows that he needs to match her nonverbal behavior, or kinesics, by sitting down and leaning forward. When the witness begins to talk, Detective Hamilton listens carefully to her words and intentionally uses similar language. He also pays close attention to *how* she talks and matches her paralanguage (speech rate, volume, and pitch). In so doing, Detective Hamilton builds rapport with the witness and, hence, increases his chances of gathering pertinent information during the interview.

Detective Hamilton and other experienced investigators recognize the crucial role that rapport plays in an interview. Derived from the French verb *rapporter* meaning "to bring back," the English word *rapport* refers to a relationship or communication characterized by harmony.[1] With this in mind, the need for rapport applies to all interviews, but especially to those

involving a victim or witness who has experienced physical or psychological abuse. The interviewer's task is similar to that of the clinical psychologist, who must initially develop a personal bond with his client before intimate feelings are shared.[2] Thus, investigators can enhance their rapport-building skills by examining some practical recommendations derived from the behavior modification technique known as *Neuro-Linguistic Programming.*

UNDERSTANDING NEURO-LINGUISTIC PROGRAMMING

In the early 1970s, John Grinder, an assistant professor of linguistics at the University of California in Santa Cruz, and Richard Bandler, a student of psychology, identified patterns used by successful therapists. They packaged them in a way that could be passed on to others through a model now known as Neuro-Linguistic Programming, or NLP.[3]

Neuro-Linguistic Programming embraces three simple concepts. First, the *neuro* part of NLP recognizes the fundamental idea that all human behavior originates from neurological processes, which include seeing, hearing, smelling, tasting, and feeling. In essence, people experience the world through their senses. Second, they communicate their experiences verbally, through language;[4] therefore, the *linguistic* part of NLP refers to this use of language to communicate thoughts. Finally, the *programming* aspect of NLP recognizes that individuals choose to organize their ideas and actions to produce results. Each person also decides how to organize these ideas in a specific manner.[5]

The NLP founders theorize that people think differently and that these differences correspond to individual programming or processing systems. People use their senses outwardly to perceive the world and inwardly to "re-present" this experience to themselves. In NLP, representational systems denote ways people take in, store, and code information in their minds.[6] These systems pertain to the principal human senses—seeing (visual), hearing (auditory), and feeling (kinesthetic). To a lesser degree, they involve tasting (gustatory) and smelling (olfactory). People constantly see, hear, and feel whatever transpires around them. When individuals relate these experiences to others, they mentally access the sights, sounds, or feelings associated with these experiences and communicate them through their predominant representational system.[7]

Special Agent Sandoval is an instructor in the Law Enforcement Communication Unit at the FBI Academy.

Special Agent Adams is an instructor in the Law Enforcement Communication Unit at the FBI Academy.

BUILDING RAPPORT WITH NLP

Enhancing communication and, hence, building rapport represents the most applicable aspect of NLP to investigators. The ability to communicate effectively and build rapport stands as one of the major contributors to a police officer's success in dealing with the public.[8] In an interview setting, effective communication involves the interviewer's skill in establishing rapport through specific actions and words, thereby building trust and encouraging the interviewee to provide information.

Others besides successful law enforcement interviewers have found NLP techniques helpful in rapport building. For example,

some medical hypnotists use the concept of "matching" with highly resistant clients.[9] By simply conforming their nonverbal behavior to that of each client, by using language from the client's preferred representational system (visual, auditory, or kinesthetic), and by matching the client's volume, tone, and rate of speech (paralanguage), they often can overcome the client's reluctance to communicate.

When interviewers intentionally align themselves with a witness or suspect through these matching or mirroring techniques, the interviewee is more inclined to respond to the interviewer and subsequently provide information. As one researcher points out, "people like people who are like themselves."[10] Once interviewers establish rapport, barriers disappear, trust grows, and an exchange of information follows. To achieve these results, interviewers should match or "mirror" the interviewee's kinesics, language, and paralanguage.

Building Rapport by Matching Kinesics

Matching another person's body language or kinesics probably is the easiest and most obvious technique. Kinesic behavior typically includes gestures, posture, and movements of the body, such as the hands, arms, feet, and legs.[11] However, a difference exists between mimicry and matching. Interviewers should match another person's body language with subtlety and caution; otherwise, the person easily could become offended. People who have developed rapport tend to match each other in posture and gestures. For example, individuals conversing together often adopt the same posture. Like partners in a dance, they respond and mirror each other's movements with movements of their own, engaging in mutual responsive actions.[12]

Detective Hamilton employs the kinesics aspect of NLP in his interview. When he enters the interview room, he immediately notices the witness' posture and the position of her hands. He notes that she is leaning forward with her head down. Her posture and the position of her head speak volumes.

> ***"Once interviewers establish rapport, barriers disappear, trust grows, and an exchange of information follows."***

As Detective Hamilton introduces himself, he pulls his chair close to the witness and, just like her, leans forward in his chair with his hands in front of him. As the witness begins to open up and speak about what she has seen, her nonverbal behavior gradually follows suit, as she opens herself up by sitting back. Eventually, as her trust in Detective Hamilton grows, she feels comfortable enough to relax. She realigns her posture by sitting up and facing Detective Hamilton. Through each succeeding change in her body language, Detective Hamilton matches her behavior, thereby lending credence to the belief that the deeper the rapport has been built between two people, the closer the matching of body language.

Building Rapport by Matching Language

Because people use language to communicate thoughts, the words they choose reflect the way they think. When relating experiences, an individual uses the visual, auditory, or kinesthetic representational system to identify these experiences and communicate them to others. For example, a person whose predominant representational system is visual will say phrases, such as "I see what you mean," "that looks good to me," "we see eye to eye," or "I get the picture." On the other hand, a person whose preference is auditory will use language, such as "something tells me...," "that rings a bell," "we're on the same wave length," or "that sounds okay to me." Finally, a person who is kinesthetic or "feeling" oriented will make statements, such as "I'll get in touch with you," "how does that grab you?," "you don't have to get pushy," or "how do you think I feel?"[13]

Successful investigators listen closely to the choice of words witnesses and suspects use. Then, they conform their language to match the interviewee, using similar visual, auditory, or kinesthetic phrases.

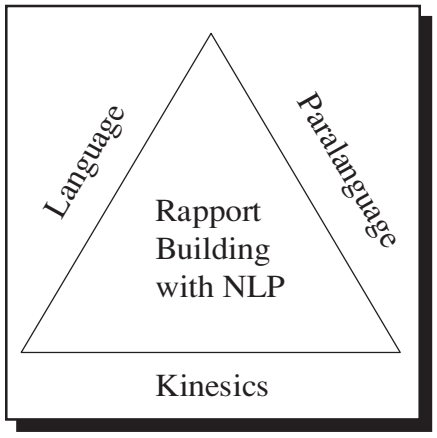
When Detective Hamilton's drive-by shooting witness finally begins to talk, she describes her situation with phrases, such as "tremendous pressure," "I feel like I'm

going to pieces," and "I can't come to grips with what's happening." The detective responds to the witness' account by matching her words. When she speaks of the "tremendous pressure," he explains ways to relieve the "pressure." He continues to use kinesthetic phrases, such as "take this load off your shoulders," to communicate in her preferred representational system.

Because individuals process information in different ways, through distinct representational systems, the investigator often acquires valuable insight into the interviewee's personal preference by paying close attention to the interviewee's eye movements. According to NLP, eye movements, referred to as "eye-accessing cues,"[14] reflect the manner in which an individual processes data. Therefore, the eyes move in specified directions, depending upon the person's preferred mode of thinking. The founders of NLP concluded that eye movements reflect whether the person has a visual preference (thinks in terms of pictures), an auditory preference ("hears" sounds), or a kinesthetic preference (feels or experiences emotion) to process information.[15]

Typically, individuals move their eyes up at an angle as they remember a picture. Some people look directly to the side, which indicates that they are using the auditory mode to recall something that they probably heard before. Finally, individuals who look down at an angle appeal to kinesthetic sensations as they recollect what they felt or experienced.[16]

If an investigator observes that a witness consistently looks up at an angle, particularly when responding to questions that require recall, the interviewer can conclude, with a measurable degree of confidence, that the person is "seeing" a picture while remembering information. In NLP terms, this individual's preferred representational system is visual. The investigator can facilitate the witness' recollection of events



by encouraging this visual recall through such phrases as "how did it look to you?" or "show me what you mean." If the witness looks to the side when asked a question concerning what the person saw, the investigator can encourage the witness to remember by using questions designed to stimulate auditory recall, such as "tell me what you heard" or "how did it sound to you?" Finally, if the witness looks down at an angle when asked a question by the investigator, this could indicate that the person has a kinesthetic preference. Therefore, the investigator can choose phrases that underscore the witness' feelings or emotions, such as "how did all of this feel to you?" or "can you get a handle on what took place?" By closely monitoring the movements of a person's eyes and aligning questions in accordance with the interviewee's observed preferences, investigators can build rapport, thereby enhancing communication between themselves and the people they interview. While NLP practitioners cite a direct neurological connection between eye movements and representational systems,[17] other researchers recognize the need for additional empirical studies.[18] Currently, investigators use interviewees' eye movements as another possible indicator of their preferred manner of communicating.

Building Rapport by Matching Paralanguage

Matching another person's speech patterns, or paralanguage, constitutes the final, and perhaps most effective, way to establish rapport. Paralanguage involves how a person says something or the rate, volume, and pitch of a person's speech. One researcher goes so far as to say that matching the other person's voice tone or tempo is the best way to establish rapport in the business world.[19] What may hold true in the business realm applies in the interview setting as well. Individuals can speak fast or slow, with or without pauses. They can talk in a loud or soft volume and in a high or low pitch. However, most people are unaware of their own speech rate or vocal tones. In fact, investigators do not have to match a person's voice exactly, just close

enough to encourage that individual to feel understood.[20]

In the interview setting, slowing the rate of speech to correspond with the pace of a halting witness allows for recall and communication at that person's pace. By the same token, if a witness speaks with more volume and at a quick rate, the investigator should try to match the person's animated and expressive manner of speech. By listening carefully and paying close attention to *how* people speak, investigators can, in NLP terms, get "in sync" with people by matching their paralanguage.

Experienced investigators continually employ this technique, usually without even thinking about the mechanics or the process involved. Detective Hamilton also uses this aspect of NLP in his interview.

The drive-by shooting witness speaks slowly, as if searching for the right words. Detective Hamilton slows the rate of his speech, giving ample time for the witness to get her point across without feeling rushed. He lowers his voice to match her soft volume and refrains from the urge to interrupt her. As the witness becomes more excitable, speeding up her speech rate and increasing her volume, Detective Hamilton increases his rate and volume as he attempts to mirror her. In so doing, he demonstrates to the witness that he is interested in her as an individual, and this allows her to communicate what she experienced in a way that is comfortable for her.

CONCLUSION

Detective Mark Hamilton's witness begins to feel support and understanding from the interviewer, who continues to match her kinesics, language, and paralanguage. When he sees her consistently looking down to her right, he realizes that she may be processing information on the kinesthetic level and encourages her to talk about her feelings. Slowly, she begins to trust Detective Hamilton.

Unbeknown to the witness, Detective Hamilton had been matching her in specified ways until she finally felt secure enough to provide full details of the drive-by shooter and his vehicle. As a result, the witness' emotional need was met and, from Detective Hamilton's perspective, the interview was a success.

> ***"Successful investigators listen closely to the choice of words witnesses and suspects use."***

This scenario illustrates the importance of carefully observing how witnesses and suspects communicate through nonverbal, verbal, and vocal means. Neuro-Linguistic Programming is not a new concept nor used rarely. In fact, most successful interviewers employ some variation of it to gain rapport. However, by being conscious of the process and the benefits associated with NLP, interviewers can use these techniques to their advantage. By matching interviewees' nonverbal behavior, the manner in which they say something, and even their choice of words, interviewers can increase rapport and enhance communication. As a result, the potential for gaining crucial information needed to help resolve investigations improves significantly. ✦

Endnotes

[1] Genie Z. Laborde, *Influencing with Integrity* (Palo Alto, CA: Syntony Publishing, 1987), 27.

[2] Ronald P. Fisher and Edward R. Geiselman, *Memory-Enhancing Techniques for Investigative Interviewing*, (Springfield, IL: Charles C. Thomas Publisher, 1992), 22.

[3] John O'Connor and John Seymour, *Introducing Neuro-Linguistic Programming* (London, England: Harper Collins Publishers, 1990), 2.

[4] Ibid., 3.

[5] Ibid., 3.

[6] Ibid., 26.

[7] Richard Bandler and John Grinder, *Frogs Into Princes* (Moab, UT: Real People Press, 1979), 5.

[8] P.B. Kincade, "Are You Both Talking the Same Language?" *Journal of California Law Enforcement* 20: 81.

[9] Ibid., 19.

[10] Jerry Richardson, *The Magic of Rapport, How You Can Gain Personal Power in Any Situation* (Cupertine, CA: Meta Publications, 1987), 21.

[11] Judith A. Hall and Mark L. Knapp, *Nonverbal Communication in Human Interaction* (Fort Worth, TX: Harcourt Brace Jovanovich College Publishers, 1992), 14.

[12] Supra note 3, 19.

[13] Supra note 7, 83.

[14] Supra note 7, 35.

[15] Supra note 7, 25.

[16] Supra note 7, 25.

[17] Supra note 7.

[18] Aldert Vrij and Shara K. Lochun, "Neuro-Linguistic Programming and the Police: Worthwhile or Not?" *Journal of Police and Criminal Psychology* 12, no. 1 (1997).

[19] Supra note 1, 30.

[20] Supra note 1, 31.

Law Enforcement Web Sites
New Utility for a New Era

By Clyde B. Eisenberg, M.S., and Brandon Porter

If law enforcement administrators were asked 10 years ago what role they thought the Internet would play in their agency's operation in the future, the response may have been "what's the Internet?" This once obscure medium, originally designed for researchers to communicate more effectively, has evolved into a communications staple for households and businesses. Recent surveys indicate that more than 153 million Americans currently use the Internet.[1]

The Law Enforcement Web Site Evolves

While most historians measure time in decades or centuries, the evolution of law enforcement's involvement with the Internet is only a few years old. One part of a police department's role in society is to provide various types of information to its citizens. For many years, law enforcement agencies have relied on traditional means of disseminating information. These standard proven methods include public service spots that appear on network and public access cable television, in newspaper articles, at displays at local fairs and expos, and in an agency's annual report. With the advent of the law enforcement Web site, agencies now can add a valuable information resource and public relations tool to that list. Even those individuals who do not own a computer or have Internet service usually can get access at their workplace, local libraries, or other nonprofit public resources. In addition to the public relations benefits, agencies can garner widespread utility from a well-crafted Web site, which now can include information ranging from crime statistics to employment opportunities.

Going On-line with a Web Site

Regardless of an agency's size, it must follow several basic steps when creating a Web site. First, an agency must identify and understand what resources are available to it in the process. When developing new sites, agencies should remember that they should custom design their Web pages to meet their specific requirements. An agency must select a host

server and register a domain name—essentially the Internet address of the organization (e.g., *www.youragency.org)*. Agencies can register their domain names with the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization that coordinates the assignment of Internet domain names. Agencies interested in registering a domain name or seeking Web site hosting arrangements can review a list of companies qualified to register domain names and provide Web site registration services within the ICANN Web site. Registering a domain name costs approximately $50 for a 2-year registration, but many packages or service bundles are available through ICANN-accredited domain name registrars.

A host is an Internet Service Provider (ISP), either publicly or privately owned, which provides a link between an agency's Web site and the Internet for little or no fee. The cost of using a private host can range from as little as $20 to as much as several thousand dollars per month, based on the size of the Web site and the amount of traffic it transmits and receives. In Florida, the State's Attorney General's Office provides free hosting to the Internet for law enforcement agencies.

A Web site can be as simple as a single page, or it may contain several hundred pages, depending on the scope of the information offered. When first creating a Web site, an agency must decide the purpose of the site. Will they use it simply as a public relations tool, merely highlighting various facets of the agency? Will it be self-contained or offer additional resource links? Will it provide interactive services to its visitors?

For those agencies that need outside assistance to develop and create a Web site, a plethora of companies exist that offer these services for a fee, which can range from several hundred to several thousand dollars, depending on the size of the site and the various options selected. However, because small Web sites are relatively easy to create, in-house personnel with above-average computer skills often can maintain the agency's site. Agencies do not require special software for basic Web site creations because most popular browsers, and even some word processing software, include a composer to create basic Web pages. However, to produce more advanced Web sites, agencies usually will need specialized software.

"A Web site can be as simple as a single page, or it may contain several hundred pages, depending on the scope of the information offered."

Web sites requiring such specialized software may offer interactive services that derive information from the agency's computer databases. This software, referred to as Internet Commerce Enabler (ICE) software, serves two major purposes. First, it acts as a firewall, allowing only certain information to enter into the site and restricting what information users can retrieve. Due to recent publicized hackings into well-known Web sites and the potential damage such an intrusion can cause, this product becomes essential when managing public access to an agency's data. ICE also converts information from an agency's database into Hyper Text Markup Language, commonly referred to as HTML.[2]

One Agency's Experience

In 1994, the Hillsborough County Sheriff's Office (HCSO) in Tampa, Florida, launched its first Web site. At its inception, the site consisted of only a few pages, limited pictures, and some information about the agency. The first venture into this new medium proved a learning experience for the HCSO; however, neither the agency nor the public gleaned much utility from this site. In 1998, HCSO management realized that having a Web site provided great potential, which led the way to a revision of the old site. HCSO wanted to furnish timely information about how the agency serves the public (e.g., various programs, agency organizational charts, location of departments) and to provide a utility for the agency and the Web site visitors (e.g., crime statistics, history, on-line forms).

Additionally, the update added state-of-the-art features to the site, allowing greater access and ease

of use. For example, the HCSO Detention Department receives hundreds of calls every day inquiring about the status of the inmates housed in the county correctional system. The new Web site now interfaces with the HCSO's mainframe computer and, because the arrest data is public information, anyone can access the information by querying either a name or a booking number.

Other law enforcement agencies also have gone on-line with inmate information. In March 2000, the Los Angeles County, California, Sheriff's Department (LASD) went on-line allowing anyone with Internet access to search the department's database of arrest records, including the names and dates of births of individuals arrested in the last 30 days, along with the charges, bail amounts, and court dates. Additionally, the LASD database includes information on the 20,000 inmates in custody and the 2,400 inmates in community-based programs.[3]

The HCSO warrants section currently has more than 90,000 active warrants, which also are public information and accessible via the Web site. Previously, the agency handled only wanted-person inquiries from citizens, private investigators, or businesses conducting pre-employment screening in person at the records section of the agency. These advances in the HCSO site have proved useful to the agency by reducing the number of walk-in requests. Additionally, those individuals or businesses seeking information benefit by receiving more timely, convenient information.

Law enforcement public information officers (PIOs) often spend a great deal of their time working with reporters. A large agency typically will have one or two full-time PIOs. The HCSO Public Information Office handles approximately 1,200 requests from the media and the public per month. By placing newsworthy press releases on a continually updated special press release Web page, the HCSO has significantly reduced the telephone inquiries to its public information office. Additionally, this special Web page provides timely information to some smaller news agencies that may not have full-time reporters. At the HCSO, most calls from the news media regard traffic conditions, particularly during the morning and afternoon rush hours, which represent some of the busiest times in the communications section that handles those inquiries. To address this problem, the HCSO Web site has interfaced a traffic advisory Web page with its computer-aided dispatch system. Television and radio stations, citizens, and any other interested parties can visit that page to view real-time dispatch information regarding vehicular accidents, detours, and road obstructions. The display indicates

Web Site Resources

- Nielsen Net ratings, available at *www.nielsennetratings.com*, offers information on Internet usage in the United States and worldwide.
- The Internet Corporation for Assigned Names and Numbers, available at *www.icann.org*, is one of the technical coordinating bodies for the assigning of domain names and numbers for the Internet.
- Officer.com, available at *www.officer.com*, provides a comprehensive, alphabetized list of law enforcement agency Web sites.
- Hillsborough County, Florida, Sheriff's Office, available at *www.hcso.tampa.fl.us*.
- Los Angeles County, California, Sheriff's Department, available at *www.lasd.org*.
- Riverside County, California, Sheriff's Department, available at *www.co.riverside.ca.us/sheriff/*.

the location of the problem and advises when an HCSO unit is en route or arrives at the scene. The HCSO Web site also allows citizens to view pictures of wanted individuals, crime statistics, and upcoming events involving the office. Additionally, the HCSO Community-Oriented Policing Program provides residents with up-to-date information on particular activities in their community.

Currently, the HCSO Web site contains 800 linked pages and receives a daily average of 40,000 hits. Visitors also can e-mail comments or questions on the site to the HCSO Web site administrator, who responds to all legitimate e-mails in a timely manner.

The HCSO started an on-line store offering T-shirts and hats for sale. Further, HCSO has created a special secure section, accessed by a password, which allows its employees access to information, such as the list of available off-duty employment jobs and recent departmentwide memos and training bulletins.

> **"...in-house personnel with above-average computer skills often can maintain the agency's site."**

Advanced Utility to an Agency

As the information technology field grows, law enforcement agencies will continue to find new ways to integrate their mission with the Internet. For the last several years, the Riverside County, California, Sheriff's Office has allowed citizens to file reports on-line.

To file a report on-line with the Riverside County Sheriff's Office, a complainant can access the Riverside Sheriff's Office Web site, click on "Crime Report Form," and complete the basic information on a user-friendly form. The complainant will receive an acknowledgment within 3 days, via e-mail, and the assigned case number. The department has limited such on-line reporting to property crimes and miscellaneous occurrences and does not allow a complainant to file on-line if the crime involved known suspects, violence of any kind, or if it required officers to collect physical evidence at the scene. Although this agency characterized the practice as a good learning experience, they consistently have received only a few on-line reports per month.

The FBI National Executive Institute Associates recently conducted a survey of agencies with more than 500 officers that had Web sites. The results of this survey yielded valuable information regarding a variety of Web site uses by law enforcement. Of the 68 agencies that responded to the survey, 27 percent provided sexual offender information, 9 percent offered accident report information, and 18 percent allowed individuals to file reports on-line.[4] These results reveal only a small percentage of the effective uses of Web sites for law enforcement.

Conclusion

Web site technology has advanced both extensively and rapidly. Daily improvements to capabilities, such as video, audio, and general accessibility, significantly increase the potential uses a Web site can offer law enforcement. As this technology continues to advance, the future utility of a Web site virtually is unlimited, given the collective imagination of an agency's members, and the vital input of the public it serves.

By developing and maintaining an informative Web site, an agency, as well as the public it serves, can benefit by conserving time and resources. More important, numerous categories of users would gain valuable, free information quickly and with minimal cost to the community. ✦

Endnotes

[1] See, *http://www.nielsonnetratings.com*; accessed January 23, 2001.

[2] HTML is the computer language of the Internet-recognized Web browsers.

[3] "Los Angeles Sheriff Puts Inmate Information On-line," *Government Technology* vol. 13, no. 8 (June 2000): 11.

[4] E. Tully, " The Present and Future Use of the Internet by Law Enforcement-Part One," *National Executive Institute Associates Research Projects On-line*, June 2000; *www.neiassociates.org*; accessed January 22, 2001.

Sergeant Eisenberg serves with the Hillsborough County, Florida, Sheriff's Office.

Mr. Porter is a software specialist in the Data Operations Bureau of the Hillsborough County, Florida, Sheriff's Office.

Making Computer Crime Count

By MARC GOODMAN

Does computer crime pose a serious threat to America's national security? Recent highly publicized computer virus attacks have shown that computer crime has become an increasing problem. Unfortunately, the absence of a standard definition for computer crime, a lack of reliable criminal statistics on the problem, and significant underreporting of the threat pose vexing challenges for police agencies.

Sensational headlines, such as "Nation Faces Grave Danger of Electronic Pearl Harbor,"[1] "Internet Paralyzed by Hackers,"[2] "Computer Crime Costs Billions,"[3] have become common. Law enforcement organizations cannot determine exactly how many computer crimes occur each year. No agreed-upon national or international definition of terms, such as computer crime, high-tech crime, or information technology crime, exists. Thus, as a class of criminal activities, computer crime is unique in its position as a crime without a definition, which prevents police organizations from accurately assessing the nature and scope of the problem.

Internationally, legislative bodies define criminal offenses in penal codes. Crimes, such as murder, rape, and aggravated assault, all suggest similar meanings to law enforcement professionals around the world. But what constitutes a computer crime? The term covers a wide range of offenses. For example, if a commercial burglary occurs and a thief steals a computer, does this indicate a computer crime

or merely another burglary? Does copying a friend's program disks constitute a computer crime? The answer to each of these questions may depend on various jurisdictions.[4]

The United States Department of Justice (DOJ) has defined computer crime as "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution."[5] Some experts have suggested that DOJ's definition could encompass a series of crimes that have nothing to do with computers. For example, if an auto theft investigation required a detective to use "knowledge of computer technology" to investigate a vehicle's identification number (VIN) in a states's department of motor vehicle database, under DOJ guidelines, auto theft could be classified as a computer crime. While the example may stretch the boundaries of logic, it demonstrates the difficulties inherent in attempting to describe and classify computer criminality.

Over the past 15 years, several international organizations, such as the United Nations, the Organization of Economic Cooperation and Development (OECD), the Council of Europe, the G-8,[6] and Interpol, all have worked to combat the problem of computer crime.[7] These organizations have provided guidance in understanding this problem. Yet, despite their efforts, no single definition of computer crime has emerged that the majority of criminal justice professionals use. Although many state and federal laws define terms, such as "unauthorized access to a computer system" and "computer sabotage," neither Title 18 nor any of the state penal codes provide a definition for the term computer crime.

> ***"To decrease the incidence of computer crime, law enforcement agencies must work with private organizations...."***

Mr. Goodman, former head of the Los Angeles, California, Police Department's Internet Unit, also has served as a law enforcement policy advisor in the U.S. Department of the Treasury.

Defining criminal phenomena is important because it allows police officers, detectives, prosecutors, and judges to speak intelligently about a given criminal offense. Furthermore, generally accepted definitions facilitate the aggregation of statistics, which law enforcement can analyze to reveal previously undiscovered criminal threats and patterns.

Benefits of Reporting Computer Crime Statistics

Crime statistics serve an important role in law enforcement. First, they allow for the appropriate allocation of very limited resources. For example, if a community suffered a 73 percent increase in the number of sexual assaults, police administrators immediately would take steps to address the problem by adding more rape investigators, extra patrol in the specific area, and increased community awareness projects. The aggregation of crime data allows police to formulate a response to a problem. Anecdotal evidence suggests that computer crime presents a growing problem for the public, police, and governments, all who rely on crime statistics for the development of their criminal justice policies and the allocation of extremely limited resources. For police to respond successfully to these crimes in the future, they must increase the resources their departments currently dedicate to the problem—a difficult task.

Agencies must justify training, equipment, and personnel costs necessary to create a computer-competent police force. How can law enforcement managers justify these costs to community leaders without appropriate data to substantiate their claims? Police must document the problem with factual

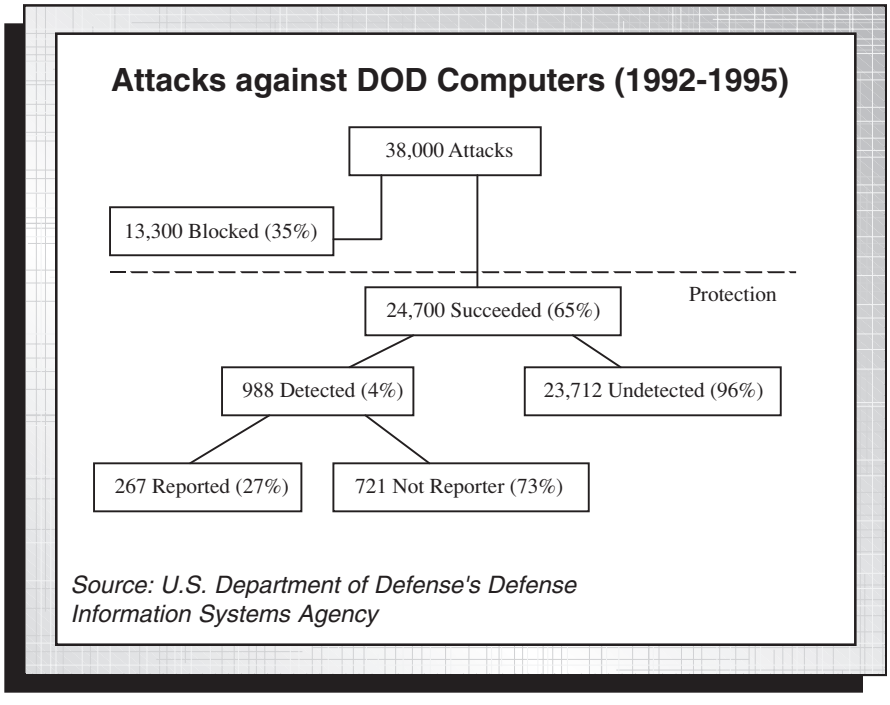
data not information based on media sensationalism or a few notorious attacks.

Second, accurate statistics on computer crime are important for public safety reasons. Computer crimes not only affect corporations but hospitals, airports, and emergency dispatch systems as well. Furthermore, surveys have indicated that many individuals fear for their safety in the on-line world and worry about criminal victimization.[8]

Businesses and individuals rely on law enforcement crime statistics when making important decisions about their safety. Many citizens contact a local police station prior to the purchase of a home in a particular neighborhood to inquire about the number of burglaries and violent crimes in the area. Just as these data provide important information for communities in the "real world," the same is true in cyberspace. For individuals and organizations to intelligently assess their level of risk, agencies must provide accurate data about criminal threats. Access to reliable and timely computer crime statistics allows individuals to determine their own probability of victimization and the threat level they face and helps them begin to estimate probable recovery costs.[9] Law enforcement organizations traditionally have taken a leading role in providing crime data and crime prevention education to the public, which now should be updated to include duties in cyberspace.

Crime statistics facilitate benchmarking and analysis of crime trends. Crime analysts use criminal statistics to spot emerging trends and unique modi operandi. Patrol officers and detectives use this data to prevent future crimes and to apprehend offenders. Therefore, to count computer crime, a general agreement on what constitutes a computer crime must exist.

In many police departments, detectives often compile and report crime data. Thus, homicide detectives count the number of murders, sexual assault investigators examine the number of rapes, and auto detectives count car thefts. Computer crime, on the other hand, comprises such an ill-defined list of offenses that various units within a police department usually keep the related data separately, if they keep them at all. For example, the child abuse unit likely would maintain child pornography arrest data and identify the crime as the sexual exploitation of a minor. A police department's economic crimes unit might recap an Internet fraud scam as a simple fraud, and an agency's assault unit might count an on-line stalking case as a criminal threat. Because most police organizations do not have a cohesive entity that measures offenses where criminals either criminally target a computer or use one to perpetrate a crime, accurate statistics remain difficult to obtain.



The Underreporting Problem

Generally, crime statistics can provide approximations for criminal activity. Usually, people accurately report serious crimes, such as homicide, armed robbery, vehicle theft, and major assaults. Many other criminal offenses, however, remain significantly underreported.

Police always have dealt with some underreporting of crime. But,

new evidence suggests that computer crime may be the most underreported form of criminal behavior because the victim of a computer crime often remains unaware that an offense has even taken place. Sophisticated technologies, the immense size and storage capacities of computer networks, and the often global distribution of an organization's information assets increase the difficulty of detecting computer crime. Thus, the vast majority of individuals and organizations do not realize when they have suffered a computer intrusion or related loss at the hands of a criminal hacker.

The U.S. Department of Defense's (DoD) Defense Information Systems Agency (DISA) has completed in-depth research on computer crime. From 1992 to 1995, DISA attacked their own DoD computer systems using software available on the Internet. System administrators did not detect the majority of attacks against DoD computers. Of the 38,000 attacks perpetrated, 96 percent of the successful attacks went undetected. Furthermore, of the detected attacks, only 27 percent were reported. Thus, approximately 1 in 140 attacks were both detected and reported, representing only 0.7 percent of the total. If the detection and reporting of computer crime is less than 1 percent in the nation's military systems, how often might these crimes go unreported when the intended victim is an individual or a small business owner?

Convincing victims who have suffered a loss to report the crime to police constitutes another hurdle facing law enforcement agencies. Surprisingly, many individuals, network administrators, and corporate managers do not realize that attacks against their networks constitute a crime. Worse, many victims who understand that a crime has taken place may deliberately keep these facts from the police. Victims may have serious doubts about the capacity of the police to handle computer crime incidents in an efficient, timely, and confidential manner. [10] These concerns are true particularly among large corporations who fear damage to their reputation or, worse, their bottom line.

> ***"...accurate statistics on computer crime are important for public safety reasons."***

In banking and financial sectors, reputation is everything. Information that a criminal has infiltrated a bank's computers and accounts potentially could drive thousands of customers to its competitors.

Businesses suffer a variety of losses, both tangible and intangible when hackers attack them. They can lose hundreds of millions of dollars of value, brand equity, and corporate reputation when a business falls prey to a hacker.[11] Most of the companies that suffer Web attacks see their stock prices fall.[12] Furthermore, in recent denial of service attacks, for example, the Yankee Research Group estimated that direct revenue losses due to blocked online transactions and the need for security infrastructure upgrades exceed $1 billion.[13] Because of the high price of victimization, most companies would not want to involve law enforcement and risk a very public arrest or trial attesting to the organization's security and business failings.

The difficulties in computer crime detection and the challenges posed by the reluctance of businesses to admit victimization might demonstrate the underestimation of all statistics related to cybercrimes. However, some less reputable computer security consulting companies may overestimate computer crime and security problems to scare business leaders who, they hope, will turn to these organizations for consulting services and support.

An annual report compiled by the Computer Security Institute in San Francisco, California, and the FBI provides a variety of statistics on computer crime by surveying computer security practitioners in both the private and public sectors.[14] The anonymity offered to survey respondents may contribute to the accuracy of their data. However, the report does not directly poll law enforcement organizations about the number of computer crimes reported to police. Many experts believe that such a task should be carried out by the government, but to date, no single governmental body maintains responsibility for

asking police forces about the prevalence of computer crimes reported and investigated.

The Development of a Definition

The development of a simple, widely agreed-upon definition of computer crime among law enforcement may form the first step in counting computer crimes. This definition would help police to communicate more effectively about these offenses and begin to accurately assess the prevalence of criminal victimization.

The earliest work in computer security provides a good foundation upon which police can build such a definition. Traditionally, all computer security efforts have sought to protect the confidentiality, integrity, and availability of information systems.[15]

Confidentiality in computer systems prevents the disclosure of information to unauthorized persons. Individuals who trespass into another person's computer system or exceed their own authority in accessing certain information, violate the legitimate owner's right to keep private information secret. Crimes that violate the confidentiality of computer systems include "unauthorized access crimes" as defined by Title 18, U.S.C. Section 1030(a)(2). Because breaking into a computer begins with unauthorized access to an information system, many believe this represents the foundational computer crime offense.

Integrity of electronically stored information ensures that no one has tampered with it or modified it without authorization. Thus, any nonsanctioned corruption, impairment, or modification of computer information or equipment constitutes an attack against the integrity of that information. Many of the malicious hacking activities, such as computer viruses, worms, and Trojan horses, fall within this category. The same is true for individuals who purposefully change or manipulate data either for profit or some other motivation, such as revenge, politics, terrorism, or merely for the challenge.

> ***"...computer crime has become an increasing problem."***

Availability of computer data indicates the accessibility of the information and that its associated programs remain functional when needed by the intended user community. A variety of attacks, such as the often-cited denial of service incidents, constitute a set of criminal activities that interferes with the availability of computer information.

Together, computer crime incidents that attack the confidentiality, integrity, or availability of digital information or services constitute an extremely precise and easily understood foundational definition of computer crime. In effect, these offenses might represent "pure-play" computer crimes because they involve a computer system as the direct target of the attack.

These three types of crimes should form the basis for an internationally agreed-upon definition of computer crime. In reality, they already are becoming the definition of computer crime because each state has some law that prohibits these offenses. Furthermore, an analysis of penal legislation in nearly 50 nations suggests that at least one-half of those countries surveyed—including most industrialized nations—had laws in place or legislation pending that prohibited crimes affecting the confidentiality, integrity, and availability of a computer.[16] A variety of international organizations also support legislative efforts prohibiting pure-play computer crimes. Groups, such as the United Nations, the G8, the Council of Europe, the OECD, and Interpol, each have delineated confidentiality, integrity, and availability offenses as forming the minimum basis of proscribed computer criminal behavior. The Council of Europe, the 41-nation body of which the United States is an observer, has been working on a draft treaty on cybercrime for several years. If adopted as currently drafted, the treaty would ensure that confidentiality, integrity, and availability offenses were outlawed in all signatory nations to the treaty, an extremely significant step forward in policing these crimes.[17]

Computer-Mediated Offenses

Defined broadly, the term computer crime or even the more common "computer-related crime" has described a wide variety of offenses. Traditional crimes, such as fraud, counterfeiting, embezzlement, telecommunications theft,

prostitution, gambling, money laundering, child pornography, fencing operations, narcotics sales, and even stalking, all could be computer related. Computer technology could facilitate or perpetrate each of these offenses.

These crimes, which represent traditional offenses perpetrated in new and, perhaps, more effective ways, differ from pure-play computer crimes, which involve a computer system as the direct target of attack. Additionally, these crimes, as a group, demonstrate that offenders can use a computer as a tool to commit the crime. The fact that a computer is not necessary to commit the crime sets these offenses apart from the pure-play computer crimes. Prostitution, counterfeiting, and frauds have taken place for hundreds of years without any computer connection. The computer-mediated forms of these crimes pose problems for law enforcement as well.

A traditional crime perpetrated with a new, high-tech twist raises the same investigative and legal challenges for police as pure-play computer offenses. The unique nature of information technology and computer networks moving at Internet speed often are highly incompatible with traditional legal models of policing. Crimes involving high technology cross multiple jurisdictions, are not covered by a single cohesive international law, become harder to track because of anonymity, result in expensive investigations, complicate efforts in obtaining forensic evidence, and require police to have specialized knowledge for a successful investigation. Because computer-related crimes pose many of the same investigative difficulties as pure-play computer crimes, documenting these criminal offenses proves useful. Once captured, these data can help police to further refine their allocation of resources and determine relevant crime trends for computer-mediated illegal activities.

Offenses where a computer is completely incidental to the crime represents the third type of criminal activity with possible computer involvement. In these cases, although a criminal might have used a computer before, during, or after the crime, it was not related directly to

the offending criminal activity. For example, a man who murders his wife and confesses 3 weeks later in an electronic document has not committed a computer crime—he has committed a homicide. Leaving behind computer-related evidence that will require specialized forensic methods does not turn murder into "cyber-homicide." For this reason, police should not count offenses that generate computer-related evidence incidental to the perpetration of the offense as either a computer crime or as a computer-related crime.

Law Enforcement's Response

How can agencies capture, analyze, and report data on these offenses in an efficient manner? In 1930, the U.S. Congress required the Attorney General to produce data on the incidence of crime in America. In turn, the Attorney General designated the FBI to serve as the national clearinghouse for the statistics collected. Since that time, the FBI has administered the Uniform Crime Reporting (UCR) Program, which obtains data based on uniform classifications and procedures for reporting from the nation's law enforcement agencies and presents this information in the annual *Crime in the United States* publication.[18] While the traditional UCR Summary Reporting System[19] tracks only eight criminal offenses (murder and nonnegligent manslaughter, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson), the new UCR National Incident Based Reporting System[20] (NIBRS) tracks 46 criminal offenses in 22 categories, including crimes perpetrated using computers.[21] However, because the transition from the traditional system to NIBRS will take considerable time, law enforcement executives proactively should review their internal procedures to ensure that they have appropriate policies in place to track and recap pure-play computer crimes.

Agencies should consider adding the following question to crime and arrest reports: "Was a computer used in the perpetration of this

offense?" Many agencies already include similar questions about the use of firearms or the occurrence of hate crimes on their internal reports. In fact, hate crimes may provide a useful lens through which to examine computer-related crime. Hate crimes often involve other crimes, such as assault, vandalism, and even murder. But, knowing what percentage hate actually motivates vandalism becomes a useful tool for police administrators attempting to understand and address community disorder problems.

Several efforts have begun to promote law enforcement's understanding of the prevalence and effects of computer crime. The FBI and the National White Collar Crime Center recently took a big step forward in counting computer-related fraud. In 2000, these organizations established the Internet Fraud Complaint Center (IFCC)[22] to create a national reporting mechanism for tracking fraud on the Internet. The center will track statistics on the number and type of complaints and forward reported incidents to the appropriate law enforcement agency. While IFCC will prove helpful in tracking Internet fraud data, it does not deal directly with pure-play computer crimes that violate the confidentiality, integrity, and availability of data. Therefore, federal, state, and local criminal justice agencies must take a more comprehensive approach.

Conclusion

To combat computer crime, law enforcement must build an internal capacity to define, track, and analyze these criminal offenses. Even if law enforcement has a highly sophisticated and well-developed system to count computer crime, agencies still must overcome the public's underreporting problem. Underreporting these crimes results from a failure on the part of the victim to realize a crime has taken place and an unwillingness to report discovered incidents to police.

To decrease the incidence of computer crime, law enforcement agencies must work with private organizations to ensure that businesses become aware of potential threats they face from computer crime. These partnerships could include working with technical experts from within and outside the government to develop solutions that improve the prevention and detection of computer crimes. Of course, even after detecting these crimes, police still must convince victims to report them.

> ***"Several efforts have begun to promote law enforcement's understanding of the prevalence and effects of computer crime."***

Police agencies must work with the business community to gain trust. Many community and problem-oriented policing techniques can help law enforcement as they deal increasingly with computer crime investigations. Government and industry partnerships, and police sensitivity about businesses' concerns, will help increase the number of these offenses brought to the attention of the police.

Most police agencies do not have the staff or funding to deal adequately with computer crime. Though the recent series of virus and denial of service attacks have increased public awareness of the problem, law enforcement organizations must prepare for offenses by developing a strategic and preventative approach to deal with this problem.

Law enforcement managers must ensure that they remain capable of responding to the changing faces of criminal activity in the 21st century. When compared to murder, rape, or violent assaults, computer crime may seem trivial. But, a person who asks an executive who loses his life savings due to the theft of intellectual property from his computer hard drive will get a different answer. The teacher who receives daily calls from credit agencies because she was the victim of on-line identity theft understands the importance of policing computer related crime as well. Similarly, so does the AIDS researcher who has 5 years of work destroyed by a computer virus. The mother of the 13-year-old girl who was lured across state lines by a pedophile will certainly demand a computer-competent police force capable of helping her. Each of these computer or computer-related crimes and their victims are real. Law enforcement agencies have a responsibility to protect and serve the public, regardless of advances in technology—a role that cannot be abdicated.

Defining the problem, gathering crime data, and analyzing the nature and scope of the threat represent natural steps in any problem-oriented policing approach. New forms of criminality do not differ—a lesson law enforcement agencies must learn to make computer crime count. ✦

Endnotes

[1] Andrew Glass, "Warding Off Cyber Threat: "Electronic Pearl Harbor Feared," *The Atlanta Journal and Constitution*, June 25, 1998.

[2] Anick Jesdanun, "Internet Attacks Raise Concerns About Risks of Growth," *San Francisco Examiner*, February 14, 2000.

[3] Michael Zuckerman, "Love Bug Stole Computer Passwords," *USA Today*, May 10, 2000.

[4] Jodi Mardesich, "Laws Across the Country Become Relevant in Connected World: Jurisdiction at Issue in Net Legal Cases," *San Jose Mercury News*, October 8, 1996, 1E.

[5] Catherine H. Conly, *Organizing for Computer Crime Investigation and Prosecution*, National Institute of Justice, July 1989, 6.

[6] These countries, several major industrial nations in the world, include the United States, the United Kingdom, France, Germany, Japan, Canada, Italy, and Russia.

[7] "International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-Related Crime," United Nations Crime and Justice Information Network Vienna: United Nations, 1994.

[8] Tina Kelley, "Security Fears Still Plague Cybershopping," *The New York Times*, July 30, 1998, G5; Michael Stroh, "Online Dangers, Offspring Protection; Security: Parents Can Find Allies on the Family Computer to Protect their Children from Harm on the Internet," *The Baltimore Sun*, May 10, 1999, 1C.

[9] M.E. Kabay, "ISCA White Paper on Computer Crime Statistics," International Computer Security Association (1998), *http://www.icsa.net/html/library/whitepapers/index.shtml*; accessed November 8, 2000.

[10] P.A. Collier and B.J. Spaul, "Problems in Policing Computer Crime," *Policing and Society* 307, no. 2 (1992).

[11] Larry Kamer, "Crisis Mode: It's About Values," *The San Francisco Examiner*, February 23, 2000, A15.

[12] Carri Kirbie, "Hunting for the Hackers: Reno Opens Probe Into Attacks That Disabled Top Web Sites," *The San Francisco Chronicle*, February 10, 2000, A1.

[13] "7 Days: Web Attacks Raise Security Awareness," *Computing*, February 17, 2000, 17.

[14] R. Power, "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends* 6, No. 1, Spring 2000.

[15] These three themes provide the basis for the Organization for Economic Cooperation and Development's (OECD) *Guidelines for the Security of Information Systems* and are included in most textbooks, legislative acts, and media articles on computer crime. The OECD document is available at *http://www.oecd.org//dsti/sti/it/secur/prod/reg97-2.htm*; accessed November 8, 2000.

[16] Based upon research conducted by the author.

[17] For further information, see *http://conventions.coe.int/treaty/EN/cadreprojets.htm*.

[18] U.S. Department of Justice, Federal Bureau of Investigation, *Crime in the United States* (Washington, DC, 1999).

[19] In the summary program, law enforcement agencies tally the number of occurrences of the offenses, as well as arrest data, and submit aggregate counts of the collected data in monthly summary reports either directly to the FBI or indirectly through state UCR programs.

[20] In NIBRS, law enforcement agencies collect detailed data regarding individual crime incidents and arrests and submit them in separate reports using prescribed data elements and data values to describe each incident and arrest.

[21] NIBRS provides the capability to indicate whether a computer was the object of the crime and to indicate whether the offenders used computer equipment to perpetrate a crime. This ensures the continuance of the traditional crime statistics and, at the same time, "flags" incidents involving computer crime. For additional information on NIBRS, contact the NIBRS Program Coordinator, Criminal Justice Information Services, 1-888-827-6427.

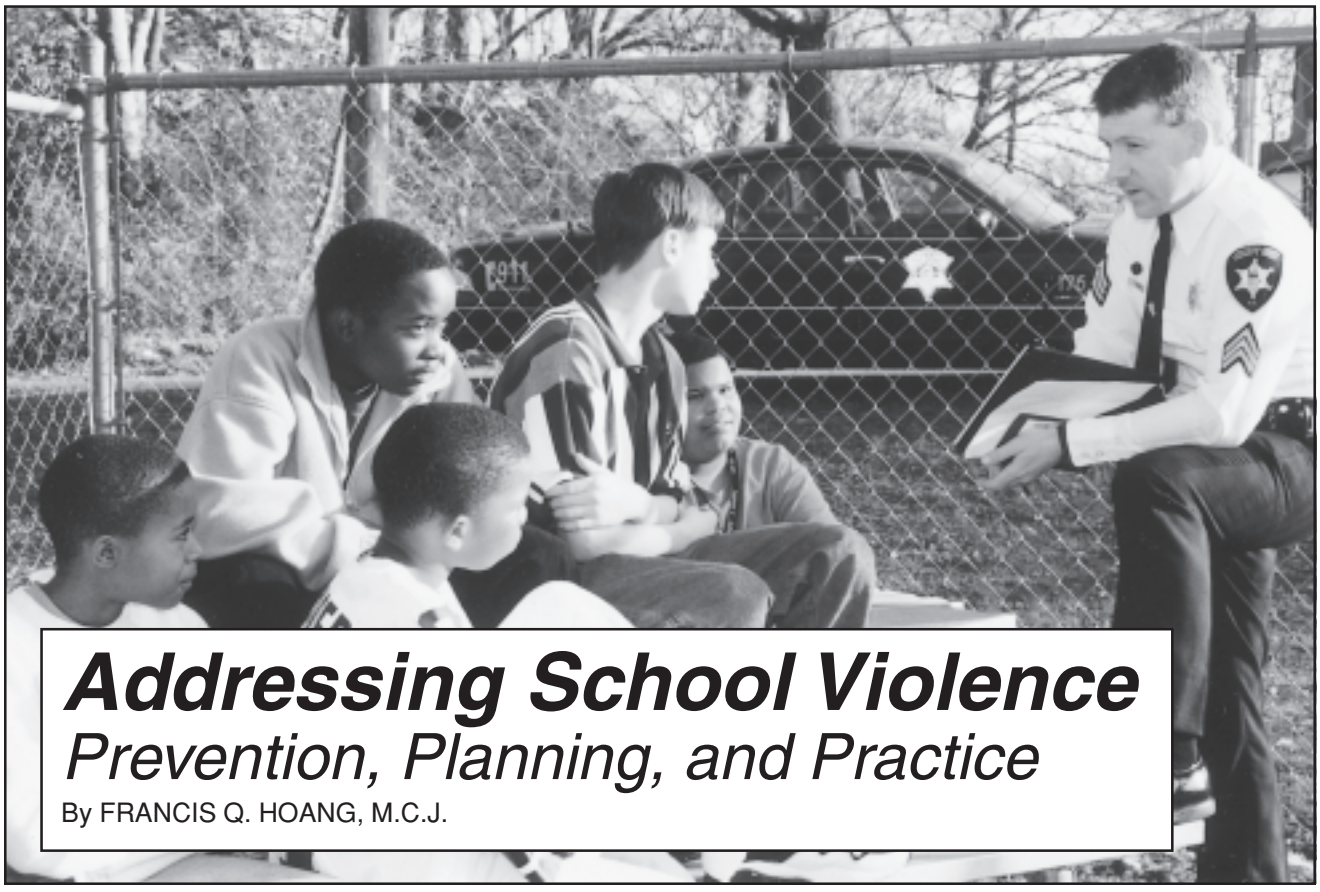
[22] Jerry Seper, "Justice Sets Up Web Site to Combat Internet Crimes," *The Washington Times*, May 9, 2000, A6, *www.ifccfbi.gov*; accessed November 8, 2000.

For further information regarding computer crime, contact the author at digitalpolice@yahoo.com.

Clarification

The article,"Police Pursuits and Civil Liability," which appeared in the July 2001 issue, contained an error. The last sentence of the third paragraph on page 19 should read as follows:

> The majority, however, concluded that the police conduct in this case did not "shock the conscience" and ruled in favor of the police.



Addressing School Violence

Prevention, Planning, and Practice

By FRANCIS Q. HOANG, M.C.J.

"It is imperative that, community by community, we find the ways to protect our children and secure for them the safe places they need to learn the hard business of growing up, to learn right from wrong, to learn to be good citizens."[1]

With these words, former FBI director Louis Freeh captured the essence of the challenge that communities face in addressing school violence. Recent high profile school shootings have led to an atmosphere of fear and apprehension among many communities about the safety of their schools. While statistics show that schools, in general, remain safer than their surrounding neighborhoods, every community must take steps to address school violence. In doing so, many questions may arise. Where does a community begin the process of addressing school violence? How can schools prevent or reduce school violence? How can communities plan for handling school violence when it does occur? Should law enforcement include exercises and training as a part of these preparations?

DEFINING SCHOOL VIOLENCE

To address school violence, communities first must understand what it is and who is involved.[2] The definition of school violence, an unacceptable social behavior ranging from aggression to violence that threatens or harms others, goes beyond highly publicized incidents of mass bloodshed to include acts, such as bullying, threats, and extortion. Therefore, school violence spans a broad range of antisocial

behavior that law enforcement must address.

IDENTIFYING PERPETRATORS OF SCHOOL VIOLENCE

Historically, individuals who commit school violence fall into one of two groups. The first group, "insiders" (e.g., students), usually can be divided into two broader categories—sociopaths (e.g., bullies who instigate fights and manipulate others) and psychopaths (e.g., socially inept loners who have the potential for great violence).[3] The second group involves visiting "outsiders," such as students from other schools or former students.

Communities must prepare for potential school violence from either of these groups. No standard profile of a school violent offender currently exists. At best, certain warning signs may indicate potential violence and specific factors may denote a greater likelihood of an individual carrying out violence.

ADDRESSING SCHOOL VIOLENCE

Primarily, communities can address school violence through three simple steps—prevention, planning, and practice. Prevention refers to taking actions to reduce or prevent school violence from occurring, planning determines what actions to take if school violence does occur, and practice entails rehearsing plans and modifying them when needed.

Prevention

Various publications provide a comprehensive overview of school violence prevention programs and offer various steps communities can take to help prevent violence in their schools.[4] First, communities should establish partnerships between schools and other public agencies. Because school violence remains a community problem, it requires collaboration from all residents, agencies, and businesses. Schools, police, business leaders, and elected officials all must cooperate to address school violence.

Next, communities should identify and measure the problem. School officials, working with law enforcement and other community agencies, should collect information that shows the size and scope of violence in their schools. This important step ensures that prevention efforts revolve around the community's specific problems.

Communities also should set goals and measurable objectives. School officials, collaborating with parents and students, should set goals (with broad results) and specific objectives (with measurable results) for their school violence prevention efforts.

Last, communities should identify appropriate research-based programs and strategies. The key to preventing and reducing school violence combines long-term strategies with short-term interventions. Community leaders and school administrators should research and examine various school violence prevention options and select techniques most appropriate for their schools. Such options fall into three broad categories.[5]

The first category involves environmental modifications and suggests that police, trained in crime prevention through environmental design, or school security managers, who have attended specialized courses in physical security, audit or survey each school. These personnel should examine a school's physical environment and recommend modifications to prevent or reduce violence.

The second category includes options for preventing and

> ***"While not every school may have to deal with a violent shooter, nearly every school experiences violent threats."***

Mr. Hoang, former deputy chief of police for the Fort Leavenworth, Kansas, Police Department currently serves as an advisor to the Rockland County, New York, Police Academy.

controlling violence based on school management. For example, this may entail establishing behavior and discipline codes, the use of criminal penalties against selected students, or the placement of problem students into alternative educational institutions.

The final category, education and curriculum-based prevention techniques, could include teaching conflict resolution courses, establishing mentoring programs, developing self-esteem initiatives, or instituting community-oriented policing crime prevention efforts.

After reviewing the various options, administrators should work with the entire community to carefully implement the selected prevention measures. Some preventive techniques may require additional resources, outside approval, or long-term planning to prove successful.

Every community should include an early identification and intervention program in their school safety efforts. These programs help prevent school violence by educating parents, teachers, and students about the signs of potential violence and, ultimately, allow the troubled student to receive help before violence occurs.[6]

Another critical element of a school safety program involves a threat management plan. While not every school may have to deal with a violent shooter, nearly every school experiences violent threats. Communities and school

School Violence Prevention Options

Possible Environmental Modifications

- Installing metal detectors and video cameras
- Hiring security guards
- Adopting dress codes
- Removing lockers
- Controlling access into buildings
- Identifying all campus visitors
- Placing adults in hallways
- Monitoring entrances
- Increasing lighting

School Management-Based Strategies

- Establishing behavior and discipline codes
- Using criminal penalties against selected students
- Placing students into alternative educational institutions
- Conducting lawful and necessary searches
- Establishing community information-sharing protocols

Education- and Curriculum-Based Prevention Techniques

- Teaching individuals conflict resolution
- Establishing mentoring programs
- Creating self-esteem initiatives
- Developing community-oriented policing and crime prevention efforts

See the OJJDP Annual Report on School Safety *for a listing of model programs and additional resources (*http://ojjdp.ncjrs.org/pubs/*).*

administrations must prepare to assess threats they receive and how to respond appropriately to them.[7]

After implementation, administrators should, at regular intervals, evaluate the school violence prevention plan against the goals and objectives previously set. Administrators must prepare to revise the plan based on the results of the evaluation.

Planning

Even with the best prevention plan in place, communities still must prepare for school violence incidents. Planning how to respond in the event of school violence requires a communitywide effort and includes numerous tasks.

Law enforcement should conduct a tactical survey of schools.[8] While the security audit serves to reduce or prevent school violence, the tactical survey gathers information for use in planning a response. The survey forms the foundation for all other planning efforts and should be accomplished before planning begins. Law enforcement, working with school administrators, should prepare and distribute tactical surveys that include elements, such as local maps, aerial photographs, property diagrams and floor plans, and interior and exterior photographs of the school.

School administrators should develop emergency response plans. Because faculty are often the first to respond to calls of school violence, their initial actions can have tremendous impact on how safely and quickly a situation is resolved. Each school should have procedures in place to handle different emergencies, including various school violence incidents. An easily accessible checklist that includes how and when to notify emergency services can prove most beneficial. Law enforcement and school officials should work together to develop procedures that cover such emergencies as anthrax scares, bomb threats, fires, severe inclement weather, bus accidents, and shootings.

> ***"Communities must prepare for potential school violence...."***

Developing first responder and immediate action drills also will prove beneficial. Past incidents have shown the need for rapid, coordinated response by the first officers arriving at a school violence incident. Patrol officers should establish a perimeter, gather information, resolve disputes, and, depending on the situation, locate and neutralize shooters. Local police agencies should establish and rehearse a mutual aid plan to ensure the use of the same response procedures.

Many school violence incidents do not require a tactical presence or may end before police tactical teams can deploy. However, tactical teams still should develop procedures for operating in a school environment. The plans should include how to integrate tactical teams with police already on the scene and how to deploy multiple teams in the event of a long-term or large-scale situation.

A large-scale school violence incident often requires more resources than one agency can provide and requires a joint response of many different organizations. Police administrators should develop an emergency management plan that outlines command, control, and communication procedures for a multiagency response, as well as general areas of responsibility for each agency.

Because school violence incidents generate media interest, agencies must develop a plan for handling the media prior to an incident. Police and schools should prepare to assist the media by providing timely briefings, designating a media representative for updates, and establishing areas safe for filming, interviews, and other media activities.

School officials should develop lock-down procedures to secure students and faculty in a school violence situation. They also should have procedures for evacuating students and faculty to safe areas, establishing accountability, conducting immediate counseling or debriefings (if required), and coordinating the pickup of students by parents. Schools should work with police in developing these plans because tactical and investigative considerations may impact the evacuation or release of students.

In a worst-case scenario, school violence can result in bloodshed—a

Keys To Successful Exercises

- Identify clear training objectives
- Conduct coordination before the exercises
- Hold exercises after developing plans and completing training
- Start with simple tasks and work progressively toward more difficult ones
- Conduct after-action reviews
- Link future training to results from past exercises

reality that officials must prepare to handle. School, police, and emergency response personnel should work together to develop a plan to triage, treat, and evacuate those injured in a school violence situation.

Even after the successful resolution of a school violence incident, much work remains. Communities should develop a plan to provide counseling and assistance to students, faculty, and emergency personnel. Police need to develop an investigative plan, establish evidence recovery methods, and determine when they will return control of the building to school officials. School administrators should prepare to find an alternate location to hold classes while police conduct their investigation.

Due to the size and complexity of a school violence response, the various agencies involved should develop and sign mutual aid and notification agreements. These agreements should specify roles and responsibilities for each agency.

School violence planning requires a large investment of time, personnel, and resources. However, the possible benefits more than justify the cost. Communities that make planning a priority will become prepared not only for school violence but also for lesser situations that may require a coordinated response.

Practice

The best-developed plans become useless if they are never rehearsed or if no one knows they exist. Practice validates plans and identifies needed changes. It familiarizes personnel with plans and partners, increases the confidence of personnel involved, and gives the community a sense of security. Additionally, conducting drills can help identify areas for future training. Practice remains a critical step in preparing for school violence and should include rehearsing school emergency response plans, first-responder action drills, tactical team actions, post-incident command exercises, media plans, mass casualty plans, multiagency exercises, and field exercises. Because no substitute for practice exists, this step remains critical in addressing school violence and requires a strong commitment by communities.

FACING CHALLENGES

In addressing school violence, communities face several key challenges. They must learn how to balance the need for a secure environment with that of a learning environment. While many parents and schools welcome the increased emphasis on security, others worry that schools have become fortresses that hamper learning. Communities must examine their approach carefully and strike the right balance for their students.

Communities must decide how to balance student and parental rights with a community's compelling interest in safety. Many of the techniques proposed to prevent school violence may infringe upon student or parental rights. At the same time, administrators have a responsibility to maintain safe schools and must balance these competing interests when developing a school safety plan.

Additionally, communities must consider how to weigh the needs of many students against the needs of a few students. Many teachers and parents applaud recent efforts at getting help for at-risk youth before violence erupts, yet some individuals criticize these efforts as putting the needs of a few students ahead of the needs of the majority of the students. Communities must decide how far they should go to address some students' special needs and consider the impact on other students.

CONCLUSION

Because every community is unique, individual approaches to addressing school violence should be slightly different. Communities

should seek the advice and help of other communities that have addressed similar problems, adapt these solutions, and tailor their approach to their specific situations.

Communities must take a team approach to addressing school violence. Addressing specific issues requires cooperation among schools, families, police, and other community members. If school violence should occur, a community will rely on many agencies to respond. No one agency holds the key; rather, teamwork stands as the definitive method of acheiving success.

Remaining well informed represents the best approach when addressing school violence. Community officials should refer to the plethora of resources available to help them make informed decisions about school violence.

Finally, and perhaps most important, communities must take a proactive approach when addressing school violence. As previous tragic events have shown, no amount of preparation can ever eliminate school violence, but proper preparation can help reduce its impact on American communities. ✦

Endnotes

[1] U.S. Department of Justice, Federal Bureau of Investigation, "The School Shooter: A Threat Assessment Perspective, 2000," (Washington, DC, 2000); *http://www.fbi.gov*; accessed March 14, 2001.

[2] For additional information on school violence, see S. Band and J. Harpold, "School Violence: Lessons Learned," *FBI Law Enforcement Bulletin*, September 1999, 9-15.

[3] Dale Yeager, quoted in R. Kanable, "Patrolling the Schools," *Law Enforcement Technology*, September 1999.

[4] See, for example, U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, "The Annual Report on School Safety," (Washington, DC); *http://ojjdp.ncjrs.org/pubs/violvict.html*; accessed February 23, 2001.

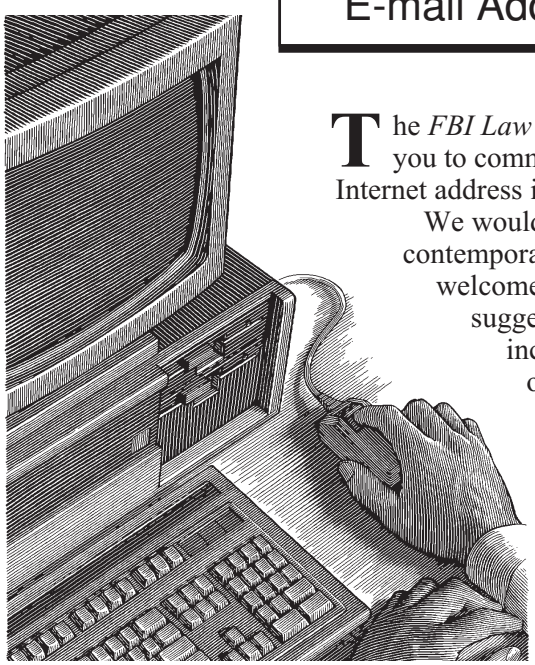
[5] Alexander Volokh and Lisa Snell, "School Violence Prevention: Strategies to Keep Schools Safe," Reason Public Policy Institute, January 1998; *http://www.rppi.org/education/ps234.html;* accessed February 23, 2001.

[6] The U.S. Department of Education has published "Early Warning, Timely Response: A Guide to Safe Schools," which describes how to develop and implement an early identification and intervention program; *http://www.ed.gov/offices/OSERS/OSEP/earlywrn.html*; accessed March 15, 2001.

[7] For additional information, see, supra note 1.

[8] For additional information, see F. Hoang, "Preplanning for School Violence," *Law and Order*, December 2000, 107-109.

The *Bulletin's* E-mail Address

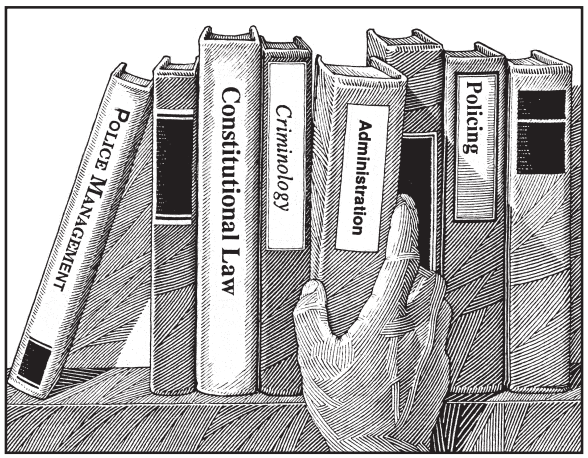


The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our Internet address is *leb@fbiacademy.edu*.

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*.

Book Review



The Loss of Innocents: Child Killers and Their Victims *by Cara E. Richards, Scholarly Resource, Inc., Publishing, Wilmington, Delaware, 2000.*

The Loss of Innocents: Child Killers and Their Victims presents a compilation of professional research efforts from 1983 through the 1990s that provides an assessment of over 200 cases of children and adults who participated in multiple murders. It supplements other research on homicide and violence, including those research and publication efforts conducted by the U.S. Department of Justice.

In view of the confidential sensitivity and protection afforded juveniles, the author's use of data extracted from newspapers of several major U.S. cities proved notable. The author identified and analyzed demographic information in terms of the perpetrators' patterns, random and selected victims, relationship with each other, rationale for killing, and methods used. Data ranged from children as the perpetrators or victims of mass and serial murdering to children as the victims of unintended and unfortunate cases of being in the wrong place at the wrong time. Those victims of bad decisions—illicit drugs in the home, animal attacks, home accidents, and drive-by shootings—represent the result of placing children at high risk, which cost them their lives.

Several case summaries on females as mass murderers and serial killers of children and adults placed emphasis on agencies revisiting their formal and accepted definitions of child killers. The author further established that the male killer of children specialized in a pattern involving targeted strangers, certain sex and age groups, or physical appearance with sexual motivations, while the females studied killed children they knew.

Research tables, in matrix form, present the data for the reader to analyze and compare. Identification of significant research problems and causal explanations supported by discussion of key factors surrounding child killers and victims comprise a vital chapter resulting from the author's efforts. Also, the author includes an interesting topology grouping of multiple child killers into five categories—disciple killer, family annihilator, pseudo-commando, disgruntled employee, and set-and-run killer.

The last section of the book contains 17 significant recommendations of the study for multiple jurisdictions to assess for reducing violence against children. They range from clarifying, simplifying, and standardizing definitions to using child killer case reviews for learning more about perpetrator and victim patterns of killings to increase gun safety education and legislation for adults and children.

The Loss of Innocents: Child Killers and Their Victims is well documented, correlated, and presented for those having no prior experience or knowledge of the subject to such professionals as juvenile and adult court judges and probation officers, prosecutors, and state legislators. It also will interest experienced and newly appointed law enforcement officers, homicide investigators, social workers and service agencies, emergency room medical personnel, prosecutors, and investigative media reporters.

Reviewed by Larry R. Moore
Certified Emergency Manager
International Association of Emergency Managers
Knoxville, Tennessee

Miranda *Revisited*

Dickerson v. United States

By THOMAS D. PETROWSKI, J.D.

© Mark C. Ide

The Fifth Amendment of the U.S. Constitution states, in part, that "...no person shall be compelled in any criminal case to be a witness against himself." Like other Constitutional provisions, this requirement has "both the virtue of brevity and the vice of ambiguity."[1] This Fifth Amendment provision formed the basis of the Supreme Court's decision in *Miranda v. Arizona*.[2] Recently, in *Dickerson v. United States,*[3] the Supreme Court further defined the impact of the *Miranda* decision on the law of interrogations. This article examines the *Dickerson* decision and its implications for law enforcement.

THE ADMISSIBILITY OF CONFESSIONS BEFORE *MIRANDA*

Prior to *Miranda*,[4] the admissibility of incriminating statements of a suspect was evaluated under a voluntariness test, which developed under early common law. Eventually, courts began to recognize that certain confessions were not trustworthy.[5] Although different standards were used to determine whether a confession was trustworthy, a confession generally was considered to be reliable only if made voluntarily.[6] In *Hopt v. Utah*,[7] the U.S. Supreme Court specifically adopted the common law rule that a voluntary confession is presumed to be reliable and, therefore, admissible. The Court held in *Hopt* that a confession is voluntary if not induced by threat or promise.[8]

Subsequent decisions of the U.S. Supreme Court recognized two constitutional rationales for the voluntariness requirement: the Fifth Amendment right against self-incrimination and the Due Process Clause of the Fourteenth Amendment. In 1897, the Supreme Court first asserted in *Bram v. United States*[9] that the Fifth Amendment privilege against self-incrimination was "but a crystallization"[10] of the common law rule that only voluntary confessions are admissible as evidence. Then, in 1936, the Supreme Court in *Brown v. Mississippi*[11] invoked the Due Process Clause as another constitutional basis for its requirement that a confession be made voluntarily. Thereafter, a confession was admissible only if voluntary within the meaning of the Due Process Clause.[12] The Supreme Court cases that followed *Brown*[13] refined the test into an inquiry that examined "whether a defendant's will was overborne" by the circumstances surrounding the giving of

Special Agent Petrowski is a legal instructor at the FBI Academy.

> ***The* Dickerson *decision did not alter the requirements* Miranda *placed on law enforcement.***

a confession and took into account "the totality of all the surrounding circumstances—both the characteristics of the accused and the details of the interrogation."[14] The rule governing the admissibility of confessions in federal court remained the same for nearly 180 years: confessions were admissible at trial if made voluntarily.

THE *MIRANDA* DECISION

A New Approach

In 1966, the Supreme Court decided *Miranda v. Arizona*. In what is arguably its most controversial criminal law decision,[15] the Supreme Court, in a 5-4 decision, changed the focus of the inquiry to determine the admissibility of suspects' incriminating statements by announcing a new approach. Specifically, the Court made the case-by-case totality-of-the-circumstances voluntariness analysis a supplementary consideration and identified a new primary focus. The Court held that any statement arising from the custodial interrogation of a suspect is presumed involuntary and, therefore, inadmissible unless the police first provide the suspect with four specific warnings.[16] The four warnings are—[17]

1) that the suspect has the right to remain silent;

2) that any statements he makes can be used against him;

3) that he has the right to the presence of an attorney during questioning; and

4) that an attorney will be appointed for him if he cannot afford one.

The Court did not eliminate the voluntariness inquiry. Consequently, an incriminating statement may be prefaced by *Miranda* warnings but still be involuntary, which may result in suppression of the statement. That is, a law enforcement interrogator cannot physically threaten or otherwise inappropriately coerce a confession simply because the warnings have been given and waived. Likewise, a clearly voluntary statement that was not prefaced by complete *Miranda* warnings also may result in suppression. For a statement to be admissible under *Miranda*, it has to be both voluntary *and* prefaced by complete *Miranda* warnings, which are intelligently, knowingly, and voluntarily waived. The Court also has held that once individuals invoke their right to counsel, officers immediately must cease interrogation until counsel is present or the suspects initiate further contact and unequivocally communicate the desire to proceed without counsel.[18]

Passage of 18 U.S.C. § 3501.

In *Miranda*, the Court said that "[w]e encourage Congress and the States to continue their laudable search for increasingly effective ways of protecting the rights of the individual while promoting efficient enforcement of our criminal laws. However, unless we are shown other procedures which are at least as effective in appraising accused persons of their right of silence and in assuring a continuous opportunity to exercise it, the...safeguards must be observed."[19]

In 1968, 2 years after *Miranda* was decided, Congress accepted the Court's invitation to show "other procedures" and enacted 18 U.S.C. § 3501[20] (hereafter § 3501). Through § 3501, Congress attempted to overrule *Miranda* and reinstate the voluntariness test as the sole determinant for admissibility of confessions in federal court. The statute explicitly abandoned the requirement of pre-interrogation warnings in favor of an approach that considers such warnings only one factor in determining

the voluntariness of a subject's incriminating statements. This left law enforcement agencies in a quandary over which rule to follow.

Despite the passage of § 3501, law enforcement agencies generally followed the *Miranda* rule and ignored the statute. This is most likely due to the common approach of law enforcement agencies to take the more conservative option when such a conflict presents itself. The Department of Justice, through the seven administrations between *Miranda* and *Dickerson*, refused to argue § 3501 and also followed the *Miranda* decision in confession cases.

THE *DICKERSON* CASE

The Facts

On January 24, 1997, an individual robbed the First Virginia Bank in Old Town, Alexandria, Virginia, of approximately $876. An eyewitness saw the robber exit the bank, run down the street, and get into a vehicle. Subsequent investigation into the bank robbery revealed that the getaway car was registered to Charles T. Dickerson of Takoma Park, Maryland. On January 27, 1997, FBI agents and an Alexandria police detective traveled to Dickerson's residence. The agents knocked on Dickerson's door and identified themselves. After a short conversation, an FBI agent asked Dickerson if he would accompany them to the FBI field office in Washington, D.C. Dickerson agreed. While in Dickerson's apartment, the agents saw evidence of the bank robbery in plain view.

At the FBI field office, Dickerson was interviewed by an FBI agent and a detective of the Alexandria Police Department. It is uncontested that at some point during the interview, Dickerson appropriately was given his *Miranda* warnings and that he knowingly and voluntarily waived his rights in writing. It also is uncontested that Dickerson confessed to the Alexandria bank robbery and numerous others and identified an accomplice. During the interview of Dickerson, the interviewing agents made application for, and received, a telephonic search warrant for Dickerson's apartment. The search warrant was executed while the interview continued. The agents conducting the search found substantial evidence implicating Dickerson in several bank robberies. He was arrested and indicted on one count of conspiracy to commit bank robbery in violation of 18 U.S.C. § 371, on three counts of bank robbery in violation of 18 U.S.C. § 2113(a) and (d), and on three counts of using a firearm during, and in relation to, a crime of violence in violation of 18 U.S.C. § 924(c)(1).[21]

> ***"Departments must ensure that their officers do not interrogate 'outside Miranda,' and immediately abandon any condoned practice or policy of intentional violations of Miranda."***

At the inevitable evidence suppression hearing, Dickerson testified that his confession was made before he received his *Miranda* warnings and, therefore, violated *Miranda.* The interviewing FBI agent testified that Dickerson confessed after receiving his *Miranda* warnings and voluntarily waiving them. There was no question that the confession was voluntary, but only whether it was made before or after Dickerson was warned and waived his *Miranda* rights. The district court judge suppressed his confession. The suppression of the confession was appealed to the U.S. Court of Appeals for the Fourth Circuit.

The Fourth Circuit decided there was sufficient evidence in the record to support the district court's finding that Dickerson had not been given his *Miranda* rights prior to confessing.[22] However, the Fourth Circuit reversed the lower court's decision to suppress the confession, finding the lower court used the wrong standard to judge the confession's admissibility. The Fourth Circuit decided that by passing § 3501, Congress had lawfully changed the test for the admission of confessions in federal court from the stricter *Miranda* rule to the less stringent totality-of-the-circumstances test. Using that less stringent standard, the Fourth Circuit found that the government's failure to give *Miranda* warnings was only one factor to be considered when judging voluntariness of the

confession. Because the lower court already had found Dickerson's confession to be voluntary, the Fourth Circuit reversed. The U.S. Supreme Court agreed to finally decide the issue.

The Decision

The U.S. Supreme Court issued its opinion on *Dickerson* on June 26, 2000. In a 7-2 decision, the court held that *Miranda* is a Constitutional decision and, therefore, could not be overruled by an Act of Congress.[23] The Court not only affirmed *Miranda* but also declared it a Constitutional rule.[24] Aside from elaborating in great detail as to why its finding that *Miranda* is Constitutionally required was consistent with its original decision and its progeny, the Court gave two other noteworthy justifications. The Court found that "*Miranda* has become embedded in routine police practice to the point where the warnings have become part of our national culture."[25] The Court also said "...experience suggests that the totality-of-the-circumstances test which § 3501 seeks to revive is more difficult than *Miranda* for law enforcement officers to conform to, and for courts to apply in a consistent manner."[26] Thus, 32 years after enactment, § 3501 has been ruled unconstitutional, and the precustodial interrogation requirements of *Miranda* have been given "a permanent place in our jurisprudence."[27]

PRACTICAL IMPLICATIONS: CIVIL LIABILITY

The Supreme Court's decision in *Dickerson* was both a surprise and a disappointment to many.[28] The decision clearly elevates the warning requirements of *Miranda* to Constitutional proportions; the single most significant practical impact of which is potential civil liability of individual law enforcement officers and their departments resulting from intentional violations of the warning requirements mandated in *Miranda*.

> ***...the Court held that* Miranda *is a Constitutional decision and, therefore, could not be overruled by an Act of Congress.***

Title 42 U.S.C. § 1983[29] (hereafter §1983) provides a federal remedy for deprivations of federal Constitutional rights by authorizing suits against public officials and government entities.[30] To recover under § 1983, a civil rights plaintiff must prove two elements: 1) intentional deprivation of a federally protected right "secured by the Constitution and the laws of the United States," and 2) state action under color of law.[31] Section 1983 was applied to federal law enforcement agencies in *Bivens v. Six Unknown Federal Narcotics Agents*.[32] A host of individual state causes of action mirror §1983 suits that can result in liability to the department and personal liability to the individual officer.

Section 1983 requires intentional conduct or gross negligence by the government employee. Mere negligence is not actionable under §1983.[33] For example, if an interrogator were to negligently give defective warnings, this would not result in §1983 liability.

In addition to the individual officer being exposed to §1983 liability, the agency or department also can be sued for Constitutional violations arising from official policy or other customs or practices of the entity.[34] Inadequate training also may be the basis for liability if the failure to train amounts to a deliberate indifference to rights of persons with whom police come in contact.[35]

Prior to the Supreme Court's decision in *Dickerson*, the clear majority view among the federal circuits was that no cause of action for money damages existed under §1983 where police officers allegedly violated *Miranda* principles by either failing to give *Miranda* warnings or by continuing to question a defendant in custody after his request for an attorney.[36] The rationale prior to *Dickerson* was that the U.S. Constitution did not guarantee the right to *Miranda* warnings. *Dickerson* only can be read to have changed this and to have created the requisite Constitutional right that satisfies the previously void §1983 element. While the Court in *Dickerson* did not expressly address the issue of civil liability and may at some future time limit §1983 liability exposure in the *Miranda* context, the only prudent course for law enforcement officers today is to proceed assuming that this §1983 cause of action is now viable.

In any §1983 civil action, the issue of qualified immunity is always present. Qualified immunity is available to defendants in a §1983 suit if they can show the actions in question did not violate any clearly established law of which they should have been aware at the time; in other words, the actions were within the law and objectively reasonable.[37] Because the issue of *Miranda's* Constitutionality has been squarely addressed by the Supreme Court—and thus "clearly established"—it is unlikely that law enforcement officers (or their department) would be entitled to qualified immunity for intentional violations of the *Miranda* requirement.[38]

The potential for actual (compensatory) damages for such a lawsuit obviously would be limited. But there is always the possibility of punitive damages[39] and attorney's fees,[40] which make even minor violations a potential suit. As any experienced law enforcement manager understands, there is no such thing as an insignificant §1983 lawsuit. Even suits that are ultimately won are costly and substantially hinder the mission of the department, thus affecting public safety. In §1983 lawsuits, "the only true victory is the avoidance of conflict completely."[41]

PRACTICAL GUIDANCE

The *Dickerson* decision did not alter the requirements *Miranda* placed on law enforcement. It did, however, establish liability exposure to law enforcement officers and their departments for failure to comply with those requirements.

Stay "Inside" *Miranda*

In Supreme Court decisions subsequent to *Miranda*, the Court recognized legitimate uses for statements taken in technical violation of the *Miranda* requirements but voluntarily made.[42] Such statements may be used to impeach a defendant's trial testimony if the defendant takes the stand and testifies inconsistently with prior statements[43] or at a subsequent trial for perjury resulting from the false trial

testimony. Witnesses identified in statements taken in technical violation of *Miranda* also may testify.[44] These permissible uses of incriminating statements obtained in violation of *Miranda* have led to a practice in law enforcement of intentionally questioning in violation of *Miranda*. This practice is commonly referred to as questioning "outside *Miranda*." In fact, numerous law enforcement agencies have encouraged and provided training in this practice, which has been impacted significantly by the *Dickerson* decision and now invites § 1983 lawsuits.

Departments must ensure that their officers do not interrogate "outside *Miranda*," and immediately abandon any condoned practice or policy of intentional violations of *Miranda*. The clearest example of this is the continuation of questioning after a suspect unequivocally has invoked his right to counsel. This also would include the practice of interrogating before the warnings are given (with a view toward having suspects make incriminating statements and then be given the warnings, which are likely to be waived because they already have incriminated themselves). While it is likely that voluntary statements made in technical violation of *Miranda* will remain admissible for the limited purposes described above, they clearly are exposing interrogating officers and their departments to civil liability. Departments must avoid even the appearance of intentionally conducting interrogations not in strict compliance with *Miranda*.

Do Not "Over-Mirandize"

Law enforcement departments must be mindful of another obvious trap for those who are unwary or lack confidence in the practical applications of *Miranda*: the tendency to repeatedly or unnecessarily give *Miranda* warnings. Any experienced law enforcement interrogator has seen this in practice. In an effort to guarantee absolute *Miranda* compliance during a conversation with a suspect, many law enforcement officers will give repeated warnings or, more commonly, provide warnings when they obviously are not required.

Repeated warnings usually happen when an officer contacts a suspect who recently has been properly warned, but gives the warnings again to ensure compliance with *Miranda*. While no Supreme Court decision addresses how "fresh" a warning has to be, the common approach is to re-advise only after an extended break in interrogation has occurred. Unnecessary warnings occur when law enforcement officers fail to realize that the suspect is not in custody and/or not being interrogated.[45] Either of these scenarios is most likely to happen when the investigation involves a serious crime or is for some other reason a high profile matter.[46]

Both "over-Mirandizing" scenarios were a problem prior to *Dickerson*.[47] Now, in addition to apprehension about statements being suppressed, law enforcement officers will be further burdened by the possibility of civil liability. The inevitable result will be an even greater tendency to "over-Mirandize." The answer for law enforcement is more training.

The Need for Training and Sound Policies

A thorough understanding of all aspects of *Miranda* by all members of a department is a substantial training task. That said, the only way to minimize lost evidence and potential civil liability caused by a lack of understanding of *Miranda* is training supported by solid department policies.

Another aspect of interrogation largely controlled by policy is the documentation used to record *Miranda* warnings and waivers. As demonstrated in *Dickerson*, the prosecution must be able to establish that the *Miranda* requirements were met. Law enforcement managers should reevaluate their policies regarding the use of written waiver forms and the number of officers present during a rights warning and waiver. They should consider videotaping at least the rights warning and waiver, if not the entire interview. The facts in *Dickerson* demonstrate how a lawful and documented advice of rights and waiver still can result in a confession being suppressed.

> ***...the Court not only affirmed* Miranda *but also declared it a Constitutional rule.***

CONCLUSION

The *Dickerson* decision elevated the warning requirements of *Miranda* to Constitutional proportions. The decision has no practical impact on the requirements placed on law enforcement departments and agencies in complying with *Miranda*. The timing of the warnings (i.e., before any interrogation occurs of a subject who is in custody) and the substance of the warnings have remained unchanged.

The critical impact of the *Dickerson* decision is that intentional violations of the requirements of *Miranda*, commonly known as questioning "outside *Miranda*," now may provide the basis for a lawsuit alleging a federal Constitutional violation. Aside from exposing officers and departments to civil liability, this may exacerbate the problem of unnecessarily providing *Miranda* warnings.

Law enforcement managers should reevaluate their existing training and policies that address the practices of their personnel conducting interviews and interrogations. Now, more important than ever, intentional violations of *Miranda* must cease. ✦

Endnotes

[1] Jacob W. Landyski, *Search and Seizure and the Supreme Court: A Study in Constitutional Interpretation* (Baltimore, MD: The Johns Hopkins Press, 1966), 42, commenting on the Fourth Amendment.

[2] *Miranda v. Arizona*, 384 U.S. 436 (1966).

[3] *Dickerson v. United States*, 530 U.S. 428 (2000).

[4] *Id*. Also see generally *United States v. Dickerson*, 166 F.3rd 667 (4th Cir. 1999).

[5] *The King v. Rudd,* 168 Eng. Rep. 160 (K.B.1783) (holding that "no credit ought to be given" to "a confession forced from the mind by the flattery of hope, or by the torture of fear") and references thereto by the U.S. Court of Appeals, Fourth Circuit in *United States v. Dickerson*, 166 F.3rd 667 (4th Cir. 1999).

[6] *Regina v. Garner*, 169 Eng. Rep. 267 (Ct.Crim.App.1848); *Regina v. Baldry*, 169 Eng. Rep. 568 (Ct.Crim.App.1852) and references thereto in *United States v. Dickerson*, 166 F.3rd 667 (4th Cir. 1999).

[7] 110 U.S. 574 (1884).

[8] *Id.* at 577 (citing *Baldry,* 169 Eng. Rep. 568 (Ct.Crim.App.1852)); see also *Pierce v. United States*, 160 U.S. 355, 357 (1896).

[9] 168 U.S. 532 (1897).

[10] *Id.* at 542 (stating that whether a confession is voluntary "is controlled by that portion of the Fifth Amendment...commanding that no person 'shall be compelled in any criminal case to be a witness against himself'" (quoting the Fifth Amendment to the U.S. Constitution)).

[11] 297 U.S. 278 (1936).

[12] The Supreme Court first defined "compulsion" in *Bram*, stating that a confession "must not be extracted by any sort of threat or violence, nor obtained by any direct or implied

promises, however slight, nor by the exertion of any improper influence." See, e.g., *Haynes v. Washington*, 373 U.S. 503 (1963); *Ashcraft v. Tennessee*, 322 U.S. 143 (1944); *Chambers v. Florida*, 309 U.S. 227 (1940).

[13] The Supreme Court applied the due process voluntariness test in "some 30 different cases decided during the era that intervened between *Brown* and *Escobedo v. Illinois*, 378 U.S. 478 (1964)." *Schneckloth v. Bustamonte*, 412 U.S. 218, at 226 (1973). See also, *Haynes*, *supra*, at 513; *Gallegos v. Colorado*, 370 U.S. 49, 55 (1962); *Reck v. Pate*, 367 U.S. 433, 440 (1961) ("[A]ll the circumstances attendant upon the confession must be taken into account"); *Malinski v. New York*, 324 U.S. 401, 404 (1945).

[14] *Dickerson,* 530 U.S. at 434, citing *Schneckloth*, 412 U.S. at 223.

[15] The *Miranda* decision is clearly one of the Supreme Court's most well-known and prolific cases. As of May 27, 2001, Westlaw reported that *Miranda* had been cited in judicial decisions, treatises or other scholarly articles 29,031 times.

[16] It is critical for law enforcement officers to understand that this is a "bright-line" rule. There is no balancing test nor good faith exception. A completely voluntary statement by a subject prompted by a law enforcement interrogator with the best of intentions will be suppressed if there is any material deviation from the *Miranda* requirements. This is contrary to the more familiar Fourth Amendment search and seizure requirements (which law enforcement officers typically spend far more time with than Fifth Amendment issues). Fourth Amendment analyses are grounded in a reasonableness/totality-of-the-circumstances approach and balance the interests of the individual versus those of the public. The Supreme Court said in *Graham v. Connor*, 490 U.S. 386, at 396 (1989) (quoting *Bell v. Wolfish*, 441 U.S. 520 (1979)) that "[t]he test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application...." But, the Court made clear in *Miranda* that the test of voluntariness under the Fifth Amendment is.

[17] *Miranda*, 384 U.S. at 444.

[18] See generally *Edwards v. Arizona*, 451 U.S. 477 (1981).

[19] *Miranda*, 384 U.S. at 467.

[20] 18 U.S.C. § 3501 provides, in relevant part:

"(a) In any criminal prosecution brought by the United States or by the District of Columbia, a confession...shall be admissible in evidence if it is voluntarily given. Before such confession is received in evidence, the trial judge shall, out of the presence of the jury, determine any issue as to voluntariness. If the trial judge determines that the confession was voluntarily made it shall be admitted in evidence and the trial judge shall permit the jury to hear relevant evidence on the issue of voluntariness and shall instruct the jury to give such weight to the confession as the jury feels it deserves under all the circumstances.

(b) The trial judge in determining the issue of voluntariness shall take into consideration all the circumstances surrounding the giving of the confession, including (1) the time elapsing between arrest and arraignment of the defendant making the confession, if it was made after arrest and before arraignment, (2) whether such defendant knew the nature of the offense with which he was charged or of which he was

suspected at the time of making the confession, (3) whether or not such defendant was advised or knew that he was not required to make any statement and that any such statement could be used against him, (4) whether or not such defendant had been advised prior to questioning of his right to the assistance of counsel, and (5) whether or not such defendant was without the assistance of counsel when questioned and when giving such confession.

The presence or absence of any of the above-mentioned factors to be taken into consideration by the judge need not be conclusive on the issue of voluntariness of the confession."

[21] On October 6, 2000, in the aftermath of the Supreme Court decision, Dickerson was found guilty after a jury trial of three of the original seven counts (one count each of the conspiracy, bank robbery, and firearms charges) in Federal District Court, Alexandria, VA.

[22] For reasons not disclosed in the record, the government relied exclusively on the testimony of the interviewing FBI agent and did not use other evidence, such as the testimony of an Alexandria Police Detective (who had been present for the entire interview) or a written statement of Dickerson that clearly demonstrated that he had received his *Miranda* warnings prior to confessing. The Fourth Circuit was unable to find as matter of law that the lower court erred in its factual findings supporting the suppression of Dickerson's statements. In reviewing the decision of the District Court in suppressing the statements, the Fourth Circuit stated that:

> [The Alexandria police detective], who was in the interview room with Dickerson at all times, stated in his affidavit that "Dickerson was read his Miranda rights before he made th[e] statements" implicating himself...in the First Virginia Bank robbery.... In fact, [the Alexandria police detective] testified that when Dickerson was read his Miranda rights he still denied any involvement in the bank robbery. According to [the Alexandria police detective], it was not until Dickerson was told that agents had found a bait bill from a bank robbery in his apartment that he decided to confess.
>
> Attached to [the Alexandria police detective]'s affidavit was a hand-written statement that Dickerson made while at the FBI field office in which he stated that he "was read [his] rights [at a time clearly before his confession and issuance of the warrant]".... *Thus, according to his own hand-written note, Dickerson was read his Miranda warnings prior to implicating himself...in the First Virginia Bank robbery*."

U.S. v. Dickerson (4th Cir.) at 676-677 (emphasis added).

[23] An Act of Congress will not be enforced by the courts if what it prescribes violates the Constitution of the United States. Such judicial review of the legislative branch was established in *Marbury v. Madison*, 1 Cranch 137, 2 L.Ed. 60 (1803).

[24] *Dickerson*, 530 U.S. 444. "In sum, we conclude that Miranda announced a constitutional rule that Congress may not supersede legislatively...[and] we decline to overrule Miranda ourselves."

[25] *Id.*

[26] *Dickerson,* 530 U.S. 444.

[27] *Id.,* (dissent of Justice Scalia). While 32 years seems a long time for an Act of Congress to be held unconstitutional, it is not the record. Apparently, the longest such delay is the 122 years it took the Supreme Court to declare18 U.S.C. 474 (enacted in 1862) unconstitutional in *Regan v. Time, Inc.*, 468 U.S. 641 (1984).

[28] To appreciate how controversial the *Miranda* through *Dickerson* line of cases are, one need look no further then the dissenting opinion of Justice Scalia, with whom Justice Thomas joins, in *Dickerson*, 530 U.S. 444

[29] Title 42 U.S.C. §1983 provides in pertinent part: "Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State...subjects, or causes to be subjected, any citizen of the United States...to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress."

[30] See *Monroe v. Pape*, 365 U.S. 167 (1961).

[31] *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 930 (1982) (quoting *Flagg Brothers v. Brooks*, 436 U.S. 149, 155-56 (1978)).

[32] 102 S.Ct. 2727 (1982).

[33] *Daniels v. Williams*, 106 S. Ct. 662 (1986). See also *Sacramento v. Lewis*, 118 S.Ct.1708 (1998).

[34] *Monell v. Department of Social Services of the City of New York*, 436 U.S. 658 (1978).

[35] *City of Canton, Ohio v. Harris*, 489 U.S. 378 (1989).

[36] Examples of federal circuit courts expressly finding no such (pre*Dickerson*) §1983 liability include: *Giuffre v. Bissell*, 31 F.3d 1241, 1256 (3d Cir.1994), *Bennett v. Passic*, 545 F.2d 1260, 1263 (10th Cir.1976), *Warren v. City of Lincoln, Neb.*, 864 F.2d 1436, 1442 (8th Cir.1989), and *Thornton v. Buchmann*, 392 F.2d 870, 874 (7th Cir.1968). The only federal circuit that allowed such §1983 actions was the Ninth Circuit. See *Cooper v. Dupnik*, 963 F.2d 1220 (9th Cir.1992), and *California Attorneys for Criminal Justice v. Butts*, 195 F.3d 1039 (9th Cir. 1999) (holding that not only was the §1983 action appropriate, but the police officers involved were not entitled to qualified immunity when they continued to question the suspects/plaintiffs after they invoked their *Miranda* rights).

[37] The standard for qualified immunity is "[G]overnment officials performing discretionary functions, generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). See also *Anderson v. Creighton*, 483 U.S. 635, 640 (1987), in which the Court defined what constitutes a clearly established right:

> The contours of the right must be sufficiently clear that a reasonable official would understand that what he is doing violates that right. This is not to say that an official action is protected by qualified immunity unless the very action in question has previously been held unlawful,...but it is to say that in the light of pre-existing law the unlawfulness must be apparent.

> ***"...questioning 'outside Miranda,' now may provide the basis for a lawsuit alleging a federal Constitutional violation."***

[38] *See Reser v. Las Vegas Metropolitan Police Department*, 242 F.3rd 383, 2000 WL 1585648 (9th Cir.(Nev.)) (October 20, 2000) where the court affirmed entitlement of qualified immunity in a §1983 lawsuit to a detective for actions occurring during an interrogation that occurred prior to the *Dickerson* decision. The court explicitly said that because the interrogation occurred before the *Dickerson* decision, the Constitutionality of *Miranda* warnings had not been clearly established at the time of the interrogation.

[39] 42 U.S.C. §1983, at subsection LVII.

[40] 42 U.S.C. §1988(b).

[41] Sun Tzu, *The Art of War* (Boston, MA: Shambhala, 1991). This is a translation of an ancient Chinese work of unknown original date.

[42] Incriminating statements made involuntarily under the Due Process Clause may never be used for any purpose. *Arizona v. Fulminante*, 499 U.S. 279 (1991).

[43] *Harris v. New York*, 401 U.S. 222 (1971). Ironically, Dickerson's suppressed confession eventually was used against him at trial to impeach his in-court testimony.

[44] While the defendant's statement would be excluded from trial, the discovery of the witness and, thus, the witness' trial testimony would not be viewed as "fruit-of-the-poisonous-tree." *Michigan v. Tucker*, 417 U.S. 433 (1974).

[45] A suspect must reasonably believe (from the perspective of an objectively reasonable *innocent* person) that he or she is in custody, regardless of the intention of the interrogating law enforcement officer. See *Stansbury v. California*, 114 S. Ct. 205 (1988). Also, there must be interrogation. That is, questioning or its "functional equivalent," which is reasonably likely to illicit incriminating information. See *Brewer v. Williams*, 430 U.S. 387 (1977) and *Rhode Island v. Innis*, 446 U.S. 291 (1980). For *Miranda* warnings to be legally required, both custody and interrogation must be present. If a suspect is in custody, warnings need not be given until interrogation begins. Likewise, if a suspect is not in custody and is being questioned by the police, warnings need not be given.

[46] See *Colorado v. Connelly*, 107 S. Ct. 515 (1987) for an excellent example of this. Connelly, who had brutally murdered a young girl, walked up to a police officer on a street corner in Denver and began explaining to the officer what he had done. Connelly was clearly neither in custody nor was the police officer interrogating him. But as soon as the officer understood this involved a possible murder he abruptly interrupted Connelly and gave *Miranda* warnings and continued to interrupt Connelly's attempts at unburdening his conscience to ascertain if Connelly was insane or under the influence of something. The officer was unwary as to the requirements of *Miranda* and attempted to compensate by grossly exceeding the requirements. See also Judge Harold J. Rothwax, *Guilty - The Collapse of the Criminal Justice System*, (New York, NY: Warner Books, 1997), 66-69, for poignant commentary on this case.

[47] The Court in *Dickerson*, as noted above, opined that *Miranda* is easier for law enforcement officers to conform to, and for courts to apply in a consistent manner, than the totality-of-the-circumstances test. They make no mention of countless incriminating statements that were never made because of unnecessary or excessive *Miranda* warnings and the impact this has had on the legitimate interests of criminal justice.

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.

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 their exemplary service to the law enforcement profession.

Officer Nicholls

While patrolling the Intracoastal Waterway in the City of Hollywood, Florida, Officer Tim Nicholls observed a 24-foot cabin cruiser on fire. After notifying the dispatcher, Officer Nicholls responded to the scene to find the boat occupied by a father and his three children. As the boat's engine burned, Officer Nicholls disregarded his own safety, boarded the burning vessel, and rescued all four occupants. After ensuring the occupants reached the safety of his police boat, Officer Nicholls then attempted to suppress the flames with a fire extinguisher. Unsuccessful at his attempts, Officer Nicholls tied a line to the burning boat and towed it to the boat ramps and awaited the fire department. Although the vessel sustained more than $15,000 in damage, Officer Nicholls' selfless actions saved the lives of three small children and their father.

Officer Rousselle

After responding to a 911 call of domestic violence at a residence, Officer David Rousselle of the North Tonawanda, New York, Police Department began searching for the male suspect who fled the scene. Shortly after, Officer Rousselle spotted the suspect in his vehicle, stopped the vehicle, and attempted to question the man; however, the suspect insisted that he was going home and proceeded to drive away. The suspect pulled in front of his residence and remained in his locked vehicle communicating with Officer Rousselle through a partially opened window. After learning his arrest was imminent, the suspect retrieved a gasoline can from inside his vehicle and began pouring gas on himself and reiterated threats that he was not going back to jail and that he was going to kill himself. When Officer Rousselle noticed that the man had a lighter and was attempting use it, he immediately broke the window and safely removed the gasoline-soaked suspect from the vehicle, without regard for his own personal safety. Officer Rousselle's quick thinking and selfless actions prevented a 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

Subscribe Now

United States Government
INFORMATION

Order Processing Code:
* 5902

☐ YES, please send _____ subscriptions to:
FBI Law Enforcement Bulletin (FBIEB) at $36 each ($45 foreign) per year.
Price includes regular shipping & handling and is subject to change.

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

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!