



Law Enforcement Executive
FORUM

Police Training: Investigation

September 2007

Law Enforcement Executive Forum
Illinois Law Enforcement Training and Standards Board Executive Institute
Western Illinois University
1 University Circle
Macomb, IL 61455

Senior Editor

Thomas J. Jurkanin, PhD

Editor

Vladimir A. Sergevnin, PhD

Associate Editors

Jennifer Allen, PhD

Department of Law Enforcement and Justice Administration,
Western Illinois University

Barry Anderson, JD

Department of Law Enforcement and Justice Administration,
Western Illinois University

Tony Barringer, EdD

Division of Justice Studies, Florida Gulf Coast University

Lewis Bender, PhD

Department of Public Administration and Policy Analysis,
Southern Illinois University at Edwardsville

Michael Bolton, PhD

Chair, Department of Criminal Justice and Sociology, Marymount University

Dennis Bowman, PhD

Department of Law Enforcement and Justice Administration,
Western Illinois University

Becky K. da Cruz

Criminal Justice and Law & Society, Armstrong Atlantic State University

Jose de Arimateia da Cruz

Political Science & Comparative Politics, Armstrong Atlantic State University

Weysan Dun

Special Agent-in-Charge, FBI, New York Division

Kenneth Durkin, MD

Department of Law Enforcement and Justice Administration,
Western Illinois University

Thomas Ellsworth, PhD

Chair, Department of Criminal Justice Sciences, Illinois State University

Larry Hoover, PhD

Director, Police Research Center, Sam Houston State University

William McCamey, PhD

Department of Law Enforcement and Justice Administration,
Western Illinois University

John Millner

State Senator of 28th District, Illinois General Assembly

Stephen A. Morreale, DPA

School of Public Policy & Administration/Criminal Justice, Walden University

Gregory Boyce Morrison

Department of Criminal Justice and Criminology, Ball State University

Michael J. Palmiotto

Wichita State University

Frank Morn

Department of Criminal Justice Sciences, Illinois State University

Associate Editors (cont.)

Gene L. Scaramella, PhD

Dean of Graduate Studies, Ellis College of New York Institute of Technology

Wayne Schmidt

Director, Americans for Effective Law Enforcement

Editorial Production

Document and Publication Services, Western Illinois University, Macomb, Illinois

Production Assistant

Linda Brines

The *Law Enforcement Executive Forum* is published six times per year by the Illinois Law Enforcement Training and Standards Board Executive Institute located at Western Illinois University in Macomb, Illinois.

Subscription: \$40 (see last page)

ISSN 1552-9908

No part of this publication may be reproduced without written permission of the publisher.

Disclaimer

Reasonable effort has been made to make the articles herein accurate and consistent. Please address questions about individual articles to their respective author(s).

Table of Contents

Editorial	i
Vladimir A. Sergevnin	
Police Training: Investigations	
Making the Collar: Theories of Criminal Investigation	1
DeVere D. Woods, Jr.	
Using Investigative Interviewing Strategies Over the Telephone: Outcomes of an Innovative Training Program	9
Catherine Layton	
John Nixon	
Murray Lee	
Paper or Plastic: The Need for Standardized Training and Knowledge Regarding Evidence Collection and Preservation	21
Vicky J. Blair	
A Quick Look at Interrogation	33
Adam Kasanof	
Mandatory Recording of Criminal Interrogations: Issues and Policy Considerations	45
James N. Gilbert	
Legal, Scientific, and Forensic Controversies Over Spectrographic Voice Analysis for Identification or Elimination	51
Herbert Joe	
Al Yonovitz	
A Police Investigation Meets Forensic Accounting	59
Timothy Pearson	
Richard A. "Dick" Riley, Jr.	
Your Investigation and the Media	73
Rick Rosenthal	
The Legality of Canine Sniffs and Motor Vehicle Stops Revisited	81
Barry M. Anderson	
Terry M. Mors	
Our Panoptical Society Where the Invisible Becomes Visible	85
Jill Joline Myers	

Law Enforcement Personnel

The Process and Utility of Psychological Fitness-for-Duty Evaluation in Law Enforcement	135
--	-----

Marva Dawkins
Marvin P. Dawkins
Amanda Reyes
Stephen Griffin

Career Paths: Maximizing Talent and Performance	149
--	-----

Lynn A. Tovar

Use of Force

Police Use of Force: Does Gender Make a Difference?	155
--	-----

Lorene M. Sandifer
O. Elmer Polk
Alejandro del Carmen

The Relationship Between Ethical Ideology and Ethical Decisionmaking Among Experienced Police Officers	171
---	-----

Dennis W. Catlin
James R. Maupin

Terrorism

Bioterrorism Preparedness: The Interdependent Relationship of the Local, State, and Federal Governments	187
--	-----

Fee F. Habtes

Materials/publications are available through the Illinois Law Enforcement Training and Standards Board Executive Institute.

Editorial

Criminal investigation represents a controversial and highly desirable field of scientific study. In support of the overall law enforcement mission, criminal investigators serve the American public by investigating potential criminal violations in a manner that fosters confidence in the criminal justice system and compliance with the law. One of the most important aspects of being a criminal investigator is training. It is crucial that investigators and support personnel maintain the highest levels of ethical, technical, tactical, and personal training proficiency.

Emerging technology and science along with advanced modern criminal investigation techniques offer new horizons of efficiency in this challenging field of law enforcement.

This collection of articles stresses the practical procedures, techniques, and applications of investigations to provide readers with a solid, current view on criminal investigations; it is designed to blend modern theories of crime detection with a practical approach to criminal investigation. Focus topic papers were written with the perception that criminal investigation is a field that relies heavily on the past experiences of investigators as well as on recent practical and technological innovations. Related articles seamlessly integrate coverage of modern investigative tools alongside discussion of established investigation policies, procedures, and techniques for the law enforcement officer.

This issue features updated and enhanced understanding of such critical topics as theories of criminal investigation, investigative interviewing strategies, collection and preservation of the evidence, interrogations and their recording, dealing with media, and terrorism and homeland security. It is intended to meet the needs of law enforcement executives and others interested in criminal investigation by presenting previously unpublished research results and best practices summaries. It is important to note that all the articles view both the uniformed officer and the criminal investigator as vital partners in the pursuit of success for every criminal investigation.

The editors of this issue hope that it will serve the needs of law enforcement executives and officers by instilling a desire for further exploration of true knowledge and skills in the field of criminal investigation.

“The first duty of a man is the seeking after and the investigation of truth.”

– Cicero, 106 BC–43 BC, Roman author, orator, and politician

Vladimir A. Sergevnin, PhD
Editor
Law Enforcement Executive Forum

Making the Collar: Theories of Criminal Investigation

DeVere D. Woods, Jr., PhD, Associate Professor, Department of Criminology & Criminal Justice, Indiana State University

Introduction

The scene opens, and we are introduced to two attractive and interesting characters. We are quickly drawn into their lives, but before we really get to know them, one murders the other. As the perpetrator makes his escape, something innocuous happens. We might not have noticed it, if not for the camera temporarily lingered on this image. This is a crucial moment. The perpetrator has just committed the mistake that will ensure his capture, but it will take the special skills of our detective to solve this crime.

The above scenario is a formula used in television programs such as *Colombo*. Week after week, Lieutenant Colombo would emerge after such a scenario to restore justice. Crime dramas, such as *Colombo*, are important because they present a theory of how investigators solve crimes. Each week, Lieutenant Colombo would reveal a murderer in essentially the same manner. Though his style was predictable, it was entertaining watching him develop his case. It also provided something most criminal investigation textbooks do not—a theory of criminal investigation. My purpose is to explore some themes to stimulate discussion in developing a useful theory of criminal investigation.

The Essence of Criminal Investigation

How do investigators solve crimes? When asked, many criminal investigators are likely to respond by describing a procedure that has worked for them, a feeling they had about the case, or a fortunate circumstance. Few offer a theoretical basis for the work they do. This is to be expected. Practitioners face pressing demands that require them to effectively process the work at hand. They often have little time or desire to ponder theory. As a criminal investigator, I also focused on resolving each case so I could move on to the next. I did this by doing what had worked in the past or trying what I thought might be productive under the circumstances. When a case was solved or deemed unsolvable, I moved on with little regard to why my tactics succeeded or failed. If I recognized a mistake, I would try to correct it in the future, but there was little time for comprehensive analysis. When something works, you have little reason to question it. When something fails, you move on to something else.

For practitioners, results are important. Theory is an academic exercise often perceived to have little value. This belief is common and long standing. In the 1880s, Alphonse Bertillon met resistance from the Paris police for attempting to inject “mere scientific theory” into police work (Gilbert, 2007). Practitioners want to know what works, not necessarily why it works. As a police supervisor, I once had a conversation with a new officer completing his bachelor’s degree. At the beginning of a new semester, he expressed his frustration with the pace of his

course by commenting, "I wish they would just tell us what we are supposed to do and forget all this theory crap!" This was a concept I may have also embraced as an undergraduate student. Theory and history are often wasted on the young.

The adage "if it's not broke, don't fix it" seems appropriate, but what if what you are doing does not work or it does not work well? It is then we need to turn to theory to improve our efforts. We need to know how something works or why it should work to correct it. Theory development might be the work of academics, but when it comes to criminal investigation, even academic textbook writers have offered little to aspiring investigators.

A Review of Textbooks

I began with a selection of current and past edition criminal investigation textbooks. These are not presented as a representative sample of textbooks in the field, but they do provide an overview of commonly used texts. A more stringent sampling frame might produce a different result, but my review showed that criminal investigation textbooks tend to be similar in their approach and vary more in style than substance. The manuscripts vary in writing style, order of presentation, and depth of detail in specific areas. Selecting a text is likely influenced by publisher support, philosophical agreement or disagreement with an approach, certain factual errors, or cost.

Most of the textbook writers discuss the qualities or skills needed to be a good investigator. Authors differ on the skills and qualities they propose, so I will focus on the most common and include some unique attributes. Some stress the importance of professional training and experience to become a good investigator (Brandl, 2004; Gilbert, 2007; Swanson, Chamelin, & Territo, 2003). Investigators need to possess skills in criminalistics and collecting evidence and have an understanding of criminal and constitutional law (Becker, 2005; Gilbert, 2007; Lyman, 2005; Pena, 2000; Weston & Lushbaugh, 2006).

Aside from being well-trained, good investigators need to possess certain personality characteristics. The ability to think logically (Bennett & Hess, 2007; Brandl, 2004; Gilbert, 2007; O'Hare, 1970) and use inductive and deductive reasoning (Becker, 2005; Brandl, 2004; Gilbert, 2007; O'Hare, 1970; Swanson et al., 2003) are commonly cited. Investigators must work systematically (Bennett & Hess, 2007; O'Hare, 1970; Pena, 2000; Swanson et al., 2003) and be resourceful, self-disciplined, verbal (Becker, 2005; Brandl, 2004; Horgan, 1974; Pena, 2000; Swanson et al., 2003), psychologically well-balanced (Bennett & Hess, 2007; Gilbert, 2007), as well as observant and suspicious (Horgan, 1974; Pena, 2000), and loyal (Horgan, 1974).

Most texts imply that good investigators are special because of these qualities and skills, but these traits can be developed through determination and hard work. Detectives are not innately unique. Horgan (1974) states the investigator must possess ordinary intelligence and common sense, but Becker (2005) contends that the investigator needs exceptional organizational skills.

A few authors (e.g., Becker, 2005; Horgan, 1974) rely upon Locard's Exchange principle, though they fail to credit the principle to Locard. Simply stated, Locard maintains that an exchange occurs between the crime scene and anyone

(particularly the perpetrator) who enters. He contends that the perpetrator leaves traces of his or her presence at the crime scene and takes something away. Locard's theory is commonly presented and credited in criminalistics textbooks (not covered here). O'Hare (1970) disputes the usefulness of this concept, believing it leads to a common misconception that all crimes are solvable.

Criminal investigation textbooks commonly describe investigative procedures by type of crime. Within each discussion, you can generally find a profile of the crime itself and some demographic information for the perpetrators. Little is presented on the psychological processes of the perpetrator and his or her impact on the investigation. Bennett and Hess (2007) briefly mention that criminals make mistakes that lead to some evidence being left behind. Brandl (2004) contends that mistakes by the perpetrator are crucial to solving crimes.

Few criminal investigation textbook authors present a theory of investigation. When they do, theory often is mentioned briefly and not developed. Lyman (2005) states that criminal investigation is both art and science; whereas, O'Hare (1970) agrees it is an art but disputes it is a science. O'Hare contends that calling criminal investigation a science is fiction; it is useful for discussing techniques but has no basis in reality.

Brandl (2004) is one of the few textbook authors to propose a theory for criminal investigation. He attempts to equate investigation to information theory. Investigation is a struggle for information with the perpetrator sending signals and the investigator attempting to collect them. The perpetrator is the source for all evidence, and the investigator must find it. A few authors suggest using the scientific method as a framework for investigation (Becker, 2005; Gilbert, 2007).

The Turner Approach

As a student, I learned criminal investigation from Dr. Ralph Turner. Turner was a criminalist who was the laboratory supervisor for the Kansas City Police Department before turning to academia. His abilities were well recognized, and they earned him an appointment to the Senate Committee investigation team that reinvestigated Senator Robert Kennedy's assassination (Berg, n.d.; Hamby, n.d.).

Turner's theory of investigation focused upon mistakes made by the perpetrator. He felt that criminals were psychologically compelled to make mistakes. Turner argued that every child is raised by someone who is a product of society. During child rearing, social norms are taught. Children are instructed in how to behave. When a child's behavior does not conform to expectations, the child is punished. The child learns that improper behavior requires punishment. Even if the caregiver is of questionable morality, enough of society's norms are imprinted upon the child, and he or she develops a sense of what is right and what is wrong. The caregiver may choose to reject society's norms, but the child still learns to distinguish between right and wrong.

For Turner, this early training in social norms can never be fully rejected. People may choose to do wrong, but in doing so, they cannot escape knowing they deserve to be punished. No matter how much they plan to avoid detection, they fall victims

to their own conscience. Turner was not saying that criminals consciously want to get caught but that they are betrayed by their subconscious.

In Freudian terms (though Turner did not use them to present his theory), the superego imposes itself on the baser actions of the id or ego (Freud, 1970). The superego betrays our attempts to deceive. The guilty child can find relief in getting caught because betrayal can be unbearable for the more transparent psyche. The criminal may not consciously want to be exposed and may be actively seeking to cover his or her crime, but deep within the superego lies the guilty child subtly betraying him or her.

Development of Criminal Investigation

As American policing began a reformation in the 20th century, criminal investigators became the focus of professional crime fighting. A movement grew to train investigators in sophisticated tactics and technologies with more specialized functions (Moore & Trojanowicz, 1988). Investigators’ level of training and status within the organization grew as they become the elite crime fighters. Their greater skills, abilities, and experience qualified them to continue an investigation beyond the efforts of other law enforcement personnel (Wilson, 1963). This “professional model” envisioned police investigators as highly trained and centrally controlled (Klockars, 1995). Detectives became information processors guided by common sense and the culture of the organization. No theoretical structure was developed.

Modeling a Theory

To address this deficiency in the development of criminal investigation, I have constructed four rudimentary models. They are derived from academic concepts and popular perceptions. Textbooks are the most likely source of information for students. The media is the most likely source of information for both students and the public—who are potential jurors. These models focus on the two principal actors in a criminal investigation: (1) the investigator and (2) the perpetrator.

Attention is focused on the investigator’s skills or talents and the perpetrator’s mistakes. This is not the only way to construct models, but it employs the most common assumptions of criminal investigation. Most textbooks focus on the investigator’s skills. Popular entertainment and Turner emphasized both the skills of the investigator and the importance of mistakes by the perpetrator.

Table 1. Perpetrator’s Mistakes/Investigator’s Ability

Investigator’s Ability	Perpetrator’s Mistakes	
	Not Focused	Focused
Extraordinary	<p>Model I Good v. Evil</p>	<p>Model II Colombo</p>
Normal	<p>Model III Professional</p>	<p>Model IV Turner</p>

Model I pertains primarily to fictional accounts of investigation. This model focuses upon the high level of skill or the exceptional talents of the investigator. Less attention is paid to actions of the perpetrator. Investigation is seen as a classic struggle of good versus evil. A detective stands above all others as a superhero. The detective possesses extraordinary skills, such as encyclopedic knowledge, exceptional powers of observation, and uncanny powers of reasoning. From Sherlock Holmes to Tony Shalhoub's Monk, no criminal can escape the investigative prowess of these detectives.

Model II focuses upon the skills of the investigator and the mistakes of the perpetrator. This model is also commonly portrayed in the media. This detective is heroic but does not possess supernatural powers or qualities. The investigator is highly skilled or has exceptional talents, but he or she needs to find the mistake made by the perpetrator to solve the case. Here, Lieutenant Colombo uses his finely developed skills to trap the perpetrator with his or her own mistakes.*

Model III views the investigator as someone who is trained and competent but does not possess exceptional abilities or talents. Hard work and diligence by the investigator is rewarded with success. The focus is on the investigator, not the perpetrator. Everyone makes mistakes, so we can expect them from criminals, too, but that is not the basis of investigation. Methodical dedication to detail leads the investigator to success. This model derives from reform, or professional, philosophies and the ideas of people like August Vollmer and O. W. Wilson and possesses many of the investigative skills and qualities described by textbook authors.

Model IV focuses upon the mistakes of the perpetrator. These mistakes are the perpetrator's downfall. Similar to Model II, once the investigator uncovers the perpetrator's mistake, the investigation is well on the way to being solved. Unlike Model II, the Model IV investigator does not possess extraordinary skill or talent. He or she is competent, well trained, and hard working but does not necessarily possess extraordinary innate ability. This model accepts many of the assumptions of Model III but focuses on the errors made by the perpetrator as the key to solving crimes. Turner's theory of criminal investigation fits here.

Conclusion

In reality, criminal investigations reflect some of each of these models. Investigators may seem to fall into more than one category. Even fictional detectives cross beyond the narrow constraints of specific models. It is not likely that any of us will

* The differences between these three fictional detectives—Colombo, Monk, and Sherlock Holmes—may at first seem trivial. Once they are on the case, the result is inescapable. The perpetrator will be foiled. His or her mistakes will be used against them. There is a fundamental difference, though, between a Colombo and a Monk or Holmes. Colombo needs to uncover the mistake to bring the offender to justice. Until it is exploited, the case cannot be solved. Monk and Holmes may also turn a case on a mistake by the perpetrator, but for them, it is more than a single act. The mistake is only one element of numerous observations and deductions they have amassed. They overwhelmed the perpetrator with their observations, knowledge, and reasoning skills. At the conclusion of one of Colombo's cases, we often feel that, but for one mistake, the perpetrator would have escaped his crime. For Monk and Holmes, once all the facts are amassed, the conclusion is elementary.

develop super powers, but some individuals are exceptionally gifted. A chance behavior or intuitive reaction can make an investigator appear exceptionally talented. An unforeseen happenstance can make a perpetrator appear inept and an investigation inanely routine. The question becomes whether these models are useful, and if so, how do we use them? If not, how can we better conceptualize criminal investigation?

Each of these models reflects social values. Model I can be found in popular entertainment as the struggle between good and evil. Though the abilities of the detective are unrealistic, this model reaffirms social norms. Good must conquer evil. Even in a lawless society, good will rise up to punish evil. Social norms must be maintained. We must value and strive to maintain our social norms. Unfortunately, this concept can become corrupted with glorified violence and an associated message that the ends justify the means.

Many of the social characteristics of Model I apply to Model II. Once again, we are looking at a popular theme in entertainment, but the protagonist and villain are made to appear more realistic. Both are formidable. Good conquers evil because our exceptionally talented detective will exploit the criminal's fatal mistake. This model also promotes social norms and is subject to the same possibility of abuse.

Model III most accurately reflects American policing. Detectives have no superpowers or abilities, but they can succeed through diligence. This model reflects the Reformation philosophies of policing and the content of textbooks on criminal investigation. The detective is principally an information processor who sorts disparate facts into a meaningful picture. The model conforms to the socially prescribed work ethic and promotes social values through the perception of deterrence. Wrongdoers face a cadre of talented and dedicated investigators who work meticulously to bring them to justice. This model, however, does little to explain how the detective will accomplish this task.

Model IV accepts the principles of Model III within a theory of human behavior. Well-trained investigators focus their attention on mistakes made by perpetrators. Model III investigators also do this, but in Model IV, it is part of the design. Dr. Ralph Turner articulated this model in his classroom. It reaffirms many of the social values of the other models.

I have used Turner's theory to guide my investigations. I can offer no proof to support Turner's theory that criminals are compelled to leave behind clues. As an investigator working on a difficult case, I was challenged to find evidence of such behavior. Solving cases is difficult work, and criminals seem uncooperative. Turner's theory, though, is useful. Both as a crime scene investigator and when teaching investigation, I relied on Turner's theory. It is a useful motivational tool. If you adopt Turner's theory, you must also accept the challenge to find evidence. It is the fundamental assumption of his theory. You may not find the evidence you seek, but the failure becomes yours, and you are pressed to continue your search. Others may find Turner's premise improbable, and they may need to find alternative assumptions to guide their investigations. Insight into the nature of criminal investigation will benefit from continued discussion.

References

- Becker, R. F. (2005). *Criminal investigation* (2nd ed.). Boston: Jose & Bartlett Publishers.
- Bennett, W. W., & Hess, K. M. (2007). *Criminal investigation* (8th ed.). Belmont, CA: Thompson Wadsworth.
- Berg, S. O. (n.d.). Reminiscences of the pre and early AFTE years: The 1975 re-examination and testing of the Robert Kennedy firearms evidence. Retrieved June 15, 2007, from www.afte.org/AssociationInfo/a_berghistory.htm
- Brandl, S. G. (2004). *Criminal investigation*. Boston: Pearson, Allyn and Bacon.
- Freud, S. (1970). *A general introduction to psychoanalysis*. New York: Pocket Books.
- Gilbert, J. N. (2007). *Criminal investigation* (7th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Hamby, J. E. (n.d.). The history of firearm and toolmark identification. Retrieved June 15, 2007, from www.firearmsid.com/A_historyoffirearmsID.htm
- Horgan, J. J. (1974). *Criminal investigation*. New York: McGraw Hill.
- Klockars, C. B. (1995). The Dirty Harry problem. In V. Kappeler (Ed.), *The police and society: Touchstone readings* (pp. 329-356). Prospect Heights, IL: Waveland Press.
- Lyman, M. D. (2005). *Criminal investigation: The art and the science* (4th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Moore, M. H., & Trojanowicz, R. C. (1988, November). Corporate strategies for policing. *Perspectives on policing*, Number 6. Washington, DC: National Institute of Justice, Department of Justice.
- O'Hare, C. E. (1970). *Fundamentals of criminal investigation* (2nd ed.). Springfield, IL: Charles C. Thomas Publishers.
- Pena, M. S. (2000). *Practical criminal investigation* (5th ed.). Incline Village, NV: Copperhouse Publishing Company.
- Swanson, C. R., Chamelin, N. C., & Territo, L. (2003). *Criminal investigation* (8th ed.). Boston: McGraw Hill.
- Weston, P. B., & Lushbaugh, C. A. (2006). *Criminal investigation* (10th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Wilson, O. W. (1963). *Police administration* (2nd ed.). New York: McGraw Hill.

DeVere D. Woods, Jr., PhD, is an associate professor in the Department of Criminology and Criminal Justice at Indiana State University. He is a former police investigator, who now consults and researches policing issues. His current research includes community policing, police management, policy implementation, criminal investigation, and crime analysis. He is a previous contributor to the *Law Enforcement Executive Forum Journal*.

Using Investigative Interviewing Strategies Over the Telephone: Outcomes of an Innovative Training Program

**Catherine Layton, PhD, Sub-Dean (Learning & Teaching), Faculty of Arts,
School of Policing Studies, Australian Graduate School of Policing,
Charles Sturt University**

John Nixon, MA, Lecturer, Charles Sturt University

**Murray Lee, L1B, Lecturer, School of Policing Studies, Charles Sturt
University**

This article outlines a training program developed for conducting investigations and interviews over the telephone by call-center operators to handle potentially fraudulent small insurance claims. Historically, it has not been economically feasible to investigate these claims by traditional means, and they were paid out by the insurer without scrutiny. The training involved the adaptation of existing models of investigative interviewing through the identification of core principles. Significant reductions in fraudulent claims were reported by the insurance agency in question. While the training itself focused on the needs of the insurance industry, we suggest that the positive outcomes have implications for call-center behaviours and investigation practices in the wider policing context. It is posited that the core principles and a simplified model may well form the basis of any investigative interview, from the short interview in the field to the detailed recorded interview.

Introduction

The fields of cognitive and social psychology have had a major impact on police interviewing techniques over the past 20 years, resulting in different styles of interviewing suspects and witnesses. Research now suggests that the most effective interviews are conducted by people who have some knowledge of the science and psychology of interviewing, a wide range of practical tools upon which to draw, and substantial practice in a learning environment and those who are supervised and given feedback on their real-life interviews (Griffiths, Retford, & Milne, 2006; Schollum, 2005).

This does not mean that there is a unitary or clear path forward for interviewers, managers, or trainers. For example, the PEACE model of interviewing (outlined below) was first used in England and Wales from 1993, but evaluations in 2000 and 2001 showed that it had not lived up to expectations (Schollum, 2005). Schollum (2005) gives the following reasons for this result: minimal support from management and supervisors, inconsistent implementation and resource allocation, and poor transfer of skills from classroom to workplace. Moreover, others comment that the model places considerable cognitive demands upon the interviewer; therefore, memory enhancing components are not regularly implemented, the lack of time to prepare for interviews is a problem, and the PEACE model itself is perceived to be inflexible (Dando, Wilcock, & Milne, 2006; Walsh & Milne, 2006).

Another influence of psychology on investigative interviewing concerns the skills and ability of an investigator to determine the validity of information gathered during an interview. Research has shown that experienced and inexperienced investigators alike have difficulty distinguishing truth from deception during an interview (Kassin & Fong, 1999; Vrij, 2000). Much of the research conducted into the application of deception detection by law enforcement has been in relation to criteria-based content analysis (CBCA), which is the forensic analysis of written statements; however, findings here also suggest caution. Research conducted into the effectiveness of Scientific Content Analysis (SCAN) training for the United Kingdom's Home Office found no clear evidence that the training significantly improved an experienced investigator's ability to ascertain the validity of written statements. It was shown, however, to be effective in highlighting parts of an interviewee's account that required further inquiry (Smith, 2001).

These problems, however, may reflect an attempt to apply theory to practice, rather than work with theory, practice, and research simultaneously and generate new knowledge across all three. It is important not to see adaptations of investigative interviewing theory and research as lesser versions of a "pure" process. They are, rather, part of the process of enhancing our understanding and increasing our capacity to make good judgments about what best to do in a particular situation (Carr & Kemmis, 1986, p. 93; Usher, 1991, p. 308; Usher & Bryant, 1989, p. 67). It is important, then, to build upon the tools and knowledge one does have—that is, the PEACE, Cognitive Interview (CI), and Conversation Management (CM) models, as well as CBCA, and everyday experiences (in this case, teaching police and police students).

While there is research into the fit between an adapted PEACE model and fraud sector investigative interviews (Shawyer & Milne, 2006), it has involved the examination of tape recordings of live interviews. Here, we focus on the critical assessment of what might be needed in the call-center environment with a concomitant review of the effectiveness and impact of training in that call-center. We consider the background to the training program and how existing models of investigative interviewing might best be adapted to the call-center context. Also considered is the development of core interviewing skills and a simplified model of deception analysis. We go on to provide a brief overview of the outcomes of the training program before considering the implications of our experiences for police investigations and training.

Background

In late 2005, the Centre for Investigative Studies and Crime Reduction (CISCR) at the Australian Graduate School of Police Management (AGSPM) was approached by one of the major financial/insurance organisations in Australia and New Zealand to develop a training course in investigative interviewing. CISCR is an initiative of Charles Sturt University to provide practical training and education for investigators and industry professionals in the areas of fraud, compliance, and criminal intelligence. An integral part of all investigator courses is training in investigative interviewing, which focuses on the PEACE, CI, and CM models.

The PEACE model of investigative interviewing, as developed by law enforcement in the United Kingdom and introduced to policing in Australia by Charles Sturt

University's School of Policing Studies (SOPS) in 1997, is considered to be the benchmark of best practice for a structured approach to investigative interviewing in Australia. PEACE is an acronym representing a foundational structure that is applicable to any interview situation, whether it be an interview conducted with a cooperative or uncooperative subject (Milne & Bull, 1999; Ord, Shaw, & Green, 2004; Shaw, 1996). The constituent elements of the PEACE model as taught to law enforcement in Australia are as follows:

- **Planning & Preparation** – background/aims and objectives/legal considerations/logistics
- **Engage & Explain** – building rapport/explanation of the interview process and procedures to be followed/invite questions
- **Account** – the information-gathering stage of the PEACE model in which either the CI or CM model is applied, depending on the subject being interviewed. There are three core skills that are also applied at this stage: (1) the use of open questions, (2) active listening, and (3) comprehensive note-taking
- **Closure** – summarise main points/maintain rapport/future actions/invite questions
- **Evaluation** – information obtained/investigation in light of information obtained/performance

The CI model, as developed by Geiselman and Fisher (1985), has been taught to both police recruits and experienced investigators as the best practice model for “. . . improving completeness and accuracy of eyewitness accounts . . .” (Schollum 2005, p. 58). This model is founded on memory enhancement techniques, which are applied in a structured manner, varying from a 12-step model (Stacey 1997a) to a modified 5-step model for recruits (Mary Dorahy, personal communication, March 4, 1999).

The CM model, as developed by Shepherd (1986), has also been taught through SOPS and CISCRA as the best practice model for gaining information from suspects and uncooperative witnesses, as modified for Australian jurisdictions (Stacey, 1997b). The CM model promotes ethical practice in interviews with subjects who are silent, hostile, lying, and evasive and give “no comment” responses (Milne & Bull, 1999, p. 187; Shepherd, 1986). The focus of the questioning technique in the CM model is on challenging interviewees on errors and discrepancies in their version of events, as well as the disclosure of evidence implicating the suspect.

Unlike the investigative interviewing courses already developed and delivered by CISCRA, all of which were all designed for face-to-face interviewing in the context of law enforcement, the client was interested in developing practices similar to those used by some insurers in the United Kingdom—in which telephonists, trained in CI and CBCA, conduct interviews with potentially fraudulent claimants with the aim of identifying fraudulent claims and obtaining a withdrawal of the claim by the insured.

Owing to the expense of engaging private insurance investigators on potentially fraudulent claims, it had not been seen as economically viable to investigate low-

dollar value claims (under \$5,000 AUD, or approximately \$3,750 USD). As a result, these “small” claims were not being investigated, and the extent of fraudulent claims was unknown, as were the costs to corporate profits. There were concerns about continuing this practice, however, given the results of research that showed that 7% of persons surveyed had committed insurance fraud, and a staggering 48% refused to rule out making a fraudulent claim in future dealings with insurance companies (Association of British Insurers, 2003). Although the client was aware of the need for fraud reduction and detection through investigation in this area, it was recognized that a method of investigation had to be developed that incurred minimal costs but still achieved effective results in detecting and reducing fraud. CISCR was invited to develop a training program along similar lines to that used in the United Kingdom.

In the field of insurance, there have been few studies on the effectiveness of these emergent investigative interviewing techniques, despite the proliferation of research in policing and law enforcement. There appeared to be no standard interviewing process for loss adjustors (Fahy & Greenford, 2006; Greenford, 2001), let alone for call-center operators, despite the high-cost implications to the industry. In 2004, the exaggeration of legitimate insurance claims was believed to be the most prolific form of fraud, and on a basis of 10% of all claims being fraudulent in one way or another, the costs to the industry were estimated at \$2.1 billion AUD or \$73 AUD per insurance policy (IAG & The Economist Intelligence Unit, 2004). It is interesting to note that this estimate of the cost of insurance fraud in Australia had almost doubled from \$1.4 billion AUD in a 1997 study (Baldock, 1997). The expectations of the client were that trained telephone investigators would be able to achieve savings of up to \$1 million AUD (approximately \$750,000 USD) initially and become a powerful fraud prevention tool for the future.

Adapting the Models

Given that the SOPS and CISCR existing courses were, at face value, unsuitable for the task at hand, it was decided to modify the existing models of investigative interviewing—the PEACE, CI, and CM models. So far as CBCA was concerned, there were no existing courses, given the very limited application of CBCA in Australian law enforcement practice. It was considered evident that the PEACE model could be readily adapted from policing to the telephone interview, as it is a sound, well-researched, flexible, and proven structure to approach any investigative interview. The difficulty arose in the Account stage of the PEACE interview and designing a model of deception detection to be incorporated into the new training package.

As noted above, either the CI or CM models are used (depending on the degree of cooperation by the subject) to gather the interviewee’s account of events under investigation. In the context of law enforcement, interviews are generally conducted face to face, and the interviewing officer should be able to clearly define the two categories of interviewee and which model to apply. The interviewee in the context of a telephone interview, however, is an unknown entity and may be either a genuine or fraudulent claimant. The challenge was to cater for the client’s specified needs. Although the client had requested training in the CI model, it was pointed out that the CI model was clearly unsuitable for telephone investigation, so it was necessary to design an adapted model.

The CI model as used by law enforcement is predicated on face-to-face interviewing, with the use of numerous memory retrieval triggers (e.g., sketching, sensory imagery, and reverse recalls), which are unsuitable for use over the phone. There are suggestions that the CI techniques of context reinstatement, imagery, and reporting “everything” are more about rapport and improved communication than they are about recall (Memon, Wark, Holley, Bull, & Koehnken, 1997) and that the overall approach increases not only correct information but also incorrect information and confabulation (Memon & Stevenage, 1996).

What was needed was an interview model that could be used whether the claimant was genuine or fraudulent. A simplified model was needed for our prospective learners, who were telephonists or call-center operators with no investigative background at all. Another factor to be considered in the simplification of the models was the limited training time available.

Furthermore, there were concerns over a recurring problem with the teaching of these models that had been identified in the course of facilitating interviewing workshops at both SOPS and CISC (with detectives from all Australian jurisdictions, private and public sector investigators, as well as student police). There was an overall model of PEACE interviewing, which people were able to understand and apply relatively easily. When the idea that other interview models (CI and CM) had to be applied at the Account stage of the PEACE model was presented, students had difficulty conceptualizing what was required. They became confused about the relationship between the three different models. This problem had been acknowledged in the United Kingdom, during a revision and updating of the PEACE training package, by dispensing with the terms *CI* and *CM* to reduce the number of labels used (Clarke & Milne, 2001, as cited in Schollum, 2005, p. 48). This issue was considered in the design of an adapted model for telephonists.

To design this new model, both the CI and CM models were analysed for aspects that would be applicable in creating one model for the Account stage in the PEACE model for telephone interviewing. The CM model seemed to have a lot of the necessary structures to meet the needs of telephone interviewing. Very few aspects of the CI model seemed applicable, except for the commonalities CI had with CM, and it was on this basis that the new telephone interview model was designed. Both the CI and CM models can be simplified into two distinct phases or agendas: (1) the interviewee’s phase or agenda and (2) the interviewer’s phase or agenda. Working from these commonalities and the useful structure of the CM model, a much simplified interview model could be designed for use at the Account stage of a PEACE investigative interview. This new model could cater to both types of claimants, and there would be no need to teach the concepts behind two different interviewing models.

With a much simplified single model, the next most important aspect of the training, which had been informed by our own experiences teaching investigative interviewing, was the need to focus on the core skills of interviewing. These skills revolved around communication strategies for building and maintaining rapport, active and critical listening, questioning, and note-taking. No matter what model is used, interviewing will not be effective without the investigators being competent in these core skills. The necessity to master these skills informed the manner in which the experiential learning component of the training was to be designed,

namely the conduct of role-play interviews, critiquing, and debriefing, which were to form the vast majority of the course schedule.

When we turned to the issue of CBCA, research indicated that the investigator would face additional problems in dealing with identified claims, as the interviews would always be conducted by telephone. When taking details from a claimant over the telephone, the investigator is unable to utilize the full range of deception detection techniques available in face-to-face dealings to determine whether the claim is fraudulent or otherwise, such as using videotapes to detect fleeting and rapidly suppressed facial expressions preceding a lie (as outlined by Frank & Ekman, 1997) or the use of CBCA for written statements (Vrij & Mann, 2006).

The use of CBCA, while not able to unequivocally discern lies from truth, could be seen as a helpful tool for the telephone investigator. Even in its typical use in traditional investigation, there were recognized benefits that would be of use in telephone investigation. As noted above, it could be useful to identify a possibly deceptive area in the claimant's version (Smith, 2001). Following a limited review of literature available on methods of deception detection (Adams, 2002; Burgoon, Buller, & Floyd, 2001; Canter & Alison, 1999; Nance, 2003), a simple method advocated by Walters (2000), which incorporated most of the major points arising from research, was seen to fit the needs of inexperienced people for whom training time was limited. Walters' (2000) *The Truth About Lying: How to Spot a Lie and Protect Yourself from Deception* became a prescribed text for course participants so that they could make continued reference to it as their interviewing skills developed and experience increased.

As part of the course, participants would be trained to use a checklist (based on Walters, 2000) for identifying areas of possible deception, both when engaged in the actual interview and also when reviewing the recording of their interviews. When the triggers for deception were identified in the live interview, the telephone investigator was to focus in-depth questions on those areas, when checking and confirming the complainant's version. Detailed questioning was seen as the most effective method of defeating a claimant's deception or evasion, as having to expand on lies during prolonged questioning places great cognitive demands on the fraudulent claimant. This meant that there would potentially be increased discrepancies and errors in their version, which would be put to the claimant. There was also the back-up of the recorded interview to pick up deception triggers missed during the live interview, which could be further questioned in a subsequent interview.

In consultation with the client, it was decided that there would be a need for two distinct interviews to be conducted, if the interviews were to have the desired result of identifying and reducing fraudulent claims. The first interview conducted would be purely an information-gathering exercise and would be recorded with the consent of the interviewee. The purpose of this first interview was to gather substantially more detailed information from the claimant about the circumstances of the claim than would be gathered when the claim was first lodged. In this first interview, the telephone investigator is expanding on the claimant's version of events to a much higher level of detail than was required by the initial call-center taking the claim. The questions asked of the claimant by the claims call-center were merely *pro forma* and not adaptive for in-depth information gathering.

By the completion of this interview, the claimant would be tied to a detailed account of the circumstances surrounding the claim. Taking the detailed information gathered during this first interview, the investigator is now able to check the accuracy of the claimant's version of events, through the use of corporate databases, police reports, telephone companies, information sourcing companies, other publicly available information (e.g., on the Internet), as well as other people nominated in the claim. This would allow for the confirmation of a legitimate claim or the identification of inconsistencies and outright deceptions.

This behind-the-scenes investigation would then become the basis of the second interview. Initially, it would determine whether there was a need for a second interview, based on the information gained, indicating a possible fraudulent claim or the verification for payment of a legitimate claim. If the second interview was needed, it would be one that challenged the claimant about the legitimacy of the claim. The claimant would be given the opportunity to confirm his or her earlier account of the circumstances surrounding the claim. The points that would then be at issue, from any inconsistencies or deception identified, could then be challenged. The claimant would then be given the opportunity to explain or withdraw the claim.

Outcomes of the Program

The program was delivered to five staff members over a 5-day initial course. All were drawn from call-centers within the organisation, having sound knowledge of the insurance products but (with the exception of the team leader) with no experience in investigation or interviewing. The program itself was team-taught by Murray Lee and John Nixon, on the client's premises, with the team leader as support, particularly in relation to the specifics of the client organisation and insurance generally. This location was invaluable because it allowed access to corporate databases; telephone recording equipment; liaison with management; and, importantly on the last day, access to claim files and the ability to make actual calls with real claimants.

As a result of a follow-up monitoring session about a month later, some interesting results were noted. The telephonists were very smoothly applying the simplified PEACE model without any reported difficulties. Their core skills of investigative interviewing were already showing marked improvement, as were their capacities in picking up on deception and evasion cues and questioning the identified areas within the live interview. Most importantly, they were achieving a remarkable result of uncovering approximately one fraudulent claim out of every four claims made.

Implications for Policing

There are several implications of this experience with training insurance telephone investigators for police, particularly given the marked trend towards telephone reports of crimes, disorder, and disputes. In New South Wales, for example, there is a dedicated Police Assistance Line (PAL) for reporting of non-urgent crime, such as breaking and entering and theft when the perpetrator is no longer on the premises. The call-center operators on PAL take an initial report and from the information gained and discerned, determine whether the attendance of police to conduct further investigation is necessary.

Using the model developed here allows police to work from call-center data, which is richer in detail and relevant information, with little contamination of evidence, as opposed to information gathered according to *pro forma* questions. Research also indicates that the sooner the follow-up contact by investigating police, the better, but sooner is not necessarily the rule in busy police commands. Hope and Fisher (2006) report in a recent study that the completeness and accuracy of information provided by witnesses, through using a "Scene of Crime Recall Tool" (a self-administered checklist, based on cognitive interviewing principles) as soon as possible after the event, supports an increase in the number of details available for later recall. If timely information-gathering from victims and witnesses is necessary after an event, the use of a telephone interview conducted by trained operators may be a viable option when a face-to-face interview cannot be arranged within a short period of time. These findings also raise the question of possibly expanding the role of call centers, such as PAL, in future police investigations.

Finally, our experience in teaching investigative interviewing, and therefore, our experience in teasing out what is essential for learners who are largely going to be involved in investigating low-level crimes, for which little time is available, has allowed us to demonstrate the adaptability of research-based models of interviewing to the practice environment. We can see this principles-based approach allowing for police to select their interview approach and meeting quite specific and sometimes unusual demands.

Conclusions

The focus of this project was to adapt investigation skills to a specific environment, drawing on research into investigation and deception detection and our own experiences in education. The approach was not to put theory on a pedestal, but to employ it in ways that might best meet the needs of learners and the organization alike. To achieve these goals, a simplified model of investigative interviewing, based on the PEACE, CI, and CM models, was developed.

At its most basic level, the model described here can be used in training investigators with no experience in criminal investigation to conduct quality investigative interviews in simple investigations. It is also suggested, however, that the model can be adapted and enhanced with various investigative tools for use at much higher levels of criminal investigation, perhaps through a staged process of training that allows for periods consolidating particular skills in the field. Indeed, a significant finding of this project was the importance of training focused on the core skills of investigative interviewing and the development of deception detection skills. By focusing on the substance of an interview, as opposed to a complex and demanding structural approach, the inexperienced interviewer may be more able to develop higher order interview skills. Further research is required into the balance of these core skills with the intent to refine teaching practice and investigative practice alike.

Finally, while the training itself focused on the needs of the insurance industry, we suggest that the extremely positive outcomes have implications for call-center behaviors and investigation practices in the wider policing context. It is posited that this simplified model, along with the emphasis on core interviewing skills,

may well form a foundation for improved interview practice, from the short interview in the field to the detailed recorded interview.

References

- Adams, S. H. (2002). *Communication under stress: Indicators of veracity and deception in written narratives*. Unpublished doctoral dissertation, Virginia Polytechnic Institute and State University, Falls Church.
- Association of British Insurers. (2003). *Tackling fraud*. Retrieved June 25, 2007, from www.abi.org.uk/Display/default.asp?Menu_ID=946&Menu_All=1,946,0&Child_ID=148
- Baldock, T. (1997). Insurance fraud. *Trends and issues in crime & criminal justice*, No. 66. Retrieved June 25, 2007, from www.aic.gov.au/publications/tandi/ti66.pdf
- Burgoon, J. K., Buller, D. B., & Floyd, K. (2001). Does participation affect deception success? A test of the interactivity principle. *Human Communication Research*, 27(4), 503-534.
- Canter, D., & Alison, L. (Eds.). (1999). *Interviewing and deception. Offender profiling series: Vol. 1*. London: Ashgate, Dartmouth.
- Carr, W., & Kemmis, S. (1986). *Becoming critical: Education, knowledge and action research*. Melbourne: Deakin University.
- Dando, C., Wilcock, R., & Milne, R. (2006, July 3-7). *Victims and witnesses of crime: Inexperienced police officers' investigative interviewing behaviour*. Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Fahy, H., & Greenford, B. (2006, July 3-7). *Exploring the role of adjustors' investigating insurance claims*. Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Fisher, R. P., & Geiselman, R. E. (1992). *Memory enhancing techniques for investigative interviewing: The cognitive interview*. Springfield, IL: Charles C. Thomas.
- Frank, M., & Ekman, P. (1997). The ability to detect deceit generalizes across different types of high stakes lies. *Journal of Personality and Social Psychology*, 7(6), 1429-1439.
- Geiselman, R. E., & Fisher, R. P. (1985). Interviewing victims and witnesses of crime. *National Institute of Justice Research Brief* (NCJ-99061).
- Greenford, B. (2001). *The management of personal injury claims by insurers in England and Ireland*. Unpublished doctoral dissertation, University of East Anglia, Norwich, UK.

- Griffiths, A., Retford, S., & Milne, R. (2006, July 3-7). *Is all training good training? A comparison study of two different witness interview training programs*. Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Insurance Australia Group (IAG) & The Economist Intelligence Unit. (2004). Hidden costs: Insurance fraud in Australia. Retrieved June 25, 2007, from <http://iag.com.au/pub/iag/results/submissions/media/20041119a.pdf>
- Hope, L., & Fisher, R. (2006, July 3-7). *Immediate interviewing: Supporting eyewitness memory with a self-administered scene of crime recall tool*. Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Kassin, S. M., & Fong, C. T. (1999). "I'm innocent!" Effects of training on judgments of truth and deception in the interrogation room. *Law and Human Behavior*, 23, 499-516.
- Memon, A., Wark, L., Holley, A., Bull, R., & Koehnken, G. (1996). Interviewer behaviour in investigative interviews. *Psychology, Crime and Law*, 3, 135-155.
- Memon, A., & Stevenage, S.V. (1996). Interviewing witnesses: What works and what doesn't. *Psychology*, 7(6). Available online at www.cogsci.ecs.soton.ac.uk/cgi/psyc/newpsy?7.06
- Milne, R., & Bull, R. (1999). *Investigative interviewing: Psychology & practice*. West Sussex, UK: John Wiley & Sons, Ltd.
- Nance, J. (2003). *Conquering deception* (2nd ed.). Kansas City, MO: Irvin-Benham.
- Ord, B., Shaw, G., & Green, T. (2004). *Investigative interviewing explained*. Australia: LexisNexis Butterworths.
- Schollum, M. (2005). *Review of investigative interviewing*. Wellington, New Zealand: Office of the Commissioner of Police.
- Shaw, G. (1996, January 5). The new PEACE. *Police Review*, 104(5350), 26-27.
- Shawyer, A., & Milne, R. (2006, July 3-7). *Fraud and PEACE*. Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Shepherd, E. (1986). Conversational core of policing. *Policing*, 2, 294-303.
- Smith, N. (2001). Reading between the lines: An evaluation of the Scientific Content Analysis technique (SCAN). *Police Research Series, Paper 135*. London: Home Office.
- Stacey, H. (1997a, July). Cognitive interviewing. *Policing Issues and Practice Journal*, 36-40.

- Stacey, H. (1997b, October). Investigative interviewing: Conversation management. *Policing Issues and Practice Journal*, 7-14.
- Usher, R. (1991). Theory and metatheory in the adult education curriculum. *International Journal of Lifelong Education*, 10(4), 305-315.
- Usher, R., & Bryant, I. (1989). *Adult education as theory, practice and research: The captive triangle*. New York: Routledge.
- Vrij, A. (2000). *Detecting lies and deceit: The psychology of lying and the implications for professional practice*. London: Wiley.
- Vrij, A., & Mann, S. M. (2006). Criteria-based content analysis: An empirical test of its underlying processes. *Psychology, Crime & Law*, 12(4), 337-349.
- Walsh, D., & Milne, R. (2006, July 3-7). *Are government investigators in the UK giving PEACE a chance? Are they keeping the PEACE when undertaking investigative interviews? Is there actually PEACE in our time?* Paper presented at the Second International Conference on Investigative Interviewing, Portsmouth, Hampshire, UK: University of Portsmouth.
- Walters, S. B. (2000). *The truth about lying: How to spot a lie and protect yourself from deception*. Naperville, IL: Sourcebooks.

Catherine Layton, PhD, has worked in police education since 1989, beginning her career with the NSW Police. In 1994, she began working with Charles Sturt University in the Constables Development Program, writing and delivering distance education packages (in subjects such as crime prevention, problem-oriented policing, supervision, multiculturalism, and safe custody) for an associate's degree offered at that time. Crime prevention has since become her main area of teaching, both within the School of Policing Studies and the Australian Graduate School of Policing.

Her research has combined her interest in how people learn with her teaching role. Her PhD focused on how police students' identities changed through their participation in a community placement. She was awarded a HERDSA Fellowship in 2006 and is currently Sub-Dean (Learning and Teaching) in the Faculty of Arts.

John Nixon, MA Ed (Adult Education), has taught in a variety of educational institutions including primary schools, technical and further education colleges, and Charles Sturt University. He has taught in learning difficulties areas, communication for police and security guards, and investigative interviewing. He has successfully completed the Investigators' and Commercial Crime short courses with Charles Sturt University and is currently enrolled in the Graduate Certificate of Fraud Investigation. In the fraud area, he has been involved in designing and implementing courses for fraud prevention for insurance agencies.

Murray Lee, LLB, has been working for Charles Sturt University at the School of Policing Studies since May 2002. He served for 10 years with the Australian Federal Police, working principally in the areas of Covert Services, Intelligence, and Drug Operations. He has also worked as an investigator with the NSW Ombudsman, investigating complaints against members of the NSW Police. He has also worked in the security industry and as a paralegal/advocate for a Sydney law firm, practicing in the areas of industrial law and conveyancing.

He has taught on a wide variety of subjects in both the internal and distance programs at associate and bachelor degree levels, including Communication in Policing, Police as Investigators, Law & Society, Investigative Interviewing, and Evidence & Investigation. He also teaches at and coordinates short courses for the Centre for Crime Reduction & Investigative Studies.

Paper or Plastic: The Need for Standardized Training and Knowledge Regarding Evidence Collection and Preservation

Vicky J. Blair, MS, Certified TCLEOSE Instructor, Crime Scene Consultant

Whether a civilian or a member of a law enforcement agency, some people tend to think that every crime scene holds a wealth of information. While this is true in some cases, it is not likely to be the case the majority of the time. No matter the amount of evidence available, the problem lies in the fact that it may or may not be identified, collected, preserved, or processed correctly. Contaminated or invalidated evidence can preclude a suspect identification, force a crime to remain unsolved, or allow a guilty person to be acquitted. The quandary remains on how to do the job most effectively and with universal precision.

Bellefeuille et al. (2003) describe the protocol standards for DNA evidence recovery, which can also be used when collecting other types of evidence. Officers or criminalists entering a crime scene must remain keenly alert to the possibility that evidence could be all around them. They must be "diligent to protect the evidence and the crime scene from post-crime transfer of DNA, and this is what is commonly referred to as contamination" (Bellefeuille et al., 2003, p. 730). When collecting evidence, especially a murder weapon, it is recommended that an investigator changes gloves often to avoid site-to-site contamination; double gloving makes it easy to discard one pair while still protecting the officer's or criminalist's hands and the integrity of the evidence (Bellefeuille et al., 2003).

The international quest for forensics is to have every agency informed and properly trained, thereby replicating the proficiency standards that have been carefully outlined. Not only do the requirements include the need to preserve ethical and personal standards; objectiveness; and respect for liberty, equality, and justice, they also include a need for each individual involved in a forensic crime scene career to be adequately trained and obtain certification in the area(s) in which they participate. Testing procedures are strict, and an acute knowledge of the area of specialty is required (IAI, 2006). In spite of this, some agencies are not up to date on their training, knowledge, or skills, which may result in either wrongful convictions or no convictions at all. Wrongful convictions can happen, no matter whose case it is; however, it is not just the one who committed the original error who suffers the consequences. Imprisonment, years of legal battles to clear one's name, and death may result from flawed evidentiary testimony.

In *Herrera v. Collins*, 506 U.S. 390, 1993, Chief Justice William Rehnquist presided over the appeal request of Lionel Torres Herrera who requested that his conviction be overturned because new evidence proved his factual innocence. By a vote of 6-3, the Supreme Court rejected his request stating, "Since appeals are based on issues of law rather than those of fact, claims of actual innocence alone are deemed irrelevant" (Rehnquist, 1993, Summary section, para. 1). The Supreme Court

further holds that the “execution of a factually innocent person, if condemned, would violate neither the 8th Amendment’s prohibition of cruel and unusual punishment nor the 14th Amendment’s protection of an individual’s right to due process” (Rehnquist, 1993, Summary section, para. 1). Herrera, an innocent man, was eventually executed (McBride, 1995).

Every piece of evidence related to a crime must be handled with care. The most simple and basic item that should be remembered at all crime scenes is gloves, whether latex or nitrile. Other types of gloves, like the ones used to make deli sandwiches, are extremely thin and prone to leak. Many are made of vinyl, which creates a whole new array of problems. Should a latex glove be too thin, the wearer is apt to leave his or her own fingerprints on anything touched, which could be very detrimental to an investigation. If gloves leak, it is highly likely that blood, biological evidence, or processing chemicals will come into contact with the wearer. These are not viable options. Gloves may come with or without powder on the inside, but they do not come with built in germicidal protection. Again, an easy way to deter problems of this nature is to wear two pairs of gloves. Handling evidence with gloves on, yet acting carelessly, could remove latent fingerprints or other trace evidence from the surface of the item. Gloves do not allow arbitrary actions to take place. Evidence should be handled as minimally as possible, whether by gloved hands, hemostats, or tweezers, and then properly packaged.

The type of packaging used to preserve evidence depends partly on the type of evidence collected. Most evidence, even if wet, can be placed in paper bags and transported safely to the department for final packaging and/or processing. Paper bags are capable of breathing—allowing air to enter and exit the bag—and are less likely to promote evidence spoilage. With that in mind, however, one must be certain that wet evidence has had the opportunity to thoroughly air-dry prior to packaging and placing it in the evidence facility because moisture can seep through the paper bag and cross-contaminate other evidence, or the original evidence itself could decay. Even if evidence does not appear to contain moisture, condensation may eventually form inside a plastic bag; firearms can rust and biological evidence can be destroyed (Texas Department of Public Safety, 1997).

Evidence security and survival can be relatively simplistic. The knowledge and skills needed to ensure the integrity of every piece of evidence is not overly onerous to learn. Basic techniques and applications could become second nature to anyone in law enforcement charged with the duty of evidence collection, provided training classes and pocket-sized evidence handbooks—like CliffsNotes®—are made available to them.

Shelef and Elkayam (1997) of the Israel National Police conducted research relating to the hazards that field investigators in Israel encounter, which prompted them to devise a system that would be beneficial to all involved. Because the investigators in Israel are charged with working multiple scenes concerning explosives or chemicals (i.e., weapons of mass destruction), the first concern was in regards to the safety of all personnel involved in evidence collection, handling, and processing. Next, they needed to tackle the issue of evidence preservation and analysis. Finally, unreliable chain-of-custody issues were addressed. For assistance in determining their best course of action, Shelef and Elkayam (1997) relied heavily on the writings of Barry Fisher and the FBI.

The first issue was handled by simply equipping field personnel with protection equipment other than just gloves, so face masks, protective footwear, and safety goggles were issued. Field personnel were then instructed on the proper usage of these supplies (Shelef & Elkayam, 1997). In addition, Shelef and Elkayam (1997) constructed evidence collection kits that contained some basic, but essential, items: plastic and nylon evidence bags, glass containers, paper wrapping, cardboard boxes, and plastic containers for sharp objects. Finally, evidence bags bearing preprinted chain-of-custody forms were obtained. The chain-of-custody form would now “follow” the evidence from collection to the lab and on to the court-room (Shelef & Elkayam, 1997). These three simple steps greatly increased the preservation of evidence, which substantially improved the reliability of the laboratory test results and thereby had a significant impact on the conviction rates in Israel.

The Federal Bureau of Investigation (FBI) developed *The Handbook of Forensic Services* (2004), which suggests specific procedures for safe and effective methods of collecting, preserving, packaging, and transporting evidence. It also lists explicit procedures for forensic examinations. This handbook is available to any agency that requests it.

Various law enforcement agencies offer an array of classes that are open to officers and civilians from other agencies. The Texas Department of Public Safety (TxDPS) regularly holds training classes and seminars regarding forensic work. In 2001, the Knoxville, Tennessee, Police Department conceived the idea for a National Forensic Academy, where new criminalists and those with informal training would spend 10 weeks learning the specifics of the job. The training would be intense; however, it would be extremely beneficial not only to the criminalist but also the crime laboratory and the judicial process (National Forensic Academy, 2001).

Aside from classroom and online training, many crime scene investigation texts are available. One of the most respected books is *Techniques of Crime Scene Investigation* by Barry Fisher. Over 500 pages of knowledge cover the methods of applying assorted forensic techniques, professional ethics, expert witness testimony, health and safety issues, and the need for teamwork, along with photographs to explain and enhance the information (Daher, 2000).

Improper training can lead to horrendous results. In 2004, the Houston Police Department’s Toxicology Unit was closed down after a 28-year veteran examiner failed to pass a competency test that was needed for laboratory accreditation. Prior to that event, a Harris County (Houston) Texas ballistics expert was killed as he prepared to test a firearm. The weapon had never been cleared of ammunition, and the examiner assumed it had been. Even the FBI, which is insistent on guidelines and proper technical applications, is not above reproach; they have canceled the use of a lead analysis test used in ballistics examinations due to altered data by laboratory personnel. Had the individuals in Houston and the FBI been properly trained, supervised, and/or followed pertinent guidelines, these events could have been avoided (“Houston PD,” 2004).

It is not that there is a lack of desire by personnel to do their very best in every case; it is that there is a lack of funding and training. Former U.S. Attorney General Janet Reno took notice of this situation and made the following comment in 2000:

Actions taken at the outset of an investigation at a crime scene can play a pivotal role in the resolution of a case. Careful, thorough investigation is key to ensure that potential physical evidence is not tainted or destroyed or potential witnesses overlooked. While many agencies have programs in crime scene processing, the level of training and resources available varies from jurisdiction to jurisdiction, as does the opportunity to practice actual investigation. . . . the guide is one method of promoting quality crime scene investigation. The type and scope of a crime scene investigation will vary from case to case. Jurisdictions will want to carefully consider the procedures in this guide and their applicability to local agencies and circumstances. (TWGCSI, 2000)

The guide she refers to is published by the Department of Justice and is titled "Crime Scene Investigation: A Guide for Law Enforcement." The research and finished work was compiled by the Technical Working Group for Crime Scene Investigation (TWGCSI) in 2000.

The International Association of Chiefs of Police established a code of ethics for law enforcement personnel in 1957, which is repeated at academy graduation exercises around the globe and is considered morally binding throughout the career of an officer. A poignant statement at the end of the code states, "I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence" (Grant, 2002).

Dr. Saferstein (1998), in his book *Criminalistics – An Introduction to Forensic Science*, states, "forensic science occupies an important and unique role in the criminal justice system—a role that relates the scientist's ability to supply accurate and objective information that reflects the events that have occurred at a crime" (Saferstein, 1998, p. 2). A criminalist, like a scientist, must be trained and qualified to do the job right; not just anyone is capable of collecting evidence correctly, just as not everyone is capable of being a cop. Also, a good criminalist utilizes his or her mental peripheral vision because there is no room for mental blindness.

Are law enforcement agencies trained sufficiently enough to collect evidence on everything from a burglary of a vehicle to a homicide? The intent of this research is to determine the training and knowledge levels of Texas municipal police departments, constables, city marshals, sheriff's departments, the Department of Public Safety state troopers, and Texas Rangers to ascertain whether these participants perceive their current level of training to be sufficient or whether more is necessary and to establish whether they realize that funding is available to assist them in obtaining the knowledge and skills needed to advance their capabilities and correct any possible deficiencies in the area of evidence handling.

Methodology

In order to determine the training and knowledge levels of the various law enforcement agencies in Texas, a list of every local, county, and state agency was compiled; however, some of the listed police agencies include campus police and district attorneys' offices, which were summarily omitted. The primary list was divided into subcategories to include police departments, sheriff's offices,

Texas Rangers, state police, city marshals, and constables. Stratified random sampling was used to select one-third of the agencies from each subcategory for participation in this study, which increased the representative nature of the samples and decreased possible sampling errors. The agencies in each subcategory were listed in alphabetical order. Starting point numbers were randomly selected for each category; then every third agency on each list was selected.

Survey questionnaires were sent to the supervisor of each selected agency along with explicit instructions regarding their voluntary participation in the study, their right to discontinue participation at any time, and the necessary response time. These questionnaires were divided into three sections: (1) a demographic survey, (2) a perspective analysis, and (3) a knowledge exam. The demographics to be considered included size of agency, type of agency, length of service, rank, age, respondent's gender, and prior evidence collection training.

The perspective survey contained statements regarding training and funding in the respondent's department and were patterned using the Likert Scale. The responses were numbered 1 through 3, with 1 being "agree," 2 being "no comment," and 3 being "disagree."

The method used to test the respondents' knowledge of various evidentiary procedures was an exam containing 25 representative questions drawn from the State of Illinois Basic Evidence Technician Final Exam (ET exam). Questions included categories relating to evidence (e.g., trace, biological/blood, ballistics, tool marks, footwear impressions), fingerprints, photography, crime scene investigation, and safety issues. Using the ET exam in its original formatted order, a randomly selected starting point number of 3 was chosen, and every other question from that point on was selected for use. The exam was graded accordingly: 90-100 = A, 80-89 = B, 70-79 = C, and 69 or below = F.

The knowledge exam scores were combined with the demographic survey to determine the collective knowledge of the respondents and whether or not agency size, type, length of service, rank, age, gender, or prior training determine knowledge level. The demographic survey variables were also combined with the results of the perspective analysis to determine whether agency size, type, length of service, rank, age, gender, or prior training determine the amount of evidence training received and the amount of money spent on training. Additionally, the knowledge exams were combined with the perspective analyses to determine whether the respondents' knowledge levels were associated with their perspectives. Finally, the incorrect answers on the knowledge exams were analyzed to determine whether there were any general misconceptions, what they might be, and what particular information may need to be addressed through additional or updated training programs.

MicroCase statistical software, version 4.7 (1987-2001) was used to analyze the data. Descriptive and inferential statistics were reported. The data was analyzed using the Chi Square test of statistical significance and related measures of association. Measures of association were used to summarize the strength of a relationship and whether the relationship was positive or negative.

The questionnaires were summarized using frequency distributions to show the number of participants in each score level on the knowledge exam (e.g. 5 participants scored 99%, 15 participants scored 87%, etc). In addition, the measures of central tendency were determined and conveyed in percentage distributions and graphs. Cross-tabulations were utilized in order to compare the percentage distributions of the variables and determine whether they were associated, which included bivariate frequency and percentage tables to show any positive, negative, or curvilinear relationships between the variables.

Data Analysis

In order to complete the task of data collection, survey questionnaires were mailed to 1,000 Texas law enforcement agencies in the following increments: 370 state troopers, 258 municipal police departments, 230 constables, 83 sheriffs' offices, 39 Texas Rangers, and 20 city marshals. Responses were received from 79 municipal police department employees, 33 state troopers, 27 sheriffs' office employees, 20 constables, 8 Texas Rangers, and 4 city marshals for a total of 171. The return rate per agency was 33% for sheriffs' offices, 31% for municipal police departments, 20% for city marshals, 20% for Texas Rangers, 9% for state troopers, and 7% for constables, with an overall return rate of 17.1%.

Demographic Survey

Each rank was represented, although chiefs and sheriffs were shown to have completed one-third of the surveys. As such, more respondents listed their current duty assignment as "other," meaning their duties include, but are not limited to, the administrative functions of police work. A majority of responding agencies reported having 49 employees or less. Most of those employees (65.9%) stated they have received 40 hours or more of forensic crime scene training. Of the respondents, 153 were male, 17 were female, and one did not report a gender. Due to the unrepresentative nature of the number of female respondents, state troopers, city marshals, and constables, postulations toward the general population of female law enforcement officers, state troopers, city marshals, and constables would be pure conjecture; therefore, they are not listed as individual reporting variables. The information garnered from their responses, however, was used in the broad spectrum of the data analysis.

Perspective Survey

Nearly three-fourths (73.8%) of all respondents felt that their agency operated efficiently with the forensic knowledge it currently had, yet more than half (55.4%) of the respondents were not required to attend at least one crime scene processing class offered by another agency, and less than half (44.9%) regularly offered in-house training classes. Most respondents (83.9%) felt they would benefit from additional forensic training, while few (15.5%) maintained they did not collect much evidence or need additional evidence collection training. One hundred twenty-one agencies (72.5%) conveyed that they had written instructions regarding evidence handling or procedures, while 28 (16.8%) stated they did not.

Of the respondents, 90.6% stated that their agency expected their employees to have at least a minimal amount of evidence collection and handling knowledge.

Only 22.2% depended on another agency when it came to collecting evidence. Fewer than half (43.9%) of the respondents reported that their agency had a crime scene unit that handled a majority of their evidence collection, with only 35 agencies (20.5%) employing civilians in the unit. Only 16 agencies (9.4%) believed that they should have all civilians in their crime scene unit.

Forensic training funds were placed in the annual budget by 72 (42.1%) of the agencies, but for 66 (38.6%) of the agencies, they were not. Only 32 (18.7%) agencies obtained grant money for forensic training. When respondents attended a training class on their own time, slightly more than half (52.0%) of the agencies were reimbursed for their expenses. Nearly half (49.7%) of the agencies admitted to spending more on office supplies than they did on forensic training, and 22.8% refused to comment on this issue.

Knowledge Exam

Of the 171 respondents, nine did not complete the knowledge exam, and one only answered the first three questions. Sixty-one respondents received a score of 69% or less (35.7%), and only two (1.2%) scored a 90% or above; none received a score of 100. Excluding the 10 exams that were not completed, 37.3% of the respondents surveyed failed the Knowledge Exam.

Additional areas of interest arise when combining the Knowledge Exam scores with the Perspective Analysis variables. Comparing the Knowledge Exam scores to the Perspective Analysis statement, "Your agency operates efficiently with the forensic knowledge it currently has," shows that 43 of the agencies that believe they operate efficiently failed the Knowledge Exam.

When comparing the Knowledge Exam scores to the Perspective Analysis statement regarding in-house training classes, of those that agreed, 27 failed the Knowledge Exam, and 23 of those who disagreed failed. Overall, 37.7% of the respondents that failed the exam reported that their agency does not offer in-house training classes. Fifty-six respondents stated that their agency required them to attend a crime scene processing class offered by another agency, and 93 said theirs does not; of those that do not, 44.3% failed. More than half (55.7%) of the agencies that failed the Knowledge Exam did not send someone to a state or international forensic conference. Of the 171 respondents, 155 reported that their agencies expected their employees to have at least a minimal amount of evidence collection and handling knowledge, yet close to one-third (32.7%) of them failed the exam.

Seventy-two respondents stated that their agency regularly put forensic training funds in the annual budget, and 66 said they did not; of those that did not, 23 failed. While a majority (101) of the respondents did not receive grant money for forensic training, of those who said their agency did not, 37 of the respondents failed the Knowledge Exam. Eighty-five respondents stated that their agency spent more money on office supplies than it did on forensic training, and of those, 32 (37.6%) failed the exam. Nearly one-third (29.5%) of respondents who failed the Knowledge Exam stated their agency would not reimburse their expenses if they attended a training class on their own time.

Of the respondents, 121 said that their agency provided written instructions regarding evidence handling or procedures, yet 46 (38%) of them failed the exam. With that in mind, 73 respondents admitted their agency had a problem with evidence that was contaminated by other evidence, and 28 of them failed the exam. Of the agencies that had secured property and evidence rooms, 36.9% did not pass the exam.

Finally, the Knowledge Exam scores were combined with the Demographic Survey Variables and the Perspective Analysis Variables and examined for statistical significance (see the following table).

Knowledge Exam Scores by Demographic Survey Variables and Perspective Analysis Variables

Variable	Chi-Sq.	df	Sig.	V	C	Lambda
Exam Scores/Agency Size	15.906	8	p<.05	.216	.292	.026
Exam Scores/Assignment	47.057	20	p<.01	.262	.465	.040
Exam Scores/Minimal Knowledge	22.265	12	p<.05	.208	.339	.032
Exam Scores/Processes for Latents	27.513	12	p<.01	.232	.372	.052
Exam Scores/Processes for DNA	21.157	12	p<.05	.203	.332	.038
Exam Scores/Benefit from More Training	40.332	12	p<.001	.280	.437	.014
Exam Scores/Spends More on Office Supplies than Training	25.237	12	p<.02	.222	.359	.061

Conclusions

The main finding of this study is that there is a severe deficit of knowledge in evidence identification, collection, and preservation procedures among Texas law enforcement officers. The main value of this information lies in the realization of the need of continuing professional education in this area. Due to the low number of respondents, however, these results cannot be applied to the general law enforcement population nationwide; any assumptions made would be pure conjecture.

More than one-third (approximately 37%) of the respondents failed to achieve a minimum passing score of at least 70% on the Knowledge Exam. Furthermore, only two of 171 respondents attained a score of at least 90%. Worse, those engaged most directly in handling physical evidence fared poorly. Nearly half (approximately 48%) of those with a current assignment of patrol/traffic and approximately 34% of detectives did not receive a passing grade. Most alarmingly was that almost one in five (approximately 18%) respondents who reported their primary assignment as “crime scene unit” failed the examination. The potentially negative consequences of these findings include a failure to identify offenders, wrongful convictions of innocent persons, and the release of guilty persons due to improperly collected, handled, processed, or preserved evidence.

The data showed that approximately 31% of the respondents whose agency did not offer in-house training failed the Knowledge Exam. Approximately 54% of the respondents were not required to attend training offered by another agency; of those, 27 failed the exam. Nearly 34% of the respondents whose agency did not put forensic training funds in the budget and approximately 36% who did not obtain

grant money for forensic training scored 69% or less. While it is unknown how much is spent on forensic training by the agencies of those who passed the exam, it is apparent that any amount is better than no amount. An increase in forensic training funds would increase the accuracy, reliability, and professionalism of law enforcement personnel.

Even though most respondents (124) felt that their agencies operated efficiently with the forensic knowledge they currently had at the time of the study, over 34% of them did not pass. These results convey that while the respondents may perceive that their agency maintains competence in this area, over one-third of them did not possess enough personal knowledge to achieve a minimum passing score. Of the 73 respondents who stated that their agency never had a problem with evidence contamination, 28 (approximately 38%) of them failed the Knowledge Exam. This means that although they believed that their agency did not have problems with contamination, they were unqualified to identify contaminating factors. Approximately 38% of the respondents whose agency maintained written evidence handling and procedures scored 69% or less; this proposes that either the written procedures contained errors, or they were not emphasized and implemented. Whatever the case may be, their evidence handling and procedures manuals should be reviewed and/or updated.

According to the answers received on the Knowledge Exam, areas that may benefit from additional forensic training concern the manner and means by which to handle and collect trace evidence, OSHA requirements and bio-hazard issues, the proper sequence of events when processing a crime scene, camera operations and photographic techniques, the collection and handling of impression evidence, and class characteristics of nonbiological evidence. Additional research in the areas of mentioned deficiencies and the methods by which to facilitate the training necessary to correct them may be warranted. In all, the data shows that the amount of training received by Texas law enforcement agencies directly affects the individual knowledge level of each employee; therefore, the hypothesis is accepted, and the null hypothesis is rejected.

Recommendations

It is known by various agencies and organizations that inadequacies in these areas do exist, and efforts are being made to help correct them; however, the use of these programs is not widespread. Efforts have been made by some organizations to advance the knowledge and training levels of laboratory and field personnel. Unfortunately, many agencies do not know about or take advantage of available programs.

A National Institute of Justice article states, . . .

Criminalists, who examine evidence within the context of an entire case, must have sufficient knowledge and experience to make appropriate recommendations to investigators and attorneys. . . . In order for this evidence (DNA) to stand up in court, however, legal counsel and judges must be confident, and a jury convinced, that evidentiary samples were collected properly and that a qualified person, using sound procedures, performed the tests and analyzed the results accurately. (NIJ, 1995)

Their strategy is to have and sustain certified forensic specialists in laboratories, which will in turn enable detectives and prosecutors to more easily and effectively do their jobs.

Although not ready for use, the American Board of Criminalists (ABC) is preparing an examination that can be used to test the knowledge of students in forensic science programs to determine their strengths and weaknesses (Healy, 2006). Association with the ABC could be fruitful for law enforcement training.

The International Association for Identification (IAI) offers Crime Scene Investigator and Crime Scene Analyst certification programs, which are intended for field personnel as opposed to crime laboratory specialists. The reference material the IAI suggests for use in preparation for these certification tests covers many of the areas listed above that may be deficient (IAI, 2006).

It is understandable that not all agencies can afford to send every officer to every class to learn everything about evidence, photography, and crime scene investigations. Each state should be concerned with what occurs within their borders; they should insist that anyone handling evidence receive ample training. Regardless of agency size or type, each state should make available adequate forensic training funds to help those agencies that cannot help themselves. If the states cannot afford this option, then the federal government might want to sit up and take notice; it is in its best interest, as well, that all agencies have similar levels of knowledge and capabilities and obtain the same evidentiary results through proper collection and testing procedures.

Before the implementation of any statewide forensic training program can commence, additional studies and research are necessary in order to ensure that a high-quality, uniform curriculum is established. As noted, many areas of forensic crime scene field work need to be addressed and the information firmly grounded in the minds and evidence procedures manuals in the possession of Texas law enforcement agencies. The next phase would include the recruitment of instructors.

Qualified individuals are available to teach classes in all aspects of crime scene processing; photography; evidence collection and handling; and fingerprint processing, collection, and identification. The formation of forensic training squads, funded at the state or national level or both, could be beneficial because these squads could set up training sessions, and agencies would be able to send their personnel for free or a minimal fee. With an ample number of qualified training squads in each state, agencies across the United States could be better versed in evidence collection and preservation procedures, as well as photography, crime scene investigations, and safety issues within a few years.

References

- Bellefeuille, J., Bowen, K., Dixon, P., Hanniman, J., Hillier, E., & Lama, D. (2003, November/December). Crime scene DNA collection: Research and practical considerations. *Journal of Forensic Identification*, 53(6), 729-734.
- Daher, R. (2000, November/December). [Review of the book *Techniques of crime scene investigation* (6th ed.), by Barry A. J. Fisher]. *Journal of Forensic Identification*, 50(6), 595-596.
- Federal Bureau of Investigation (FBI). (2004). *The handbook of forensic services*. Retrieved March 7, 2006, from www.fbi.gov/filelink.html?file=/hq/lab/handbook/forensics.pdf
- Grant, J. K. (2002, December). Ethics and law enforcement. *FBI Law Enforcement Bulletin*, 71(12). Retrieved March 11, 2006, from www.fbi.gov/publications/leb/2002/dec2002/dec02leb.htm#ethics
- Healy, M. (2006). *President's message 2006*. American Board of Criminalists. Retrieved February 26, 2007, from www.criminalistics.com/pdf/announcements/ABC%20President%20Message%20704.pdf
- Houston PD harvests new crime-lab trouble as toxicology unit is closed. (2004). *Law Enforcement News*, 24(613). Retrieved March 14, 2006, from www.lib.jjay.cuny.edu/len/2004/01
- International Association for Identification (IAI). (2006). IAI forensic certifications. *Journal of Forensic Identification*. Retrieved March 10, 2006, from www.theiai.org/certifications
- McBride, J. (1995). Capital punishment as the unconstitutional establishment of religion: A Girardian reading of the death penalty. *Journal of Church & State*, 37(2), 263-288.
- National Forensic Academy. (2001). Curriculum. Retrieved March 10, 2006, from www.nfa.tennessee.edu/curriculum.asp
- National Institute of Justice (NIJ). (1995, July). Certification of DNA and other forensic specialists. *National Institute of Justice Update*. Retrieved February 25, 2007, from www.ncjrs.gov/pdffiles/dnacert.pdf
- Rehnquist, W. (1993). *U.S. Supreme Court Decision in Herrera v. Collins*, 506 U.S. 390. Retrieved March 24, 2006, from www.lexis.com/research/retrieve/frames?_m=a108927aa3aca9563adc800b808fd626&csvc=le&cform=&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVtb-zSkAt&_md5=2e762d87e7234b7057430442b6586c61#1100-400
- Saferstein, R. (1998). *Criminalistics – An introduction to forensic science* (6th ed.). Englewood Cliffs, NJ: Prentice Hall.

Shelef, R., & Elkayam, R. (1997, May/June). Collecting and packaging exhibits from the scene of the crime for transfer to the forensic laboratory. *Journal of Forensic Identification*, 47(3), 276-282.

Technical Working Group on Crime Scene Investigation (TWGCSI). (2000, January). *Crime scene investigation: A guide for law enforcement*. Washington, DC: Department of Justice Office of Justice Programs. Retrieved March 7, 2006, from www.ncjrs.gov/txtfiles1/nij/178280.txt

Texas Department of Public Safety (TxDPS). (1997). *Crime scene search core course manual*. Austin, TX: Author.

Vicky J. Blair recently obtained her Master of Science in Criminal Justice from the Graduate School of Criminal Justice at Kaplan University. She graduated Magna Cum Laude, was elected for membership to the Alpha Beta Kappa National Honor Society, and had the honor of authoring the University's first thesis. Prior to attending Kaplan University, she worked as an identification technician (CSI) for the Wichita Falls, Texas, Police Department from 1996 to 2005. From 1992 to 1996, she worked for the Tom Green County District Attorney's Office in San Angelo, Texas, as the Grand Jury Secretary. She is currently a certified TCLEOSE instructor and works as a self-employed crime scene consultant. She is employed by Kaplan University and Ellis College of New York Institute of Technology—both places as an online criminal justice instructor. She also works at Vernon College in Wichita Falls, Texas, as an adjunct criminal justice instructor.

A Quick Look at Interrogation

Adam Kasanof, Lieutenant (Retired), New York Police Department; Principal, The Kasanof Group, Inc.

*What follows in this article is general information about principles of interrogation; however, you need to be thoroughly familiar with the current law governing interrogation in the jurisdiction where you work. This law varies from place to place, and changes constantly. Do **not** assume that the legal discussion here applies exactly in your jurisdiction until you have thoroughly checked it. Nothing in this article constitutes legal advice.*

Soft Interrogation

We're going to look primarily at "soft" interrogation, which is the opposite of the screaming, forceful stuff you always see on television and in the movies. Soft interrogation is often more effective than harder styles. Each case is different, however, and there is no one method that works in every case. Also, soft interrogation requires more acting skill than hard interrogation and doesn't fit everyone's personality effectively. Not everyone can credibly do soft interrogation any more than every actor can play every kind of part on TV or in movies. Investigators need to use techniques that they can manage, they are comfortable with, and fit the specific case they are investigating.

Note: Decide carefully what kind of interrogation style you want to use in a case. If you start with a **soft** interrogation style, you can go to a harder style later if you need to. If you start with a **hard** interrogation style, it will be very difficult to switch to a soft style later and have it work.

Rapport: The Key to Soft Interrogation

To make soft interrogation work, you need to develop a rapport with the suspect. That can sometimes be hard, especially if the suspect is accused of a very serious or disturbing crime, such as the murder or sexual abuse of a child. Polygraph expert Richard O. Arther and Rudolph R. Caputo, in their book, *Interrogation for Investigators* (New York, W. C. Copp and Associates, 1959), suggest that, no matter what the suspect may have done, you try to find something that you and the suspect have in common. Perhaps you went to the same school, were in the same branch of the military service, are of the same religion, or whatever it might be. You need something to help you bridge the gap between you and the suspect because if you can relate to the suspect only as an object of hatred or disgust, he or she will instantly know it and won't want to talk to you.

For Supervisors and Executives: Managing Interrogation

Pick the Right Investigator for the Case

One of your most important jobs as a detective supervisor or investigative supervisor is assigning cases to investigators. It's particularly important that you assign cases involving critical interrogations to investigators who are well suited to those specific cases. The rapport between the interrogator and the suspect is

critical; if an investigator doesn't have the necessary rapport with the suspect, have another investigator handle the interrogation, if possible. It can be hard to take a case away from an investigator who is your friend and a capable investigator, and give that case to someone else, but the effective handling of the case has to take top priority. An investigative unit is very much a team, and everyone needs to work together to solve cases, regardless of ego. You can explain courteously to the investigator who is not selected for the interrogation why you think that it is best for someone else to do the interrogation in this specific case. You can make clear that your decision is not a criticism of the investigator and that there will be other times when he or she will get a case instead of someone else, based on the situation in that case.

Let the Detectives Do the Detecting

Former NYPD Chief of Detectives Richard Nicastro used to say, "Let the detectives do the detecting," and that's very sound advice. As much as you may want to be involved in an investigation, and as much as you may feel you are an excellent investigator, your main job is to manage and supervise investigations, and *not* to do investigations yourself. Though it may seem heresy to say this, it is even possible to be a very good investigative supervisor and *not* be the best investigator in the unit.

In his excellent management book, *Top Performance* (New York, Berkeley, 1987), sales and management author Zig Ziglar notes the difference between a "super-worker" and a "super-visor." A "super-worker" does the job better than their subordinates could do it. A "super-visor" gets their subordinates to do the job better than they could do it themselves. Your goal is to be a supervisor and get your team to do more and better work than any single one of them (including you) could do alone. The three main things you must do are as follows:

1. Get your investigators the resources that they need.
2. Assign cases appropriately, based on the strengths and weaknesses of each investigator.
3. Keep your investigators focused on their investigations, without micro-managing them.

Interrogation from the Investigator's Point of View

Let's look at how to do a soft interrogation in a serious case, but first, let's look at the key principles you have to keep in mind to do an excellent interrogation.

Safety First

- **Be cautious about your firearm whenever you are in an interrogation room with a suspect.** Especially if you have your jacket off, your firearm is exposed to the suspect, and if you do not use a plainclothes security holster, it will be far easier for a suspect to grab your holstered firearm. Investigators and plainclothes personnel should seriously consider using modern plainclothes security holsters, such as the Blackhawk Serpa.
- Do *not* carry a firearm while fingerprinting a suspect.

- Do not let any suspect have access to a locker room, gun locker, detective's desk drawer, evidence locker, or any other place where a firearm could be stored.
- Do not give a suspect anything that could readily be used as a weapon (e.g., boiling hot coffee in a heavy mug, soda in glass bottles, etc.). Be cautious when suspects are using pens or sharp pencils to write or sign statements or other documents.
- Do not leave suspects alone, especially if they are under arrest. Do not assume that you can handcuff suspects to a chair, rail, etc.; leave them alone; and then find them still there when you return. Note also that an unsupervised suspect may be able to get access to an unsecured firearm or another object that could be used as a weapon.

The Goal of an Interrogation: To Get Accurate Evidence You Can Use in Court

Obviously, you don't want to get false confessions from innocent people or inaccurate statements from witnesses, and there is no point in getting statements you cannot use in court. Remember that if you get a statement illegally and that statement leads you to other evidence, a court may well decide that you cannot use the other evidence you found because of the statement. So, a bad interrogation can poison your whole case. To avoid this, remember the following:

Do Not Make Promises and/or Threats.

Remember the detective's favorite words: "I can't promise you anything, but . . ." If you make promises to suspects, or threaten them, that can make their statements inadmissible in court. Even if you *do* manage to get a statement admitted in evidence, how convincing will it be when a jury hears that you falsely promised the suspects that they wouldn't do jail time, or told them that you would arrest their grandmother if they didn't talk?

Do Not Engage in Physical Abuse or Mistreatment.

It goes without saying that you cannot physically abuse suspects, and defense lawyers will often argue that you did so based on claims that their client makes to them. Treat the suspect humanely, and document that you did so. Give the suspect bathroom breaks, and document it. Give the suspect a drink if he or she would like one (e.g., water, decaffeinated coffee, or caffeine-free soda like 7-Up®, ginger ale, etc.). Avoid giving the suspect drinks with caffeine in them. Remember that you may have been up for 30 hours working the case before the interrogation, while the suspect may even have been sleeping. Don't give the suspect anything to keep them alert while you are using toothpicks to keep your eyes propped open. Document that you gave the suspects drinks or snacks.

Know Clearly Whether the Suspect You Are Questioning Needs to Be Given Miranda Warnings.

Whenever you have suspects in custody and want to interrogate them, you will need to give them Miranda warnings if you want to use their statements in

court against them, or if you want to use any evidence you get because of their statements. Generally, someone is “in custody” whenever a reasonable person in their position would *not* feel free to go. So, anyone you have arrested *must* get Miranda warnings before you question them, and anyone who has just confessed to a serious crime would generally need Miranda warnings before you could question them. For example, someone who has just admitted to a police officer that he or she committed a murder would obviously *not* feel free to go.

Since Miranda warnings are required only when someone is in custody, if someone you are questioning in your office, or elsewhere, is present voluntarily, you have not arrested him or her, and he or she has not confessed to anything, tell him or her, “You know that you are free to go,” to make it clear that he or she is *not* in custody.

If you *talk on the phone* to suspects in another location, who is free to leave or hang up, you generally don’t need to give them Miranda warnings, as they usually wouldn’t be considered to be in custody. (Questioning of jail or prison inmates is a more complicated issue, as they will often have the right to counsel, as mentioned below.)

Note: For purposes of Miranda warnings and right to counsel (see below), *interrogation* means more than just questioning designed to gather incriminating evidence on the suspect. An interrogation could be almost anything else that investigators intentionally do, if they reasonably should know that it will tend to get incriminating evidence from the suspect. So, having staged conversations with other investigators that suspect is meant to overhear, or talking to the suspect about how anxious the considered victim’s family is to find the victim’s body for a proper burial, can both be interrogations, even though no one asks the suspect any questions at all.

Know Whether You Can Question the Suspect Without a Lawyer Present.

Even if you give a suspect Miranda warnings, and even if the suspect is not in custody, there may still be cases in which you might not be able to question that suspect without a lawyer present. In these cases, the suspect has the right to counsel and must waive that right before he or she can be interrogated. These cases may include the following:

- When the suspect has a lawyer representing him or her in the case you are asking about or in a related case (or, in some jurisdictions, even an unrelated case)
- When a lawyer representing the suspect notifies you or your agency that the suspect is *not* to be questioned
- When the suspect has already been formally charged in that case or another case (e.g., the suspect has been indicted, or had a complaint, information, or other accusatory instrument filed against him or her, or has been arraigned. This is often the case for jail or prison inmates). Note that in some jurisdictions, charges are formally filed whenever an arrest warrant is issued for a given charge.
- The suspect asks for a lawyer.

Note: In some jurisdictions, once a suspect has the right to counsel in some of these situations, the suspect may not waive that right unless a lawyer is present.

You need to thoroughly know the law about Miranda warnings and right to counsel for suspects in your jurisdiction.

Know Exactly What Your Legal Responsibilities Are if the Suspect Asks for a Lawyer.

If a suspect in custody asks for a lawyer, you should stop questioning that person. The suspect may still make spontaneous statements after asking for a lawyer, and these may still be valid as evidence, but you generally may not question the suspect. Some jurisdictions may allow suspects to ask for a lawyer, then change their mind; you can then question them without a lawyer, but only if they “re-initiate” the *interrogation* and agree to be questioned without a lawyer. *You* cannot make the first move to re-start the interrogation. Other jurisdictions say that once a suspect in custody asks for a lawyer, the suspect may *not* agree to be interrogated until a lawyer is present. You need to know exactly what the applicable law is in your jurisdiction if a suspect, whether in custody or not, asks for a lawyer.

Know Exactly What Your Legal Responsibilities Are if the Suspect Decides That He or She Wants to Remain Silent, or Stop Talking Once an Interrogation Has Begun, but Does Not Ask for a Lawyer.

Once suspects invoke their right to remain silent, you must stop questioning them. In most jurisdictions, however, the suspect invokes the right to remain silent, but does *not* ask for a lawyer, the suspect may change his or her mind and decide to start talking to you again. In some cases, *you* may be able to re-start questioning if enough time has passed since you first gave Miranda warnings (typically several hours), if you have given the suspect Miranda warnings again, and if the suspect knowingly and voluntarily waives his or her Miranda rights. You cannot, however, try to badger or coerce suspects into agreeing to be interrogated once they have invoked their right to remain silent. Again, you need to know the specific legal requirements in your jurisdiction.

Make Sure You Know *Exactly* What You Are Allowed to Say and Do Legally in an Interrogation.

In many jurisdictions, you are allowed to lie to suspects about certain things, but not about others. For example, you might be allowed to say to a suspect, “We found your fingerprints at the scene,” but not be allowed to show the suspect a fake fingerprint and say, “We recovered this fingerprint from the scene, and it matches your right thumb print.” That would be considered fabricating evidence. Before you say or do something in an interrogation, you need to know that it is legal.

Special Cases: Juveniles and Persons with Cognitive/Psychiatric Disabilities

Use Extra Care When Interrogating Juveniles, or Persons with Cognitive/Psychiatric Disabilities (e.g., Mental Retardation, Brain Injury, or Severe Mental Illness).

Defense lawyers often argue that juveniles, and persons with cognitive/psychiatric disabilities, have been coerced or unlawfully tricked into confessing. To help make sure that the statements you get will be admissible, and effective in court . . .

- **Strictly follow the laws in your jurisdiction, and your agency's policies, on the questioning of juveniles.** If you need to notify a juvenile's parents, or question the juvenile only in a specially designated area, do so.
- **Know that you may have to tone down the style of interrogation that you use when questioning a juvenile, or someone with a cognitive/psychiatric disability.** Especially in a videotaped statement or confession, jurors will not be sympathetic to your case if you look as if you have arm-twisted or unfairly conned a juvenile or person with mental retardation into making a statement.
- **Understand that some persons with a cognitive/psychiatric disability may be willing to tell you what they think you want to hear, even if it isn't true.** They may want to please you because they have been taught to be cooperative, or they may think that you are smarter than they are, so, if you say something is true, you are probably right, and they should agree with you. In questioning them, it is probably better to let them tell you what happened than to give them leading questions or press them for specific answers. Don't worry about using this soft interrogation technique; if they're fabricating a story, that will usually be apparent to you without using cross-examination-style questions. Also, avoid putting suspects with mental retardation together with suspects who are not; the latter suspects may try to convince them to take the fall for a crime or say something incriminating so that the other suspect can report this "confession" to you.

Also, make sure that you speak directly to the person with a cognitive/psychiatric disability and not just to whoever may be accompanying them.

- **Understand that some juveniles may be willing to tell you what they think you want to hear, even if it isn't true.** Yes, there are tough street kids who would never lie to incriminate themselves, but there are also juveniles who are more submissive to authority, or just not very bright. So, as when questioning persons with cognitive/psychiatric disabilities, you may need to start your interrogation by letting them tell their story and working from there in a softer style than you would use on most adults.
- **Consider checking whether the juvenile or person with cognitive disability understands the difference between telling the truth and telling a lie.** You can ask something like "If I said that a red light means 'go' is that the truth, or a lie?" Or, you could hold up your hand, point to it, and say, "If I said that this was my

foot, would that be the truth or a lie?" Use a simple example that you think the particular suspect would understand.

Needing to be cautious in questioning juveniles doesn't mean that you can't be effective. Some tips for interrogating juveniles effectively include the following:

- Try to separate juveniles from their friends or parents (to the extent you can do so legally, and in accord with your agency's regulations, since law or regulations may require that some juveniles be questioned only with a parent or other responsible adult present).
- Consider a soft interrogation technique. Kids expect (from watching TV and movies) that an investigator will be hard on them, and their self-esteem and status with their peers may not be very high. So try complimenting them.

Suppose you had a juvenile sex crime suspect, a boy who had raped a girl. You might start talking to him with some idle chit-chat to put him at ease, and make him feel like "one of the boys," then lean in close to him, and ask, "What's her beef? You're a good looking guy." This kid, who is used to being the last guy picked for dodgeball in gym and hearing people say he will never amount to anything is now getting an actual compliment from an adult.

Among other benefits, using a soft style has the important advantage that, on cross-examination in court, it is much nicer to be able to tell a defense lawyer that you complimented his client, than that you yelled at or insulted his client.

By contrast, in a hard interrogation style, the investigator might try to play on the kid's negative feelings about . . .

- The victim, by saying things like, "You can tell me; I know she deserved it," or by saying that the victim disparaged the kid's appearance, etc.
- Women, by saying things like, "I know you hate women."
- The suspect's family, by saying things like, "I know your mother didn't take care of you."

Some investigators prefer this hard style interrogation of juveniles when they feel that the juvenile dislikes them so much and has so little rapport with them, that the juvenile must be provoked by anger into opening up to them.

Know Some of the Common Motivations and Behaviors of Juveniles.

Of course, every individual kid you question is different, but generally speaking . . .

- Kids like to show off.
- Kids are often egotistical.
- Girls may be vain and jealous.
- Boys may be macho and competitive.

Preparation: The Key to Good Interrogations

An Effective Interrogation Starts Long Before You Set Foot in the Interrogation Room.

You need to prepare thoroughly, and that means . . .

- **Reviewing the case materials.**
You need to know the facts you have and the evidence you have (and don't have), especially any evidence (e.g., surveillance camera video, other witness statements, crime scene investigation reports, etc.) that may contradict what you think the suspect will say.
- **Deciding what the goals of the interrogation will be.**
You can't go on a random fishing expedition and expect to get good statements from the suspect.
- **Talking to the people who will be helping you in the interrogation.**
This is critical. Every good interrogation is a play, and the best ones are usually not one-person shows but performances with several actors. You're the director of this play, so make sure that everybody helping you knows exactly what their job is, exactly when they are supposed to come in, exactly what they are supposed to say or do, and exactly when they are supposed to leave.
- **Setting up the interrogation room.**
Even the set up of the room where you will be questioning the suspect is important. This room is the set for your play, and you want it to give you the biggest psychological advantage in questioning the suspect. Here's one layout you can use:
 - **Have an "obvious" chair near the center of the room in which the suspect thinks he or she is supposed to sit.**
When the suspect sits in it, have him or her move. You are establishing that *you* are in charge.
 - **Have the chair you want the suspect to sit in behind a table, near the side of the room.**
You're "pinning" the suspect between the wall and the table in front of him or her. The table and chair need to be set up so that you can move closer to the suspect and touch him or her if necessary.
 - **Have a chair off to the side for another investigator, if needed.**
For example, you may want another investigator to sit in a corner and appear to read the paper but actually be taking notes. You don't want the suspect to be able to read those notes while you're conducting the interrogation.
- **Separating the suspect from others.**
If possible, avoid questioning a suspect with his or her friends, relatives, etc. present. In some cases, this won't be possible; for example, when you question a juvenile, you may be required by law or agency regulations to have the suspect's parent or guardian present. Bear in mind that suspects may be embarrassed

or unwilling to discuss certain things truthfully when their family or friends are present. The “suspect” may even turn out to be a *victim* who would be intimidated by family or friends from telling the truth.

Outline of an Interrogation: The Murder of Jane Green

Let’s see how these principles work by looking at a quick scenario. What follows is just an outline, to illustrate key principles of interrogation. In real life, a major interrogation may take hours and involve several different sessions, sometimes with large gaps of time between them. This example is not meant to be the only way to conduct an interrogation or a one-size-fits-all script for you to follow exactly in every case. You will need to use your skill and judgment to decide the right approach for you in each individual case. Of course, you also need to know the applicable law about interrogations, Miranda warnings, and right to counsel in your jurisdiction.

Background on the Case

Jack Smith’s girlfriend, Jane Green, was murdered; she was stabbed to death. You think Jack did it; you have cell phone records placing him near the scene at the time of the murder and some surveillance camera footage from a store near the scene that clearly shows Jack walking down the street. You have a statement from Phil Jones that Jack did it, but Phil is a dope dealer, and if all you have to go on is his testimony, it might not convince a jury. You need more evidence. Jack has always said that he is innocent, and he has agreed to come in and talk to you voluntarily. Jack is an adult; he is not under arrest; and he has not asked for a lawyer. He is not currently charged with any crime.

Setting Your Goals

Of course you would like a full confession from Jack, but you have decided that you want just two things from this interrogation:

1. Jack’s DNA and fingerprints
2. A statement from Jack putting him at the scene

Note: A statement from a suspect, saying that he or she was at the scene of a crime when it was committed, can often be nearly as good as a confession. In this case, once you have a statement from Jack putting him at the scene of Jane’s murder, you will not have to hear Jack’s new girlfriend say that he was with her watching the ballgame at the time of the murder or any other alibis. You could use other witnesses and evidence to show Jack committed the murder once Jack himself has established that he was there when it happened.

You have talked to your fellow investigators and your boss and set up the interrogation room. Now, it is show time.

Setting the Scene

Jack goes into the room, sits down in the chair near the center, and then you move him to the chair near the wall, behind a table.

Taking Notes

Bill, your fellow investigator, is sitting in the corner, apparently reading a newspaper but actually taking notes. It's best that you not take notes yourself the first time you question a suspect; it distracts you, and the suspect will constantly be trying to get a glimpse at your notes to help him or her keep track of his or her lies.

Engaging the Suspect Emotionally

In the course of questioning Jack, you'll show him a picture of Jane's body (and note his reaction; if he will not look at the picture, that may be an indicator of guilt), and you refer to her by name a lot.

A Zig or a Zag: Breaking the Suspect's Rhythm

Jack is well rehearsed, so you break the rhythm of his phony answer with a seemingly unrelated statement. He has nice shoes on, so after you ask a question, before he answers, say, "You have really good shoes!" That throws off his smooth delivery. Then, ask your question again.

Getting the DNA and Fingerprints

Of course, you give Jack a nice glass of water when he wants one. He picks it up and drinks from it; now you have Jack's prints and DNA. You don't want to tip him off. Exactly as planned, your friend Bill opens the door: "Hey, we need this room! Remember?" You tell Jack, "Sorry, we'll have to use the room next door." You get up, he follows you, and the glass stays on the table, where Bill will pick it up and run it to the lab as soon as you and Jack are in the other room. Of course, you get Jack another glass of water if he wants one.

Note: Be sure to get the DNA and fingerprints *before* you need to give the suspect Miranda warnings to make sure that the DNA and fingerprints are admissible as evidence.

Another way to get DNA is on a cigarette butt. You can let the suspect smoke and simply collect the butts afterward.

Note: Be sure that you know the legal rules for collecting DNA and fingerprints in your jurisdiction.

Catching the Suspect in a Lie

You continue to question Jack, and he denies he was near the murder scene. You know that he was; you have the cell phone information putting him near the scene, the surveillance camera video of him, and the statement from Phil. Before you go further, it is time to give Jack Miranda warnings because you need to make sure that everything Jack says is admissible as evidence; however, you don't want to tip him off so that he stops talking and asks for a lawyer. So it is time for a break.

The Break: Giving Miranda Warnings

You glance at your watch: "Hang on a minute, I've gotta make a call," you tell Jack. "Hey, if we're stopping this, I want to go to the bathroom," your friend Bill, who's been taking notes, says. You go to the door, and yell for someone to come in and watch Jack. You and Bill go out, as your friend Joe comes in. Joe goes straight to the corner, picks up Bill's paper, and starts reading it. Now, instead of the traditional "good cop, bad cop," you are doing "good cop, bored cop." After a while, Jack starts talking to Joe, asking what's going on. Joe tells him, "Listen, I don't really know anything about this case," and then goes back to reading the paper. After a while, Jack may start talking to Joe about the case, but it is important that Joe not *question* Jack about the case since you haven't given Jack Miranda warnings yet.

After a while, you come back in, and Joe leaves. Then, Bill comes back. You sit down, and tell Jack: "Sorry; let's get started again." Before you begin questioning Jack, the door opens; it is your boss, Sergeant Harrison. "Hey! Have you guys given Mr. Smith Miranda yet?" "No, sorry, Boss, we'll do it right now," you say, and your boss leaves. "Sorry," you tell Jack as you hunt for a Miranda warning card; then you give him the Miranda warnings. Now, Jack has received the Miranda warnings, but you have made it seem routine, just another thing you have to do because of "the rules."

Going Over What the Suspect Has Already Said

Once the break is over, you want to go over Jack's story with him again. This gets the interrogation back on track and establishes that Jack repeated his first story *after* getting Miranda warnings.

Confronting the Subject About the Lie

Now, you move close to the suspect. You place your knee between his two knees, you put your hand gently on his elbow. "Listen, I want to help you. We know you were there; we have surveillance video of you, and we have cell phone records showing where you were." You show him pictures from the surveillance camera. Now you move quickly, before Jack can ask for a lawyer. "I know there's a reason why this happened; she attacked you, right? You had to defend yourself; anyone would have done the same." You know that Jack hasn't had time to figure out how to respond to this; the last thing he ever expected was to deal with a self-defense claim. He knows you have evidence that puts him near the scene. He thinks it is better to admit that he was at the scene but say that he didn't murder Jane. He says that yes, he was there, and she attacked him.

Congratulations. Thanks to your careful preparation and the help of several colleagues and your boss, you reached the goals you set before you started the interrogation. You have Jack's fingerprints and DNA, and you have Jack's statement that he was at the scene, and even that he stabbed Jane.

Again, this example is just to illustrate the general principles of good interrogation and is not meant to be an exact model for you to copy, and it cannot be said too many times: you need to know the applicable law about interrogations, Miranda

warnings, right to counsel, and gathering DNA and fingerprint evidence in your jurisdiction.

Acknowledgments

I'd like to thank two former colleagues, and experienced investigators, Lieutenant Gene Whyte of the NYPD's Office of the Deputy Commissioner, Public Information, and retired NYPD Detective First Grade Detective Helena Melisi, President of NYC She Spies, Inc., for their invaluable assistance with this article.

Adam Kasanof retired as a lieutenant from the NYPD, where he performed many functions over his career, including patrol supervisor, police academy law instructor, precinct operations coordinator and integrity control officer, and confidential aide to the chief of department. He is a lawyer and writer who has written articles for *Police, Law & Order*, and other leading police and firearms publications. He is also the author of the book *How to Be an Expert Witness: A Guide for Law Enforcement Trainers*. He is the principal of The Kasanof Group, Inc., in Arlington, Virginia.

Mandatory Recording of Criminal Interrogations: Issues and Policy Considerations

**James N. Gilbert, PhD, Professor, Department of Criminal Justice,
University of Nebraska–Kearney**

As anyone knows who has either researched, worked with, or been employed as a law enforcement practitioner, change comes slowly to the police of America. Law enforcement is a typically conservative governmental entity by nature and experience. While some changes come from within, and pragmatically focus on improving organizational effectiveness, other changes are externally introduced to policing in order to ensure a greater sense of justice. When law enforcement perceives that an organizational, technological, or scientific advance may directly improve the ability to identify and/or arrest suspects, the change is often readily accepted and quickly adopted. The rapid acceptance and usage of DNA, wearing of ballistic vests, and the conversion of nearly all departments from the revolver to semi-automatic handgun are examples of recent changes motivated by internal perception of increased effectiveness.

Yet other forms of major change are often externally introduced to the law enforcement community and are just as often viewed with great caution and suspicion. Generally conceived by those outside of police work, this form of change is commonly instituted to ensure a greater standard of justice and fairness. Law enforcement rarely agrees with this perception, however, and is slow to embrace the motivations so obvious to the external change agents. Such concepts may be viewed (at least initially) by law enforcement personnel as being counterproductive to agency efficiency. The Miranda Warning, community policing, dash mounted cameras within patrol vehicles, and civilian review boards were all resisted for years until their effectiveness or usefulness were demonstrated.

Relatively recently, the concept of mandatory videotaping of police interrogations has become a significant issue across the nation. Like most meaningful justice issues, it has evolved over time and had many supporters and detractors prior to actual policy implementation. Initially viewed by many police officers as a change concept to be resisted due to the potential to inhibit police questioning techniques, it is now widely viewed by many departments as a highly effective interrogation protocol.

The Videotaping/Interrogation Movement

Videotaping is a visual and aural method of recording suspect interrogations but can also extend to victim and witness statements and interviews. Its greatest value and potential for controversy is centered upon criminal suspects. As the technology and affordability of video cameras became a practical reality for consumer markets in the late 1970s, the devices were mainly used to record family recreational activities and provide surveillance in retail stores and banks. Audiovisual technology began

to find a place in law enforcement in the mid-1980s. Initially used for training purposes and recording major crime scenes and civil riots, the technique was not immediately adopted into the interrogation room (Gilbert, 2007).

In March 1993, the National Institute of Justice (NIJ) published the results of a groundbreaking study detailing the use of video technology within criminal interrogations. The report disseminated considerable national data regarding the use of the technique and carefully defined the issues inherent in videotaping interrogations. The study concluded that in 1990, nearly one-third of all American police agencies serving populations of 50,000 or more were videotaping (to some degree) interrogation sessions of a custodial nature (Geller, 1993). Following the widely read NIJ study, various individual police agencies began to draft internal policies that required detectives to record selected types of interrogations. In some cases, only homicide interviews were required to undergo recording; in others, the mandatory recording extended to all felony custodial interrogations. In time, two other models of mandatory police videotaping emerged, and both were externally foisted upon the police. The first method involved state legislation action, and the second resulted from legal decisions by respective state Supreme Courts. Compulsory suspect videotaping has been enacted by legislative action in the District of Columbia, Illinois, Maine, and New Mexico. Many authorities are convinced that legislative legal enactments are the superior method to implement interrogation videotaping. As detailed by Sullivan (2005), . . .

Legislation is the best method because it is inherently more comprehensive. Statutes are more likely to spell out in detail when and where recordings shall be required, the exceptions to the requirement, the consequences of failing to record, how the equipment will be funded and where it will be stored, how officers will be trained, and, where necessary, when recordings may be exempt from applicable eavesdrop/wiretap laws. (p. 113)

When police agencies and state legislatures fail to act, some states have chosen to enact mandatory suspect videotaping via judicial action. Typically, this occurs when defense initiated challenges reach a state Supreme Court ready and willing to set policy through legal precedent. Such cases are generally based on an issue that could have been resolved had the authorities recorded a critical interrogation rather than leaving it to notes and memory. Alaska, Minnesota, New Jersey, Massachusetts, and New Hampshire have mandated various forms of statewide judicially required suspect videotaping by this method.

Supportive Issues for Mandatory Taping

Those who support the mandatory videotaping of criminal interrogations are not unanimous as to the specifics of policy. Some favor recording only the most serious of felony interviews (e.g., exclusively involving homicide cases). Others support the taping of all (and only) felonies; some believe the issue is best settled by practicing it whenever there is a custodial interrogation. Regardless, the supporters of mandatory videotaping agree that fundamental advantages will be inherently achieved through its utilization. Taping protects the police against baseless claims of illegal coercion or other forms of constitutionally prohibited abuse. Once it becomes widely known that one's interview has been permanently preserved through filming, suspects will be deterred from making false claims of

abuse and lack of voluntariness. The deterrent effect also applies to police behavior. In a similar manner to suspects becoming aware that every word and gesture is recorded, the interrogator's behavior is likewise preserved for future evaluation by supervisors, judges, and juries. Accordingly, taping promotes and goes far to ensure legal and ethical police questioning tactics. It has the potential to eliminate the temptation of an "end justifies the means" attitude by police, who, when asked during a trial to detail questionable techniques may conveniently forget their implementation during non-taped sessions.

Other positive outcomes of taping center upon the problems of memory and traditional recording of interrogations through note-taking. Interrogators have relied exclusively upon their memories and notes to recount details of the interrogation at later dates. Some detectives would take extensive notes, and other's efforts varied from some to none at all. This varying subjective practice is effectively eliminated through mandatory videotaping. In the past decade, a substantial number of "false confession" cases have advanced through the justice system, causing greater concern among the general public and tighter judicial surveillance by appealed courts. Such cases involve a suspect confession that is later recanted due to claims of unethical or coercive interrogation tactics by the police. Such cases typically allege that police pressured an otherwise innocent subject into admitting false guilt. False confessions are often based on claims of intense psychological tactics by interrogators, which are difficult to describe by the defendant and equally difficult to comprehend by juries. While the true extent of such cases is contested, their reality is beyond dispute (Davis & Leo, 2006). Interrogation videotaping certainly helps a judge or jury determine whether questioning tactics were employed that could have convinced an innocent individual to become convinced of his or her guilt.

Possibly the most convincing positive factor supporting the taping of interrogations is the duality of support by both defense and prosecution counsel. Endorsed by both the National Association of Criminal Defense Lawyers in 2002 and the National District Attorney Association in 2004, this rather rare stipulation by opposing judicial forces gives powerful support to the taping concept (National Association of Criminal Defense Lawyers, 2002; Sullivan, 2005). Additionally, the American Bar Association summarized the support of the legal community by passing a resolution supporting mandatory taping, stating, . . .

The American Bar Association urges all law enforcement agencies to videotape the entirety of custodial interrogations of crime suspects at police precincts, courthouses, detention centers, or other places where suspects are held for questioning . . . further (they resolve) urging legislatures and/or courts to enact laws or rules of procedure requiring videotaping of the entirety of custodial interrogations . . . (Saulny, 2004).

Opposing Issues for Mandatory Taping

As police gradually became aware of the importance and external interest regarding mandatory suspect videotaping nearly 20 years ago, their initial reaction was one of caution. Experienced detectives worried their interrogation goal of obtaining a confession would be compromised by altered police or suspect behavior due to the effect of the taping procedure. There is little empirical evidence to support this

belief, as the rates of confession appear unaltered whether taping is utilized or absent. Additionally, the same percentage of suspects elected to be interviewed (approximately 70%) by the police as before the public's general knowledge of the existence of interview taping (Bratton, 2000). Some are concerned that suspects who would otherwise talk during an interrogation, will refuse if they are aware the session is being taped. This concern is, of course, similar to objections to the institution of the Miranda warning and is not supported by fact. In Illinois, the Kankakee Police Department reported nearly 60% of all suspects agree to be videotaped, and the county sheriff's office indicated a 95% suspect agreement rate (Mills & Higgins, 2002). Accordingly, while some officers and agency heads still oppose mandatory taping totally or prefer individual discretionary judgment when it should be employed, widespread police resistance has dramatically dissipated. Indeed, it is quite common for law enforcement agencies to draft mandatory taping policies in states lacking either legislative or judicially imposed taping laws (Lights, camera, interrogation, 2004).

With gathering police support has come considerable academic research interest. Various studies have not only indicted the effectiveness of this tactic in protecting police from false allegations but have demonstrated important tactical knowledge. For example, research has recently documented that videotaped confessions with the camera focused directly on the suspect more often convinces jurors to conclude a suspect's guilt than when wider camera angles are employed. The research suggests that camera perspective must be taken into account during suspect taping, or unintended prejudice may be produced upon later viewings (Lassiter, 2002).

Curiously, federal investigative agencies have not embraced mandatory taping of interrogations, nor has Congress or federal courts actively created policy to replace individual discretion. Historically, the federal level has led the way through legal mandate in achieving greater questioning fairness and efficiency. The evolution of the Miranda Warning, among many other now standard behaviors inherent to interrogation, began on the federal level and was then judicially imposed upon local and state agencies. Federal investigators, however, continue to employ individual discretion in the matter of mandatory videotaping of suspect interrogations.

Many of the remaining objections to mandatory taping tend to revolve around financial, technical, and jury comprehension. The actual financial expenditures to institute a mandatory taping program are actually quite low when compared to other police equipment. When the costs are compared to the often enormous settlements resulting from false confession and false brutality lawsuits, which could have been resolved favorably with a tape of the interrogation, the start-up costs are small indeed. The technical knowledge needed to install and operate interrogation taping systems is not extensive and is often assigned to a lead detective who has attended an inservice training seminar prior to the inauguration of the program.

A valid concern among some opponents of mandatory taping focuses upon whether the average jury member can comprehend the standard interrogation tactics used by police and not incorrectly conclude they are coercive or blatantly unjust. Most Americans are indeed not aware that it is legal, and often quite common and effective, for interrogators to fabricate facts and evidence during an interrogation.

There is no constitutional protection that invalidates police claims that they possess evidence that they do not or prevents them from claiming other falsehoods indicating the suspect's guilt. Some investigators fear that when juries actually witness such tactics, they will never convict a defendant, believing the police used illegal tactics to obtain a confession or admission of guilt. This concern, however, underestimates the sophistication of today's jury and their ability to comprehend these perfectly legal techniques and their necessary widespread usage. It is up to the prosecutor to make juries aware that such tactics are legal, and courts have established national precedent that holds innocent people will not confess to a crime if they did not commit the crime, regardless of the degree of fabricated evidence seeking to convince them otherwise. In addition, judges typically reaffirm the legality of these interrogation techniques as they instruct juries prior to deliberation.

Conclusion

Police interrogation of criminal suspects has always been a subject of intense public curiosity and judicial surveillance. It is right that it should be so, given its often dubious history and potential for abuse. Progressing from the early third degree stereotype to the breakthrough of *Miranda*, the interrogation sits at the core of the investigative process. Successful interrogations produce a confession, and while this complete admission of criminal wrongdoing is less significant than in the recent past, it is still a very powerful indicator of guilt. How confessions are obtained is the essential test of not only the interrogator's skill but of the enormous power relegated to the police. Interrogation tactics test the ability of law enforcement to be fair and avoid the temptation of obtaining confessions through an "end justifies the means" rationale. Any new tactic or instrumentation that furthers effective investigative goals without sacrificing the ability of the police to fulfill their mission deserves to be utilized.

As mandatory interrogation videotaping appears to be one of those rare issues in which police, prosecution, and defense counsel all generally agree upon, it is likely it will become a standard law enforcement technique in the near future. Support for mandatory videotaping is at present generated primarily from within government. Selected police agencies, the courts, and legislatures all have contributed to its development and implementation, but only when the general public recognizes its benefit and obvious unbiased value in determining truth, will its usage become as standard and expected as the provision of the *Miranda* warning.

Bibliography

- Bratton, W. (2000, October). A law enforcement view of confessions. *Court TV.com*. Available online at www.courtstv.com/archive/movie/crowe/law.html
- Davis, D., & Leo, R. (2006). Strategies for preventing false confessions and their consequences. In M. Kebbell & G. Davies (Eds.), *Practical psychology for forensic investigations and prosecutions* (pp. 121-149). San Francisco: John Wiley.
- Geller, W. A. (1993). *Police videotaping of suspect interrogations and confessions*. Washington, DC: National Institute of Justice.

- Gilbert, J. (2007). *Criminal investigation* (7th ed.). Upper Saddle River, NJ: Prentice Hall.
- Kuboviak, J. (2004). Legal admissibility of digital video recordings. *Law and Order*, 55, 92-95.
- Lassiter, G. (2000). Illusory causation in the courtroom. *Current Directions in Psychological Science*, 6, 204-208.
- Lights, camera, interrogation. (2003, January). *Law Enforcement News*, 30, 11-12.
- Mills, S., & Higgins, M. (2002, January 6). Cops urged to tape their interrogations. *Chicago Tribune*. Available online at www.chicagotribune.com/news/nationworld/Chi-0201060325jan06,1,4743821
- National Association of Criminal Defense Lawyers. (2002, May 4). Available online at www.nacdl.org/public.nsf/26cf10555dafce2b85256d97005c8fdo/7cac8b1
- No more excuses. Go to the tapes. (2002, April 21). *Chicago Tribune*. Available online at www.chicagotribune.com/news/nationworld/chi-020421dpeditorial,1,7349540.story?ctrack=3&cset=true
- Peters, J. (2006, April 11). Detroit police videotaping interrogations. *New York Times*. Available online at www.nacdl.org/sl-docs.nsf/freeform/mandatory:015
- Saulny, S. (2004, February 10). National law group endorses videotaping of interrogations. *New York Times*. Available online at www.nacdl.org/_85256BE4005CBECB.nsf/0/FB09AFED3033075D85256E360070A866?Open
- Sullivan, J. P. (2005a). Electronic recording of custodial interrogations: Everybody wins. *Journal of Criminal Law and Criminology*, 95, 1127-1140.
- Sullivan, J. P. (2005b). Recording custodial interrogations. *Law and Order*, 53, 46-50.

James N. Gilbert, PhD, is professor and former chair of the Department of Criminal Justice at the University of Nebraska at Kearney. He is the author of *Criminal Investigation* (7th ed., Prentice Hall) and *Criminal Investigation: Essays and Cases* (Charles E. Merrill). He has authored numerous articles and papers concerning the criminal investigative process and is a former Berkeley, California, police officer and Florida Department of Law Enforcement special agent.

Legal, Scientific, and Forensic Controversies Over Spectrographic Voice Analysis for Identification or Elimination¹

Herbert Joe, MA, JD, LLM, BCFE, Partner, Yonovitz & Joe, LLP
Al Yonovitz, PhD, CCC-A, Partner, Yonovitz & Joe, LLP

Since 1923², the standard for admissibility of scientific evidence in federal courts was governed by the “Frye Test,” in which evidence was admitted if it was based on principles “generally accepted” within that scientific community. This basically meant that the relevant scientific community would in effect decide whether a particular scientific methodology would be admitted or not. One significant shortcoming of the Frye Test was its failure to distinguish new or novel scientific or technological procedure. That was the law of the land (at least for federal courts) for 70 years until the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals*³ ruled otherwise in 1993.

The U.S. Supreme Court overruled the Frye test in the *Daubert* case, which is the foundational case for the admissibility of scientific evidence and arguably affects tort reform more than any other single case. The *Daubert* case made the trial judge the “gatekeeper” in admitting the good sciences and barring the junk sciences. The *Daubert* test, now the rule of law for all federal courts, is a nonexclusive list of factors used by the federal courts to determine the reliability of the expert testimony or scientific principles utilized thereof. If an expert relies on unreliable data or methodology, then his or her entire expert opinion is likewise unreliable and should be excluded from the jury.

Some laws have come down since *Daubert* to clarify its rulings: In *General Electric v. Joiner*,⁴ the U.S. Supreme Court held that a trial court’s decision to admit or deny expert testimony is reviewed under an abuse of discretion standard at the appellate level. In *Kuhmo Tire v. Carmichael*,⁵ the U.S. Supreme Court held that *Daubert* applied to all forms of expert testimony, not just scientific testimony, and in 2000, Federal Rule 702⁶ was amended to include the logic of *Daubert* and *Kuhmo Tire*.

Currently, admissibility of expert testimony in federal courts is necessarily governed by *Daubert*; however, state courts are not bound by *Daubert*. A significant minority of states (11) have state statutes that specifically adopt *Daubert*⁷ in determining the admissibility of expert testimony in state courts. Thirteen states—including Illinois—are still applying the *Frye* test,⁸ and 11 states, along with the military courts, apply a variation of the *Frye* test.⁹ The remaining states have a history of rejecting both *Frye* and *Daubert*.

Spectrographic voice analysis was developed at Bell Labs in 1941 and introduced forensically in 1961; however, forensic phonetics, which actually predates spectrographic voice analysis, was the topic of a widely published study on

comparing voices.¹⁰ At any rate, the basic premise of spectrographic voice analysis is that each of us has unique vocal characteristics; sinus cavities, vocal chords, and articulators (i.e., lips, teeth, tongue, etc.) confer vocal characteristics, which are individually unique when spectrograms are made. Unfortunately, there is a (mis)perception by the general public that voice ID (VID) is straightforward. This misperception was reinforced by the introduction of the term *voiceprint* or the phrase *voiceprint identification*,¹¹ Hollywood dramas like *CSI*, and the like.

VID or voice spectrographic analysis has been controversial since its forensic outset. This is partially manifested by roughly as many jurisdictions that allowed expert testimony on VID as those that did not before *Daubert*.¹² Since *Daubert*, no federal appellate court has approved the admission of voice spectrographic expert testimony into evidence. The Fifth Circuit federal Court of Appeals has stated that the state of the law concerning expert voice identification is “ambiguous” in the wake of *Daubert*.¹³ One state Supreme Court, however, has allowed expert testimony on VID since *Daubert*, namely, *State v. Coon*, 974 P.2d 386 (AK, 1999) (admission of testimony based on voice spectrographic analysis was not an abuse of discretion).

The Alaska Supreme Court did note that the scientific literature “permit[ted] a conclusion that there is significant disagreement among experts in the field of voice spectrographic analysis regarding the reliability of the technique.”

The same expert who testified in the *Coon* case is the same expert in the *Angleton* case.¹⁴ In *Angleton*, the federal District Court held that the proposed expert testimony on aural spectrographic voice identification method failed to meet the *Daubert* standard for reliability, and the protocol followed by the expert did not protect against several sources of error, further reducing the reliability of the expert’s testimony. Stephen Cain, the expert in the *Angleton* case, testified that he followed the protocol of the American Board of Recorded Evidence (ABRE) in his analysis.

Mr. Cain and Dr. Nakasone testified that the ABRE was formed after a dispute arose among the members of the voice identification board of the International Association of Identification (IAI)¹⁵ over the standards for aural spectrographic analysis. In *Angleton*, Dr. Nakasone testified that the group that left the IAI to form the ABRE felt the IAI’s standards for voice identification were too stringent because they required examiners to obtain a second opinion and to include a statement of accuracy in their reports. Furthermore, . . .

The record before this court shows that the remaining proponents of the use of aural spectrographic voice identification for courtroom testimony are a handful of consultants who apply the techniques for the purpose of litigation. The proponents, including Cain, are not performing scientific research in aural spectrographic voice identification and testifying as experts as an aspect of their research work.¹⁶

In addition, Mr. Cain acknowledged that it is not uncommon for VID analysts reviewing the same recordings to have differing opinions as to the identity of the speakers on the recordings.¹⁷

The state of *forensic flux* of expert testimony on voice *spectrographic* analysis is also significantly manifested by the changing views of Dr. Hirotaka Nakasone.

Dr. Nakasone has been working in the field of speech recognition since 1977. While working on his doctorate in speech sciences from Michigan State in 1984, Dr. Nakasone conducted voice spectrographic research for the Los Angeles County Sheriff's Department and on several occasions testified as a proponent of the VID method in courts and administrative tribunals. Since 1992, Nakasone has worked for the Federal Bureau of Investigation (FBI), conducting research in audio forensic identification. His current research is in developing computer-assisted voice identification systems. As late as 1989, Dr. Nakasone testified in *U.S. v. Smith*, 869 F.2d 348, 353-54 (7th Cir. 1989) that the voice spectrographic technique was reliable and had a low error rate.

Recently, Dr. Nakasone has testified that his initial belief that the VID technique is sufficiently reliable for courtroom purposes has eroded over time, as a lack of research efforts have failed to support the underlying premises of the voice identification techniques or to produce reliable testing for error rates. Dr. Nakasone has testified credibly that this failure is the basis of the FBI's approach to voice spectrographic analysis. (The FBI does not permit the use of voice spectrographic analysis for courtroom identification but only for investigation.)

The bottom line, however, is that when the courts ask the wrong questions, they will only get the wrong answers. Likewise, when "experts" primarily or exclusively use a flawed technique, then false positive or false negative answers will occur. As emphasized above, there is a justifiable state of *forensic* flux of expert testimony on voice spectrographic analysis.¹⁸

VID analysis relies extensively on merely matching patterns between spectrograms. Thus, VID analysis (alone) is unreliable because several significant vocal characteristics are not available on spectrograms, and almost every putative expert on VID is not formally (academically or clinically) trained in the speech and hearing sciences¹⁹—a prerequisite to recognizing and distinguishing the vocal characteristics that are not available on spectrograms but are available through other instrumental means including expert aural perceptual analysis.

Specifically, the Aural-Acoustical methodology for Voice/Speaker Identification or Elimination incorporates a single dimensional scaling of the conclusion along a continuum. (Although the Aural-Acoustical method does not rely on spectrographic analysis as its principal basis, it can be supplemented by spectrographic analysis.) This continuum holds as its basis that at one end of the scale, a very high probability (or positive) "identification (match)" exists, and at the other end of the scale, a very high probability (or positive) "elimination (non-match)" exists.

Assuming samples of the recorded evidence and the exemplar recording contains sufficient and intelligible speech materials, the Aural-Acoustical method of speaker identification or elimination has as its basis both acoustical (objective) and aural (subjective) procedures. It is therefore possible that error exists; however, the probability of error decreases with the competency of the forensic scientist. The methodologies have been long established in the speech, hearing, and language sciences and represent ordered analyses of obtained data.

The speaker identification or elimination procedure employed is one in which an unknown voice is taken from an evidence tape and compared to exemplars of a

known voice. In this manner, samples of a number of comparisons between the unknown and known combinations are placed in pairs or composites for direct and repeated comparisons. The Aural-Acoustic method of analysis follows the protocol and standards described in publications as well as a number of presentations to professional organizations, including the Acoustical Society of America and the American Speech, Hearing and Language Association. The principles of this protocol are to provide a basis for voice/speaker identification or elimination that is consistent with the known principles and evidence-based practice of the hearing, speech, and language sciences.

The Aural-Acoustic method has evolved from earlier standards developed by the IAI²⁰ (and the ABRE whose standards practically mirror those of the IAI). For example, section VII.B.5 of the 1996 “Voice Comparison Standards” of the Voice Identification and Acoustic Analysis Subcommittee (VIAAS) of the IAI and section 7.2.5 of the “Voice Comparison Standards” of the ABRE are entitled “Speech Characteristics.” Speech and hearing scientists and phoneticians are particularly skilled in forensically assessing speech characteristics.²¹ Examiners trained in spectrogram pattern matching receive little or no training in the assessment of speech characteristics.

Section VII.B.5.i (“Vocal Quality”) of the 1996 “Voice Comparison Standards” of the Voice Identification and Acoustic Analysis Subcommittee (VIAAS) of the IAI states . . .

Vocal quality is the perception of the complex, dynamic interplay of laryngeal voicing (pitch, intonation, and stress), articulator movement, and oral cavity resonances. *Since each individual’s voice is relatively unique in vocal quality, comparisons can provide important information regarding similarities and differences between the voice samples.* (emphasis added, quoted verbatim by the ABRE in its “Voice Comparison Standards,” Section 7.2.5.i. “Vocal Quality”²²)

This Aural-Acoustical method uses a number of instrumental or digital signal processing procedures that delineate the microstructure of various vocal qualities or characteristics, such as those described in the acoustic process below. It utilizes, with due caution, the use of these measures, not to overextend the conclusions that may be offered. Two publications discussing the Aural-Perceptual methods at length are Hollien’s *Acoustics of Crime* (Plenum, 1990) and Hollien and Hollien’s *Forensic Voice Identification* (Academic Press, 2001). The very significant vocal qualities or characteristics present in speech but not in simple spectrograms include the following:

- Complex co-articulation patterns of vowels and consonants
- Voice quality²³ (e.g., measurements of resonance, vocal fry, and/or nasality)
- Linguistic and paralinguistic features (e.g., prosody, rate, and/or melodic patterns)
- Speech abnormalities (e.g., misarticulation and/or fluency)
- Dialect
- Fundamental frequency²⁴—absolute and variable
- Jitter²⁵
- Shimmer²⁶

In summary, there has been and will always be a great need for various applications of speech processing, speech sciences, and speech technology. Voice or speaker identification or elimination is one of those applications. The forensic comparison of voices or speakers for identification or elimination purposes—by any means—is not infallible. VID, especially by those untrained academically and clinically in the speech and hearing sciences, phonetics, linguistics, etc. is not a reliable means to identify or eliminate voices or speakers.²⁷ There are several significant vocal characteristics that may assist in identifying or eliminating voices or speakers that are not available on spectrograms. The Aural-Acoustic method, with or without supplementing with spectrograms, provides a basis for voice/speaker identification or elimination that is consistent with known principles of the speech, hearing, and language sciences. Under the proper conditions via an academically, clinically, and forensically competent scientist, voice/speaker identification or elimination may be reliably made and academically and forensically tenable between two vocal samples.

Endnotes

¹ Copyright is not claimed as to any part of the original work prepared by any government entity. The information you obtain in this article is not, nor is it intended to be, legal advice. You should consult an attorney for individual advice regarding your own situation. Except as stated below, none of the material or derivative works thereof may be reproduced, distributed, republished, downloaded, displayed, posted, transmitted, or copied in any form or by any means, without the prior written permission of the copyright owner. Permission is granted to display, copy, distribute, and download the materials in this article solely for personal, noncommercial use, provided that you make no modifications to the materials and that all copyright and other proprietary notices contained in the materials are fully retained. Any unauthorized use of any material contained in this article may violate domestic and/or international copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.

² *Frye v. U.S.*, 293 F. 1013 (1923).

³ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 113 S.Ct. 2786 (1993).

⁴ *General Electric Company v. Joiner*, 522 U.S. 136 (1997).

⁵ *Kuhmo Tire v. Carmichael*, 119 S.Ct. 1167 (1999).

⁶ Federal Rules of Evidence Rule 702 (2000) now states that if scientific, technical, or other specialized knowledge will assist the trier of fact in understanding the evidence or help determine a fact issue, then the witness, by virtue of his or her knowledge, skill, training, education, or experience can testify, in the form of an opinion or otherwise, if (i) the testimony is based on sufficient facts or data, (ii) the witness uses scientific methods that are reliable, and (iii) the witness properly applied those reliable scientific methods to the facts of the case.

⁷ Connecticut, Indiana, Kentucky, Louisiana, Massachusetts, Missouri, New Mexico, Oklahoma, South Dakota, Texas, and West Virginia

- ⁸ Alaska, Arizona, California, Colorado, Florida, Illinois, Kansas, Maryland, Michigan, Nebraska, New York, Pennsylvania, and Washington
- ⁹ Arkansas, Delaware, Georgia, Iowa, Minnesota, Montana, North Carolina, Oregon, Utah, Vermont, and Wyoming
- ¹⁰ McGehee, F. (1937). The reliability of the identification of the human voice. *Journal of General Psychology*, 17, 249-271.
- ¹¹ Kersta wrote a 1962 article published in *Nature* using those words. See Kersta, L. G. (1962). Voiceprint identification. *Nature*, 196, 1253-1257.
- ¹² See generally *United States v. Leon*, 966 F.2d 1455 (6th Cir. 1992) (admissible); *United States v. Smith*, 869 F.2d 348 (7th Cir. 1989) (admissible); *United States v. Williams*, 583 F.2d 1194 (2d Cir. 1978) (admissible); *United States v. McDaniel*, 538 F.2d 408 (D.C. Cir. 1976) (inadmissible); *United States v. Jenkins*, 525 F.2d 819 (6th Cir. 1975) (admissible); *United States v. Baller*, 519 F.2d 463 (4th Cir. 1975) (admissible); *United States v. Franks*, 511 F.2d 25 (6th Cir. 1975) (admissible); *United States v. Addison*, 498 F.2d 741 (D.C. Cir. 1974) (inadmissible); *United States v. Maivia*, 728 F. Supp. 1471 (D. HI. 1990) (admissible); *United States v. Williams*, 443 F. Supp. 269 (S.D.N.Y. 1977) (admissible); *United States v. Sample*, 378 F. Supp. 44 (E.D.P.A. 1974) (admissible); *United States v. Raymond*, 337 F. Supp. 641 (D.D.C. 1972) (admissible); *United States v. Wright*, 37 C.M.R. 447 (1967) (admissible); *State v. Gortarez*, 686 P.2d 1224 (AZ 1984) (inadmissible); *People v. Kelly*, 549 P.2d 1240 (CA 1976) (inadmissible); *People v. Law*, 114 Cal. Rptr. 708 (Cal. 1974) (inadmissible); *Hodo v. Superior Court*, 106 Cal. Rptr. 547 (Cal. 1973) (admissible); *People v. King*, 72 Cal. Rptr. 478 (Cal. 1968) (inadmissible); *People v. Drake*, 748 P.2d 1237 (CO 1988) (inadmissible); *Brown v. United States*, 384 A.2d 647 (D.C. 1978) (neither); *Alea v. State*, 265 So. 2d 96 (Fla. App. 1972) (admissible); *Worley v. State*, 263 So. 2d 613 (Fla. App. 1971) (admissible); *Cornett v. State*, 450 N.E.2d 498 (IN 1983) (inadmissible); *State v. Free*, 493 So. 2d 781 (LA 1986) (inadmissible); *State v. Williams*, 388 A.2d 500 (ME 1978) (admissible); *Reed v. State*, 391 A.2d 364 (MD 1978) (inadmissible); *Commonwealth v. Lykus*, 327 N.E.2d 671 (MA 1975) (admissible); *People v. Tobey*, 257 N.W.2d 537 (MI 1977) (inadmissible); *State ex rel. Trimble v. Hedman*, 192 N.W.2d 432 (MN 1971) (inadmissible); *Windmere, Inc. v. International Insurance Company*, 522 A.2d 405 (NJ 1987) (inadmissible); *D'Arc v. D'Arc*, 385 A.2d 278 (N.J. Super. Ct. 1978) (inadmissible); *State v. Cary*, 239 A.2d 680 (N.J. Super. Ct. 1970) (inadmissible); *People v. Bein*, 453 N.Y.S.2d 343 (N.Y. Sup. Ct. 1982) (admissible); *People v. Collins*, 405 N.Y.S.2d 365 (N.Y. Sup. Ct. 1978) (inadmissible); *People v. Rogers*, 385 N.Y.S.2d 228 (N.Y. Sup. Ct. 1976) (admissible); *State v. Williams*, 446 N.E.2d 444 (OH 1983) (admissible); *State v. Olderman*, 336 N.E.2d 442 (OH 1975) (admissible); *Commonwealth v. Topa*, 369 A.2d 1277 (PA 1977) (inadmissible); *State v. Wheeler*, 496 A.2d 1382 (RI 1985) (admissible)
- ¹³ See *U.S. v. Drones*, 218 F.3d 496, 503 (5th Cir.2000). Like the *Coon* court, the *Drones* court noted the “uncertainty of the current state of the law regarding the reliability and admissibility of expert voice identification evidence” (218 F.3d at 504).
- ¹⁴ *U.S. vs. Angleton*, 269 F.Supp.2d 892 (S.D.TX 2003).
- ¹⁵ One of the authors, Dr. Yonovitz, is a former member of the certification and standards committee of the International Association of Identification (IAI).

¹⁶ *Id.* at 902.

¹⁷ *Id.* at 904, citing Docket Entry No. 160, p. 158, 1.10-1.14.

¹⁸ One of the authors, Al Yonovitz, is an associate professor of the speech and hearing sciences with a doctorate in acoustics and having been involved in the academic, scientific, clinical, research, and forensic aspects of vocal production for over 30 years, opines that voice/speech/speaker identification via the Aural-Acoustic method, with or without secondary analyses via spectrography, is an accepted academic method for VID.

¹⁹ The authors recognize Dr. H. Nakasone, Dr. Harry Hollein, and Dr. Tito Poza as peer experts in the forensic area of the speech sciences. There may be other U.S. expert or forensic examiners qualified to perform proper VID via the Aural-Acoustic method.

²⁰ The IAI ceased certifying voice identification examiners in 1999 and ceased all voice identification activity in December 2002.

²¹ One of the authors, Dr. Al Yonovitz, has written numerous publications, given international presentations, produced abstracts, and taught undergraduate and graduate courses related to speech and hearing.

²² Approved by the ABRE Voice ID Board in April 1999.

²³ Voice quality encompasses the perception of the listener of the overall sound of the talker's voice. Just as different musical instruments produce different wave compositions, the human voice is similar. It is this overtone structure or timbre that can differentiate one voice from another.

²⁴ The perceived pitch is the psychophysical correlate of fundamental frequency.

²⁵ Jitter is a frequency perturbation of the glottal source signal.

²⁶ Shimmer is amplitude perturbation of the glottal source signal.

²⁷ Spectrograms may be very useful to engineers and as a voice analysis (e.g., speech pathology) tool.

Herbert Joe is an attorney who has four degrees, including two science degrees and two law degrees. The following are a result of his expertise in the area of forensic audio/video: Board Certified Forensic Audio/Video Examiner; Diplomat, American Board of Forensic Examiners; Diplomat, American Board of Law Enforcement Experts; Licensed Instructor, Texas Board of Private Investigators; Board of Legal Advisors, American Guild of Court Videographers; Fellow, American Guild of Court Videographers; and Fellow, American College of Forensic Examiners. His 21-year involvement in the area of forensic audio/video includes regional, national, and international presentations. He has also authored publications and been interviewed by ABC, BBC, and FOX television. Joe is a partner in Yonovitz & Joe, LLP, a team of forensic audio/video analysts, experts, and consultants.

Al Yonovitz, PhD, has a doctorate in physiological and psychological acoustics and 30+ years of teaching and research, including appointments at the Speech and Hearing Institute; Graduate School of Biomedical Sciences; the School of Public Health at the University of Texas Health Science Center, Houston; the Baylor College of Medicine; the Department of Biomedical Engineering at the University of Houston; and the Conley Speech and Hearing Center, University of Maine. He has been a consultant to the VA Hospital, Houston, on voice research in psychiatric patients. Undergraduate and graduate classes taught by Professor Yonovitz include Auditory Systems and Disorders, Audiology, Seminar in Fluency Disorders, Biomedical Instrumentation, Industrial Audiometry and Hearing Conversation, Computer Applications in Speech Pathology and Audiology, Hearing and Speech Science, Research Methods in Speech Pathology and Audiology, Physiological and Psychological Acoustics, Special Topics: Middle Ear Mechanics, Special Topics: Audiometry with the Difficult to Test, Special Topics: Measurement of Voice, Hearing Impairment, Anatomy of the Speech and Hearing Mechanism, Aural Rehabilitation, Speech Science, Introduction to Audiology, and Audition. He is a partner in Yonovitz & Joe, LLP.

A Police Investigation Meets Forensic Accounting

Timothy Pearson, Associate Professor; Director, Division of Accounting; West Virginia University
Richard A. “Dick” Riley, Jr., Louis F. Tanner Distinguished Professor of Public Accounting, West Virginia University

The following facts, circumstances and evidence mirror those of real-world alleged criminal wrongdoing. Due to the timing of adjudication and confidentiality restrictions, however, those facts, circumstances, and evidence have been modified so as to disguise the specific scheme and persons involved. In some places, the facts, circumstances, and evidence has been simplified to emphasize important points concerning forensic accounting investigation.

Introduction

On December 4, 2006, a CPA of a local company is working through the books and records related to the arcade portion of a business in order to complete the long overdue 2005 tax return. The owner is a notorious procrastinator and is already facing interest and tax penalties because the CPA first received the books and records in mid-November. The CPA observes that the lease billings for the arcade machines seem to be excessive compared to the bank deposits. The following depicts the actions taken by the CPA, the reaction by the company owner, the involvement of the local police department, and the incorporation of a forensic accountant into the investigative process.

The Initial Discovery

In December of 2006, Jeremiah Jones, a local CPA, is preparing the tax return for a local business. This business has several types of operations, and each one has a separate bank account and separate books and records. The financial “parts” gathered from the various business operations are then combined or consolidated into one set of internal financial statements and one tax return. Jeremiah added up the arcade deposits to determine the sales revenue for the year and gathered the expenses. As he completes this analysis, he notes that arcade expenses appear to be high and profitability appears to be low. He pulls out the tax working papers for the last several years and notes that revenues and profitability seem to have deteriorated during 2004 and 2005 when compared to prior years as shown in Table 1.

Table 1. Sales and Profits – Arcades

	2002	2003	2004	2005
Sales Revenue	\$195,000	\$197,000	\$178,000	\$149,000
Income	\$39,000	\$39,000	\$21,000	\$8,000
Income Percent	20.0%	19.8%	11.8%	5.4%

Nothing else seems to be problematic. The accounting numbers appear to tie back to supporting documentation (e.g., invoices, bank statements, etc). The bank deposits

and checks from the bank statements reconcile to the underlying accounting books and records. This type of “red flag” or anomaly is common in accounting records and in and of itself does not indicate any wrongdoing. Nevertheless, Jeremiah calls the company owner to ask him about his perception of the business and its performance.¹ He discovers the following information from the owner:

- Traffic in the areas around the arcade has been steady to increasing.
- The owner has used the same supplier of arcade machines and generally has been very satisfied with the service provided.
- The arcade machines are leased from a national dealer that specializes in such machines.
- The billing for the arcade machines is based on internal, mechanized readings taken by the owners of the machines. The lessee (arcade) commits to a monthly minimum plus additional lease costs for excess revenues (machine usage), but this arcade is in a popular location and exceeding the minimums has not been a concern in past months.
- The arcade has room for 18 machines and has been at capacity since opening.
- The arcade equipment lease agreement provides that within 24 hours of a machine breaking down, a service technician will be on sight. If the arcade machine cannot be repaired on sight, within an additional 24 hours, a replacement machine will be substituted.
- The arcade machines cost consumers between \$0.50 and \$2.00 per “game,” but the most common machines and the average usage is expected to be about \$1.00 per use.
- The arcade is open from 10:00 AM to 11:00 PM seven days a week.
- The arcade has one manager or employee on duty at all times.
- The arcade has two cash changing machines that are maintained by Wells Fargo, and no arcade personnel have access to the cash changing machines. The company pays a fee for this service.

Armed with this information, Jeremiah continues to be puzzled by the decline in revenues and profits. The most interesting accounting item is that the arcade leasing expense to rent the arcade machines has been relatively consistent across years. From an accounting perspective, expense amounts that are consistent from year to year usually do not raise concerns; however, in this case, since arcade leasing costs are tied to usage, Jeremiah expected arcade lease revenues to mirror that of the lease expense billings and be steady. As noted in Table 1, however, revenues have been declining.

Jeremiah calls the owner back and asks to have the arcade leasing invoices pulled from the accounting filing cabinets. For the years 2003, 2004, and 2005, Jeremiah ties the monthly invoice amounts to those entered into the accounting system for arcade leasing expense and traces the amount paid to the cash disbursements journal and to the 2005 bank statements. This work suggests that the amounts paid for arcade leasing agree with the numbers in the accounting system.

Jeremiah’s next step is to estimate the dollar amount of revenue given the amount of usage for the 18 machines each month for 2003, 2004, and 2005 at an average of \$1.00 per “game.” The results of this analysis are summarized in Table 2 as follows:

Table 2. Usage Versus Arcade Sales

	2003	2004	2005
Usage Units	\$192,500	\$204,000	\$196,000
Estimated Sales	\$192,500	\$204,000	\$196,000
Recorded Sales Revenue	\$197,000	\$178,000	\$149,000
Shortage	none	(\$26,000)	(\$47,000)

At this point, Jeremiah becomes concerned. On the surface, either the sales revenues and related bank deposits are too low by \$26,000 for 2004 and \$47,000 for 2005 and money is missing, or the arcade leasing invoices are too high (by the same amounts), the company has been over-billed, and the company has paid out too much money. All of the accounting information ties back to underlying supporting documentation, but it is not possible to have steady arcade leasing expense and declining revenues.

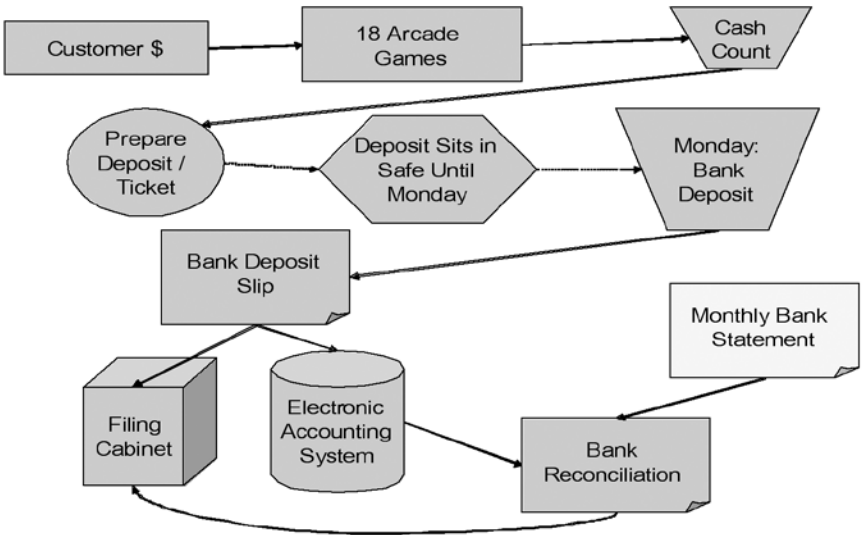
Jeremiah reluctantly calls the owner to let him know that the arcade has a potential problem and one that certainly needs further investigation. The owner loves his employees and is reluctant to believe that any of them would steal from him, and his sense is that the arcade vendor is a company with an excellent national reputation and finds it doubtful that they would risk over-billing their customers. Nevertheless, he agrees to pay the fees for the forensic accounting specialist in Jeremiah's office to investigate the problem further.

The Investigation

E.K., a forensic accounting specialist, a certified fraud examiner and a member of the Society of Forensic CPAs, agrees to start the examination to determine whether fraud has occurred. E.K. knows that even though the arcade is an active business, because a theft of money has possibly occurred, to the extent possible, he must treat the books, records, and nonfinancial arcade information as a potential crime scene. He must, therefore, take the necessary steps to identify, protect, and preserve evidence. As such, given the first indications ("red flags") noted by Jeremiah, he copies arcade deposit slips, bank statements, cancelled checks, bank account reconciliations, arcade invoices, and arcade logs in the presence of the owner after regular business hours. He also discretely calls the national arcade company pretending to be a potential customer to inquire about how the company knows how much to bill for machine usage (among other things). He finds that the arcade leasing company has a person electronically read the digital counter on each machine each month. This data is then transferred via the Internet to their company headquarters for processing and billing.

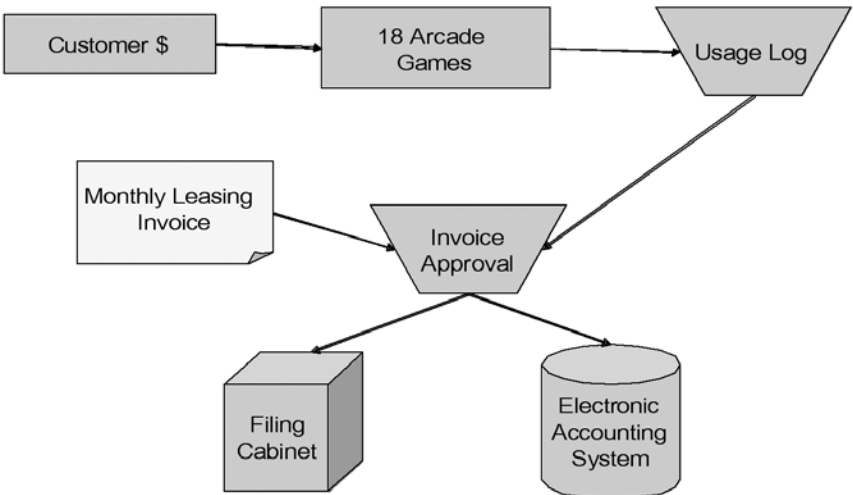
To start the investigation, E.K. first interviews the owner about how the process is "supposed to work" for the collection and deposit of money and the payment of bills. Much like crime scene professionals, E.K. makes use of graphics and draws a picture to graphically depict certain aspects of the case. First, he illustrates a simplified version of the cash collection process:

Figure 1. Flow Chart of Cash Deposits



Similarly, E.K. graphically depicts the disbursement process for the arcade leasing invoices received as follows:

Figure 2. Flow Chart of Arcade Lease Disbursements



E.K. then compares the copy of the arcade usage log obtained from the accounting department records for the 18 arcade machines to the usage amounts on the leasing company invoices. He finds that the company's internal usage logs agree with those on the arcade leasing invoice and preliminarily concludes that this does not appear to be a billing scheme. Given the usage amounts noted on both the

arcade usage logs and related invoices, however, E.K. also reaches a preliminary conclusion that deposits are significantly understated and that most likely, cash has been embezzled.² The owner of the arcade business is livid that money appears to be missing. He also knows the local police chief because the two were college fraternity brothers. As a result, Detective Tessmer was assigned to work with the forensic accountant to delve more deeply into the investigation.

Why Do People Commit Fraud?: The Fraud Triangle

Fraudsters, by their very nature are trust violators. They are persons who have achieved a position of trust within an organization and have chosen to violate that trust. According to the Association of Certified Fraud Examiners, owners and executives are involved in only about 19.3% of frauds. Managers are the second most frequent perpetrators, committing 41.2% of frauds and wreaking \$218,000 worth of damage, on average. Finally, line employees are principal perpetrators in 39.5% of schemes, yielding company losses of approximately \$78,000. Research suggests that although males are most frequently the perpetrators, in 39% of fraud cases, a woman is the principal perpetrator. Fraudsters are present in all age categories and educational achievement levels, but victim losses rise with both the age and education of the principal perpetrator. In 60.2% of the cases, the perpetrator acts alone; however, when fraudsters collude, the losses to the victim organization increase almost fivefold. Table 3 characterizes the typical fraud perpetrator:

Table 3. Fraud Perpetrator Profile

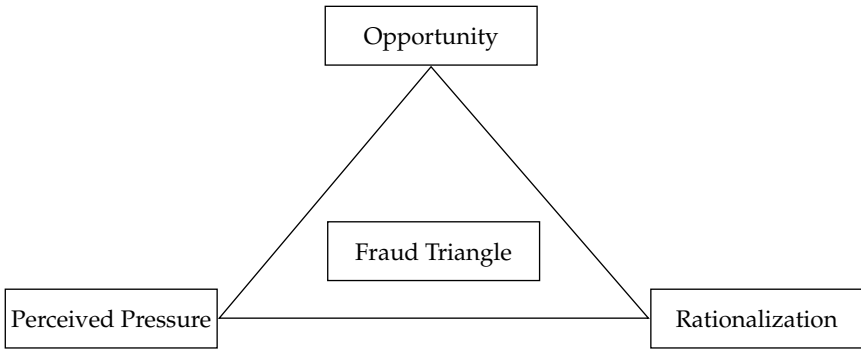
Male ³	Well Educated
Middle Age to Retired	Accountant, Supervisor, Manager, or Executive
Been With the Company for 5 or More Years	Acts Alone
Never Charged or Convicted of a Criminal Offense	

Male or female, fraud perpetrators look like average American citizens. Of all the characteristics list above, maybe most interesting, fraudsters typically do not have a criminal background.⁴ Furthermore, it is not uncommon to see fraud perpetrators who are well-respected members of their community, belong to and attend church services, are married, and have children. In 89.8% of the fraud cases examined by the ACFE, the perpetrator had been with the victim organization for more than one year. As author Steve Albrecht noted at the Fraud and Forensic Accounting Education Conference held in Pittsburgh, September 8, 2006, “Just because someone has been honest for 10 years doesn’t mean that they will always be honest.” Furthermore, the longer the tenure, the larger the average loss. In only 12.1% of the fraud cases examined did the perpetrator have any kind of prior criminal history. These last two statistics indicate that, unless the fraudster is a predator, the typical fraudster is not a pathological criminal and has most likely achieved a position of trust. Then, the critical question remains, what causes good people to turn bad?

There are three key characteristics to any fraud: (1) opportunity, (2) perceived pressure, and (3) rationalization. These characteristics are analogous to those used to investigate homicides: (1) motive, (2) means, and (3) opportunity. These combined characteristics have been referred to as the fraud triangle (See Figure 3). First, the fraudster needs the opportunity to commit fraud. Whether the issue is management override related to

a financial statement fraud or a breakdown in the internal control environment that allows the accounts receivable clerk to abscond with cash and checks entering the business, the perpetrator needs to have opportunity. Without opportunity, no fraud can occur. When it comes to fraud prevention and deterrence, most accountants tend to direct their efforts towards minimizing opportunity through the internal control environment; however, internal controls are just one element of opportunity. Other integral parts of opportunity are related to adequate training of clerical and supervisory personnel, adequate supervision, monitoring of executive-level management by auditors, audit committees and boards of directors, proactive anti-fraud programs, strong ethical culture, fraud auditing, tips hotlines, and whistleblower protections.

Figure 3. The Fraud Triangle



Many people inside any organizational structure will have at least some opportunity to take cash, checks, or other assets; however, it is the second condition, perceived pressure that causes the person to consider internal control weaknesses more than just opportunity. Fraud pressures can arise from financial problems such as living beyond one's means, greed, high debt, poor credit, financial losses from unexpected sources such as healthcare expenses for a loved one, investment losses, and children's education. Other pressures arise from vices such as gambling, drugs, and taking on an extramarital affair. Financial statement fraud is often attributed to budget pressure, deadlines and cutoffs, bonus opportunities, and maintaining stock price. Finally, pressure may stem from the mere challenge of getting away with it or family and peer pressure. The word *perceived* is carefully chosen here. It is important to understand that different persons react differently to different stimuli. It is also important that fraud investigators and forensic accountants keep an open mind. Pressures that would have no impact on the fraud examiner's personal choices may dramatically change someone else's normal mode of operation.

Finally, the characteristic that puts the fraudster over the top is rationalization. How does the perpetrator sleep at night? How does the fraudster look at him- or herself in the mirror? As noted above, the typical fraud perpetrator has no criminal history and has been with the victim company for some length of time. Since he or she is not a habitual criminal and is a person in a position of trust, he or she must have earned that position. So, in order to live with him- or herself, the fraud perpetrator has to develop some rationalization for his or her actions,

and rationalization is the issue that puts him or her over the top. Rationalizations are manyfold and include the employee/manager's feeling of job dissatisfaction; no recognition for a job well done; low salary and pay; and an attitude of "they owe me," "I am only borrowing the money," "nobody will get hurt," "they would understand if they only knew my situation," "it's for a good purpose," and "I just need the money to get over this hump."

MICE

In addition to the fraud triangle, we capture the typical motivation of the fraud perpetrator with the acronym MICE:

- M = money
- I = ideology
- C = coercion
- E = ego

Money and ego are the two most commonly observed motivations. Enron, WorldCom, Adelphia, Pharmor, and ZZZ Best provide good examples of fraud in which the convicted perpetrators seemed to be motivated by greed (money) and power (ego). Less frequently, you see persons unwillingly pulled into a fraud scheme (coercion). These lower level individuals are often used to provide insight and testimony against the ring leaders and as such, receive lesser sentences or no sentence at all. Ideology is probably the least frequently observed characteristic related to fraud and financial crimes, but society has observed this characteristic with regard to terrorism and terrorism financing. With ideology, the end justifies the means, and perpetrators steal money to achieve some perceived greater good that furthers their cause. While the MICE heuristic oversimplifies fraudulent motivations and some motivations fit multiple categories, it is easily remembered and provides investigators with a framework to evaluate motive.

Forensic Accountants Use Evidence-Based Decisionmaking

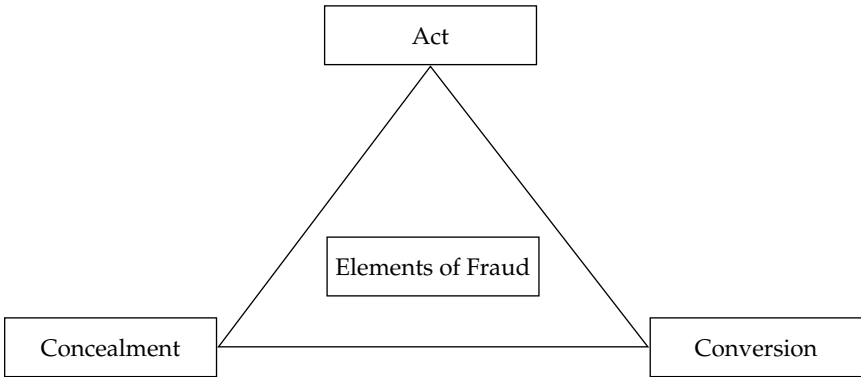
As every law enforcement officer knows, one of the best ways to ruin an investigation or fail to gain a conviction is to base investigative conclusions on logic and conjecture. Many a person has tried to convict an alleged perpetrator using the "bad person" theory. The investigator concludes that the defendant is a bad guy or will not come off well during trial, and thus, he or she must be the perpetrator or have done something wrong. Unfortunately, this approach fails to win the hearts and minds of prosecutors, plaintiff and defense lawyers, and juries and can result in significant embarrassment for the fraud professional or forensic accountant. Thus, forensic accountants develop their cases like other law enforcement personnel using evidence-based decisionmaking.

The Problem of Intent: Investigations Centered on the Elements of Fraud

While the fraud triangle provides an effective explanation for the conditions necessary for fraud to occur and is a source of red flags that require investigation in order to prove fraud, the investigator has to deal with the problem of intent. Intent, like any aspect of the investigation must be grounded in the evidence. In

a fraud case, the challenge is that short of a confession by a co-conspirator or the perpetrator, evidence of intent tends to be circumstantial. Although less famous than the fraud triangle, the elements of fraud are critical to the investigative process (See Figure 4). The elements of fraud include the act (e.g., fraud act or financial crime such as money laundering), the concealment (hiding the act or masking it to look like something different), and the conversion (the benefit to the perpetrator).

Figure 4. Elements of Fraud



Provided that the investigator has evidence that the alleged perpetrator committed the act, benefited from that act, and concealed his or her activities, it becomes more difficult for the accused or litigant to argue that they did not intend to cause harm or injury. Evidence of concealment, in particular, provides some of the best evidence that the act was intentional.

Evidence of the act may include that gathered by traditional law enforcement activities such as surveillance, wiretaps, interviewing, and other physical evidence and through tools and techniques unique to forensic accounting such as invigilation, documentation, posting to bank accounts, missing deposits, and other financial evidence. Proof of concealment can be obtained from audits, through document examination, and computer searches. Furthermore, conversion can be documented using public records searches, the tracing of cash to a perpetrator's bank account, and indirectly using financial profiling techniques. Finally, interviewing and interrogation are important methods that can be used to supplement other forms of evidence in all areas: act, concealment, and conversion. There is a current debate among forensic accounting professionals about whether tracing money to a perpetrator is adequate evidence of conversion or whether the investigator needs to show how the ill-begotten money was used. While tracing the money into the hands of the perpetrator or his or her bank account is sufficient, showing how the money was used provides a more powerful case and can provide evidence of attributes of the fraud triangle, such as pressure and rationalization and other motivations included in MICE. Generally, investigators should take the investigation as far as the evidence leads.

Examples of circumstantial evidence that may indicate the act, concealment, or conversion include the timing of key transactions or activities, altered documents,

concealed documents, destroyed evidence, missing documents, false statements, patterns of suspicious activity, and breaks in patterns of expected activity.

Armed with the knowledge concerning the fraud triangle, MICE and the elements of fraud, and the cash flow processes and with evidence suggesting that the issues are associated with cash inflows (e.g., bank deposits and revenues), Detective Tessmer and E.K. re-examine cash deposit flows for opportunity. During that process, they note the following:

- An informal (i.e., laymen's) examination of deposit slips indicate that the deposit slips do not appear to be altered and that the handwriting on the slips seems to mirror that of the arcade usage logs prepared by the manager. If necessary, these items could be sent to a handwriting expert for further examination and a professional conclusion.
- The arcade manager works 5 days a week: Thursday through Monday.
- To cover the times when the arcade is open but a manager is not present, part-time employees are used.
- During his or her shift, the manager . . .
 - Opens each arcade machine, updates the usage log, and extracts all of the cash.
 - Prepares one deposit slip.
 - Places the deposit envelope with wrapped coins in the safe.
- The same manager has been with the company since the beginning of January 2003.
- Most part-time employees are high school and college students, and none has lasted more than 9 months. This assertion was confirmed using payroll records.
- Part-time employees do not have access to the safe but are expected to open and close the arcade. The arcade has an electronic security system.

The remainder of the cash flow process is handled as follows:

- Each Monday, Wells Fargo, in the presence of the manager, retrieves the week's deposits from the safe and takes them to the bank.
- Each Monday afternoon, the manager collects the deposit receipt from the bank and sends it along with the log to company headquarters.
- Company headquarters has no access to cash.
- A clerical employee at company headquarters records the deposits.
- The accounting supervisor at company headquarters prepares the bank reconciliation. The bank reconciliations usually are completed about every 3 to 6 months in batches.
- Company headquarters has a small staff with one clerical employee and one accounting supervisor. Both work 45-55 hours per week and account for the financial transactions of the arcade and other business operations for the company.

Given this information, the person with the most opportunity appears to be the arcade manager who started work in early 2003. The forensic accountant and fraud examiner value the skills of a good interviewer as much as traditional law enforcement. At this point, it is agreed that the best approach is to interview the current part-time employees and the accounting staff. Detective Tessmer conducts

the interviews using traditional interviewing methods and protocols. E.K. then uses the information from the interviews to examine the documents collected to ensure that the information and explanations provided by these individuals agree with the underlying evidence. Based on these procedures, Detective Tessmer and E.K. draw the following preliminary conclusions:

- Since company headquarters has no access to cash, only a billing scheme would be possible (because company headquarters accounting personnel do not have access to bank deposits).
- Because accounting and the reconciliation process at headquarters are completed by different personnel, only through collusion between the accounting clerk and accounting supervisor could a fraud be perpetrated and concealed.
- Because the part-time personnel never lasted more than 9 months and the embezzlement appears to span at least two years, part-time personnel could not have orchestrated the fraudulent activity.
- Similarly, only the store manager was present for the entire period of the alleged embezzlement activity.

Thus, the investigative team concludes that based on the evidence, the only person with opportunity was the store manager.

In late December 2006, Detective Tessmer and Certified Fraud Examiner E.K., with the owner's permission, agree to confront Store Manager K.P. using interrogation methods in the hopes of gaining a confession. As soon as the two investigators confront Store Manager K.P., however, he requests a lawyer and refuses to answer any questions.

The Outcome of the Investigation

How Much Were the Losses? The Act

E.K. uses a forensic accounting technique known as invigilation to estimate the amount of losses. Invigilation is an investigative technique that considers periods before, during, and after a suspected fraud or financial crime has occurred. The method looks for patterns and changes in patterns around the time that the suspicious activity occurred. The method provides evidence of the act by helping to calculate how much money may be missing and helps to provide powerful visual evidence that a fraud has occurred.

Store Manager K.P. is suspected of stealing money from a group of arcade machines (See Table 4). Notice that the deposits decline during the period of K.P.'s employment until his termination at the end of 2006. In 2007, deposit levels rise almost to the level immediately prior to K.P.'s pre-employment period. This pattern is clear and distinct and suggests that something occurred, and the correlation between the pattern of deposits and the period of K.P.'s employment becomes a compelling piece of evidence.

Table 4. Deposits 2001-2007

Month	Prior to Hiring K.P.		Period of K.P.'s Employment				After K.P.
	2001	2002	2003	2004	2005	2006	2007
January	\$16,308	\$15,076	\$16,211	\$16,951	\$13,108	\$8,057	\$16,323
February	14,776	14,831	14,699	14,805	14,323	10,046	17,590
March	15,572	14,688	17,375	15,917	11,679	8,586	14,530
April	16,254	14,044	16,098	14,038	12,684	9,243	15,532
May	16,540	16,695	15,449	12,278	9,096	8,637	15,541
June	16,562	12,157	14,547	14,283	12,833	8,358	15,037
July	19,752	18,215	17,268	13,927	11,365	9,144	17,022
August	20,782	14,827	19,525	12,766	12,725	10,258	17,931
September	15,964	17,450	12,974	13,090	11,166	9,010	18,681
October	12,224	16,281	14,220	15,283	10,519	7,937	13,962
November	18,304	18,092	16,737	15,595	12,361	9,340	17,570
December	20,304	22,685	22,265	19,123	16,642	11,238	16,614
Actual	203,343	195,042	197,366	178,056	148,503	109,853	196,331
Expected			198,239	198,239	198,239	198,239	198,239
Estimated Overage (Shortage)			-873	-20,183	-49,736	-88,386	-1,908
Estimated Loss Dollars						-158,305	

The three years when K.P. was not employed, 2001, 2002, and 2007, can then be used to estimate the amount of losses during K.P.'s watch over the arcade machines. The expected annual deposits, assuming no increase in arcade prices is \$198,239 $([203,343 + 195,042 + 196,331] / 3)$. Next, expected bank deposited are compared to those actually made into the bank account. Based on this analysis, it appears that K.P. did not steal any money during 2003, his first year on the job; however, over \$20,000 appears to be missing in 2004. Furthermore, the estimated amount of missing money rises to over \$88,000 in 2006. The total estimated amount of missing money for the 3-year period is approximately \$158,000. Investigation becomes one piece of evidence that when combined with additional evidence can be presented as a compelling case.

How Did This Happen?: The Act

One of the main contributing factors was that company headquarters personnel was using the arcade usage logs to scrutinize invoices received from the leasing company but did not provide the same level of examination of bank deposits and arcade revenues. Had company personnel incorporated the arcade usage logs as a test of bank deposits and revenues, the alleged crime would have been caught in the first instance.

How Did This Happen?: The Concealment

In this example, the manager did very little to explicitly hide his actions. He completed his arcade usage logs, bank deposit records, and other required paperwork faithfully and did not appear to attempt to alter any of these documents to conceal his efforts. Further investigation and interviewing by Detective Tessmer, however, indicated that the arcade manager was known to make numerous calls to the accounting department. Initially, these calls were concerning his payroll checks and other store related issues, but later under the guise of wanting to create career opportunities for himself within the company, it was clear that he gradually

accumulated knowledge about how the internal control procedures worked and devised a means of exploiting weaknesses in the internal control system. Thus, the primary evidence of concealment is that he knew that the arcade usage logs were only used to check the arcade leasing invoices and were not used check bank deposits and revenues.

Another mean of concealment was that the store manager knew that the accounting staff was probably overworked. They were known to work long hours and although dedicated, did not have adequate time to carefully look at all potential problems. Furthermore, the store manager knew that the accounting staff did not spend much time analyzing company performance nor the performance of the various aspects of the business. Whether this was due to a limitation of their duties or to a shortage of time was not known.

How Did This Happen?: The Conversion

As noted above, forensic accounting and fraud professionals debate how far one must track the cash to provide evidence of concealment. The challenges are many. For example, most fraud perpetrators are clever enough to not run ill-begotten gains through their checking account. In addition, if the embezzled monies are in the form of cash, no audit trail exists for the money. In this case, Detective Tessmer set up a fixed point surveillance of the arcade using video technology at the information booth and of the manager's office where the safe is located. During that surveillance, the store manager was noted as taking rolls of coins and placing them in his briefcase. He was then seen leaving the store with the briefcase. Detective Tessmer also drove by the manager's home to observe the neighborhood and to see whether an unusual amount of "toys" (e.g., boats, cars, jet skis, etc.) had been collected. E.K. visited the county courthouse to identify records of ownership, and liens and records were obtained on ownership from the state DMV; however, none of these methods indicated that the store manager was living a lifestyle beyond his means or had an unusually high amount of personal debts. Subsequent to the attempted interrogation of the store manager, his personal bank statements (including cancelled checks and deposit records), credit card statements, and tax records were obtained, but these records did not indicate anything unusual. When indications of excessive debt or lifestyle excesses are observed, forensic accountants and fraud examiners can formally document such observations using techniques such as net worth, sources and applications of funds, and bank records analyses. The overall conclusion in this example is that the manager had taken possession of the cash, but the uses of the cash could not be determined.

Insurance Coverage: A Possible Source of Recovery

Despite this gloom, all may not be lost. If the company has an all-risk property insurance policy, it may include a rider for thefts and embezzlement. Insurance policies may present some challenges. First, the policy may require that the insurance company be notified immediately upon discovery of losses. In addition, although the insurance policy is all-risk, the rider may include provisions in which certain types of losses are excluded. Typically, the insurance rider will not cover losses arising during the normal course of business. While these issues may present a challenge, insurance coverage can help mitigate losses arising from fraud.

Lessons Learned

Trusted employees commit fraud. Even the most vigilant of employers will miss the signs of fraud until some larger signal appears or a whistleblower tip comes from someone aware of the scheme. Typically, the scheme has gone on for some time. The careful coordination of effort between the forensic accountant and police investigators can create a compelling case and potentially lead to a confession or conviction.

Additional Reading

The fraud triangle, the elements of fraud, and other forensic accounting and fraud examination topics described in this manuscript were obtained from the following primary sources:

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2006). *Fraud examination*. Belmont, CA: Thomson South-Western.

Association for Certified Fraud Examiners. (2005). *Fraud examiners manual*. Austin, TX: Author.

Crumbley, D. L., Heitger, L. E., & Stevenson Smith, G. (2005). *Forensic and investigative accounting*. Chicago, IL: CCH.

Hopwood, W. S., Leiner, J. J., & Young, G. R. (2008). *Forensic accounting*. New York: McGraw-Hill/Irwin.

Wells, J. T. (2005). *Principles of fraud examination*. Indianapolis, IN: Wiley.

Endnotes

- ¹ Readers should note that the CPA in this case is not performing an audit of the books and records. As a tax return preparer, he does not have a responsibility to complete audit tests and analytical analyses. Even in an audit, the accounting professional has a materiality threshold, under which testing is not performed, and most testing is performed on a sample basis. Thus, the involvement of a tax or auditing professional does not, nor was it designed, to identify all instances of fraud.
- ² Like all investigators, E.K. keeps an open mind about other possibilities (hypotheses) and looks for evidence that might support other possibilities as well.
- ³ According to the ACFE 2006 Report to the Nation, males perpetrate fraud 61% of the time versus 39% for females.
- ⁴ Some trust violators (fraudsters) are fired with or without paying restitution. Thus, in some cases, the fraud perpetrator is pathological in his or her work, moving from organization to organization. In those cases, some estimates indicate that the fraudster will victimize each new company within 12 to 36 months.

Timothy Pearson is a CPA, a former IRS agent, and an associate professor at West Virginia University (WVU) where he is the director of the Division of Accounting. He specializes in fraud and forensic accounting in a digital environment. He teaches in WVU's Executive MBA, Graduate Certificate in Forensic Accounting and Fraud Investigation and joint WVU-IRS Graduate Certificate Program in Forensic Accounting and Fraud Examination. Since becoming Division Director of Accounting, he has been leading WVU's efforts concerning forensic accounting in higher education including teaching, research, and service to the profession.

Richard A. "Dick" Riley is currently a Louis F. Tanner Distinguished Professor of Public Accounting at West Virginia University. His primary focus has been within the Business Masters Programs encompassing Masters of Professional Accountancy, Graduate Certificate in Fraud and Forensic Accounting, Executive Master of Business Administration, and the Center for Executive Education and Development. Dr. Riley is a forensic accountant and a certified fraud examiner who has developed and implemented education programs for the United States National Institute of Justice and the Internal Revenue Service. Dr. Riley performs expert financial analysis and litigation support for the mining, construction, and minerals processing industries and has extensive forensic litigation experience beyond these industries.

Your Investigation and the Media

Rick Rosenthal, Law Enforcement Media Relations Trainer and Consultant

Your investigation of a high-profile case will inevitably draw significant attention from the news media. You probably won't like that, but you also can't change it. Media attention in such cases is simply a fact of life: Engagement with the news media is inevitable; victory is only optional. The best-practices agencies of law enforcement understand this concept, accept it, and choose to "Win with the Media" by working with reporters in high-profile investigations while also exercising meaningful controls on the information that is being disseminated.

Commit to Working with Reporters

That choice—to work with reporters—is a major leadership decision that should be made long before your department catches the next big case. Chief Tony Kleibecker of the Muskegon, Michigan, Police Department puts it this way: "You have to be ready for the media. They're going to be there. If you're not ready, you're going to be overwhelmed. They'll get in the way; it'll interfere with the investigation and sap additional resources that you need elsewhere" (personal communication, July 6, 2007).

Effective media relations result not from a single event; rather, they come from a process that should be ongoing and as routine as all of the other daily work that you do. That means your department and your personnel should be building relationships with reputable reporters, their bosses, and their news organizations on the day-to-day events that they are interested in and building the bridges of mutual understanding and mutual respect that will give you an important edge when you undertake the investigation of a major case.

What Happens When You Don't Work with Reporters

Let's consider for a moment law enforcement's natural reluctance to work with reporters. As one public safety officer once asked me, "Why should we tell those bastards in the media anything? They're always out to screw you, and they never get it right!" Well, I did acknowledge that gentleman's concerns but tried to explain that they were misplaced. I think most mainstream media (MSM) news reporters do want to work with you, if you will just work with them, and I think most MSM reporters do try to be fair, and accurate (although sometimes with varying degrees of success.)

The point is, how can any reporter get the story right about your investigation if you and your department will not give that reporter the facts and information as you know it? Reporters have to cover your high-profile case, with you or without you (that's the definition of "high-profile"). With you, they get the story straight from reliable sources close to the investigation; without you, they begin to wander afield and find "sources" that are far less knowledgeable and far less credible. The resulting "news" is often based on innuendo, hearsay, and speculation. Jim Solomons, one-time PIO for the Orange County (FL) Sheriff's Office once told me, "Treat 'em [reporters] like animals. Just feed 'em what you can, when you can,

and they won't go foraging on their own . . . It works." It does, indeed. Feed the animals!

In fact, if reporters do go "foraging on their own" because your department has chosen the "no comment" or news blackout route, the negative impact and consequences can be serious. Angelo Bitsis spent 32 years as a law enforcement PIO in Miami and Cape Coral, Florida. Bitsis says, "You want to make sure the information the media get is directly from the [department] and is as accurate and thorough as you can make it, because as we know if you choose to withhold information or stonewall the media they're going to go elsewhere for sources and those other sources in all likelihood are not going to be speaking in the best interests of your agency or the investigation, and can often be flat wrong" (personal communication, July 9, 2007).

That's what happened during the investigation of a multiple murder case in a rural part of Will County, Illinois (outside of Chicago) in June of 2007. On June 14, authorities found the bodies of 34-year-old Kimberly Vaughn and her three children (Abigayle, 12, Cassandra, 11, and Blake, 8) inside the family's SUV on a frontage road near Interstate Highway 55 in Channahon Township. All four had been shot to death. Ten days later 32-year-old Christopher Vaughn, Kimberly's husband and the children's father, was arrested and charged with the killings. He remains in custody facing four counts of murder. Naturally, the investigation of such a horrific case drew significant attention from the news media.

After the initial response by Will County Sheriff's deputies, it was decided that the Illinois State Police (ISP) would be the lead agency in the investigation. There was an initial briefing for the news media, and then, according to Pat Barry, Director of Public Affairs for the Will County Sheriff's Office, no further official updates for the news media for the next nine days, until Vaughn was arrested in Missouri. Barry called that decision, . . .

a huge mistake [because] where no one was saying anything, nothing could be verified, so it left the field wide open for reporters to say/do anything they wanted. The State Police office and Will County State's Attorney decided to withhold all information. I think they thought if we don't give [the media] anything, we can investigate without being bothered by having to deal with the press, when the opposite is the case. (personal communication, July 6, 2007)

In fact, by choosing to not "feed the animals," it appears the investigation faced more problems with the media rather than fewer. As Pat Barry describes it, . . .

As detectives were trying to get information on the case, you had a frenzy of print and TV media that were already interviewing [family friends, neighbors, employers, other potential witnesses] . . . when detectives haven't even talked to these people yet. We had a lot of "information" that was being stirred up by the press before detectives could even get out there and verify it. . . . That hurts the investigation, hurts detectives trying to interview people. But when you're not providing information, reporters are going to go find it on their own. . . . If you provide information to them . . . you may be able to learn things from them while keeping them off your back. . . . if you don't feed 'em, you're going to get killed. (personal communication, July 6, 2007)

By giving the news media solid information about your high-profile case, you significantly increase the probability that the truth will be printed and broadcast and significantly reduce the pressure on reporters to go foraging and find “facts” (which may not be facts at all) on their own. Conversely, withholding all information, as happened for nine days in the Vaughn case, can have exactly the opposite effect. Again, according to Pat Barry . . .

After day one, the media started chasing rumors. . . . These rumors are credited to unknown sources . . . and now we were starting to see print and TV media feeding off each other for information . . . Nobody checks anything about the story, and all of a sudden somebody else picks it up, and all of a sudden you have these multiple sources, none of which are legitimate; they’re using themselves as sources. It makes it difficult for law enforcement amid a ton of misinformation, and we all know once it gets out there, you’ll never retrieve it. It makes things extremely difficult. . . . Reporters can’t find original sources because there were none. It feeds on itself with no real basis for any of this. It could lead to tragic results, the investigation could go awry or ruin someone’s reputation. It’s just crazy.

Barry’s observations—based on his personal experience in the Vaughn case—are discouraging but valid. It’s what happens in a high-profile case when law enforcement chooses to not “feed the animals.” Now, if this were an isolated instance, perhaps it wouldn’t be such a big deal, but it is a big deal precisely because such law enforcement information blackouts occur all too frequently. Take, as another example, the Gianni Versace murder case:

On July 15, 1996, serial murderer Andrew Cunanan stalked, shot, and killed international fashion designer Gianni Versace outside Versace’s mansion on Ocean Drive in Miami Beach, Florida. The murder and the subsequent investigation drew reporters in from all over the country and all over the world (i.e., it was high-profile.) The case was wrapped up 10 days later when Cunanan was found dead of a self-inflicted gunshot wound aboard a houseboat in Miami Beach.

Researcher Carlos Noriega studied the media relations aspects of the Versace/Cunanan investigation, in which—once again—law enforcement was less than fully forthcoming or cooperative with the news media. Noriega’s findings are extremely instructive and deserve to be quoted at some length:

The majority of mistakes attributed to the Miami Beach Police Department and the Public Information Office in particular involved the inability to maintain a continuous flow of information available for the media. It became painfully obvious as the investigation progressed, that the Public Information Office tried to conduct business as usual and was falling far short of the mass media’s expectations. [By “business as usual,” Noriega means the department had two PIOs who generally worked the day shift and then went home, and who did not even report for duty on the one weekend that fell in the middle of the 10-day investigation.]

The department unfortunately learned that in lieu of providing the media with timely updates and information, reporters will develop stories on their own. Media personnel demonstrated that they would not be satisfied with

having the police provide them limited information on the department's timetable. The police department missed an opportunity to use the media to their advantage and develop allies rather than adversaries. The end result produced inaccurate stories, investigative obstacles, and widespread criticism of all the agencies involved.

At the end of his dissertation, Noriega reported the "Findings of the Case Study." His conclusions are extremely enlightening for any officer or department concerned with the media relations aspects of a major investigation, and are therefore once again quoted at length:

The Versace/Cunanan case was the most publicized investigation the City of Miami Beach Police Department has ever been involved with. As such, the department was under the microscope from a media community that was prepared to expose any and every mistake made by law enforcement.

In a high-profile situation involving mass media, patience is not a luxury that competing news representatives are prepared to demonstrate. The pressure to meet deadlines and develop exclusive information is the driving force that will dictate the media's actions.

The police department's lack of experience with these types of situations became evident as the frustrations encountered by the media community immediately evolved into animosity directed towards the investigation.

The police department missed an early opportunity to set ground rules with the media by not having the Public Information Office establish open and honest dialogue from the start.

The police department failed to maintain open lines of communication with the media by keeping the Public Information Office continuously open and available throughout the 10-day period.

The police department also failed to create a controlled environment to disseminate timely, accurate, and well organized information to be reported.

With no control mechanisms in place to direct the media, a free-for-all situation developed, and there was no possible way to control their actions.

In lieu of receiving information from the investigative agencies, the media developed there [sic] own stories, accurate or not, through whatever means possible.

Finally, the police department alienated the mass media, thus becoming fair game for any criticism and/or controversy . . .

Failure to account for the media's daily involvement, especially on major events, places an organization at risk of finding unexpected obstacles, which will usually produce negative publicity and consequences. (pp. 9-10)

When the Miami Beach Police Department (MBPD) failed to “feed the animals,” the animals went foraging, tried to find something to eat on their own, and when that wasn’t sufficient, they came back and started biting the hand (MBPD) that hadn’t been feeding them. Learn from MBPD’s mistakes, and resolve to do a better job on your major investigation: Feed the animals! Feed them all the same facts and information. Feed them regularly; feed them often. You’ll have much greater control over the coverage of your investigation of your major case because reporters will be working with your facts and information, not their own innuendo, hearsay, and speculation. The positive result will be far fewer difficulties for you than MBPD encountered in the Versace/Cunanan case.

“Feeding the Animals”

How, then, do you go about working with MSM reporters? One important element is that successful management of the media in a major case requires the skills of a public information officer (PIO). With more and more electronic media (that includes newspaper websites) trying to fill more and more air time faster than ever in an intensely competitive business environment, any department that doesn’t have a PIO to manage those reporters is going to be overwhelmed. The Department of Homeland Security (DHS) and the National Incident Management System (NIMS) understand this: DHS and NIMS make the public information function a “cabinet-level” position and an integral part of management of a critical incident. You and your department should do the same (if you haven’t already done so) in anticipation of your next major investigation.

The Commission on Accreditation for Law Enforcement Agencies (CALEA) also requires “establishment and maintenance of public information” as one of the functions it deems essential for best-practices departments seeking certification. According to CALEA, “Agencies have an obligation to inform the public and news media of events that affect the lives of citizens in the community with openness and candor” (p. 54-1). Certainly, this applies when you’re investigating a major case.

CALEA goes on to state: “In large jurisdictions where media contacts are frequent and often of a sensitive nature, a full-time public information officer may be needed. . . . Where the community served is small and media contacts infrequent, the assignment of the function to an individual as a part-time responsibility may suffice” (p. 54-1). I agree. Most smaller departments do not need a full-time PIO with a specific cost line in your budget; the job can often be done well enough as a corollary duty by personnel who spend most of their time on other tasks. As DHS/NIMS and CALEA rightly assess, however, you must have the PIO function covered as an essential element of managing that high-profile case.

Please also remember that your PIO cannot operate in a vacuum. He or she is not an individual but rather a mission-essential member of your law enforcement team. In order to disseminate facts and information in a timely manner, the PIO must have access to other team members, including the chief or sheriff and other top-echelon decision-makers, as well as detectives and other investigators who are subject-matter experts on your high-profile case. All principals involved in the investigation need to support the PIO with information, including news interviews, even as the PIO is supporting your team by working with reporters.

This does not mean you have to roll over and play dead for the news media. You are not going to be media road kill. There are important controls that you need to understand and put in place to successfully manage the media in your major investigation. One of these is the Society of Professional Journalists *Code of Ethics*. The *Code* is journalism's "rules of engagement"; it's a one-page set of guidelines that detail how reporters *say* they want to behave. The four basic principles of the *Code* for journalists are as follows: (1) Seek truth and report it, (2) Minimize harm, (3) Act independently, and (4) Be accountable. (You should familiarize yourself with all of the guidelines contained in the *Code*, available at SPJ's website at www.spj.org.) As your investigation into your high-profile case is beginning, at your very first news briefing, I strongly recommend that you verbally commit your department to providing the news media and the public with as much information as you can, but also remind the news media of their own rules of engagement and insist that they give you a fair shake by adhering to the principles they themselves have outlined in their own *Code of Ethics*. I further strongly recommend that you hold individual reporters accountable when they fail to meet the basic standards of the *Code*.

You should also understand what information you can reasonably release about your major case investigation and what information you should probably withhold. Plain common sense is a good place to start. Naturally, you will not want to release any information that is going to interfere with or impede the investigation; jeopardize anyone's safety; violate anyone's rights of privacy; or violate any existing laws, policies, procedures, or union agreements. Veteran former PIO Angelo Bitsis summarizes the concept this way: "You're not always going to be able to discuss every aspect in depth on every case. The goal of a good PIO and a good law enforcement agency is to provide as much information as possible, as timely as possible, without jeopardizing the eventual successful conclusion of the investigation. . . . That can be a very tough balancing act at times" (personal communication, July 9, 2007).

One solid set of guidelines to help with that balancing act is offered by the federal Freedom of Information Act (FOIA.) Specifically in relation to law enforcement, FOIA, Title 5 U.S.C., subsection b (7) A-F provides six narrowly defined exemptions where you can (and should) withhold information, if release of the information . . .

- (A) could reasonably be expected to interfere with enforcement proceedings;
- (B) would deprive a person of a right to a fair trial or an impartial adjudication;
- (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy;
- (D) could reasonably be expected to disclose the identity of a confidential source;
- (E) would disclose techniques and procedures for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or
- (F) could reasonably be expected to endanger the life or physical safety of any individual.

The FOIA guidelines still give law enforcement wide latitude to disseminate the basic Who, What, Why, When, Where, and How of your major case. Often, that will amount to simply confirming the obvious.

Would you ever reveal a suspect's confession? Some agencies do; some don't. In St. Clair County, Illinois (across the Mississippi River from St. Louis), a suspect's confession was not only revealed, the videotape of the confession was actually

broadcast! This high-profile investigation began with the disappearance of then-17-year-old Ashley Reeves on April 27, 2006, near Belleville, Illinois. Her boyfriend, 27-year-old Samson Shelton, quickly became a suspect. Under questioning, Shelton first denied any knowledge about Reeves' disappearance but ultimately did admit they'd argued, struggled, and when she went limp he'd dragged her body into the wooded area of a local park where he left her for dead. His confession was recorded on videotape.

Shelton then took investigators to the site where he'd dumped Reeves 30 hours earlier. She was found alive and has since recovered, at least physically. Shelton was charged with one count of attempted first-degree murder. At a subsequent evidence hearing, the videotaped confession was played in open court. A local newspaper (the *Belleville News Democrat*) and three St. Louis TV stations then filed suit for public release of that videotape. Judge Milton Wharton ultimately agreed that since the confession had been played in open court, it had become a matter of public record and should be released. Shelton's confession was broadcast on the local TV stations on April 10, 2007. Prejudicial pre-trial publicity? Certainly. Immediately, there was talk of the probable need for a change of venue for Shelton's trial, but matters never went that far. On Friday, June 15, 2007, Shelton entered a plea of guilty to the attempted murder charge and was sentenced to 20 years in prison.

The point here is not whether you should or should not release information about a confession, much less the actual videotape; that's a topic of understandable concern and reasonable debate. The real point of this example is agencies of law enforcement often can release far more information about their high-profile investigation than they are inclined to, with far less impact on their case than they might expect.

Some Concluding Tips

Frequent updates are essential. If you catch a major case, you should provide information to reporters early and often. At Columbine High School in Littleton, Colorado, that's precisely what Jefferson County Sheriff's Office PIO Steve Davis did. The first reports of shots fired came in at around 11:20 that morning; Davis was on-scene by 11:41, set up his media command post, and had his first news briefing at 1:30 that afternoon. The briefings continued every hour on the half-hour for the rest of the day. When your big case hits, you should hold your first news briefing within two hours of the initiation of your investigation. Then, during the first day or two (depending on how big a case it is) you should follow with at least three formal updates per day: at 9:00 AM (in advance of the noon TV newscasts); at 3:00 PM (in advance of the early evening newscasts); and at 8:00 PM (in advance of your late evening newscasts.)

Always be straight with reporters. Never lie. Never speculate. Never tell them what you think you know, only what you're sure you do know. Deal in facts and information, period. If you get a question and don't know the answer, then an honest "I don't know" is the perfect reply. Says PIO Bitsis, "There's nothing wrong with saying I don't know, if you follow with '. . . as soon as we do know, we'll be happy to share that with you.' . . . There are always going to be questions. Don't ever give the impression that you're hiding or stonewalling" (personal communication, July 9, 2007).

Choose your words carefully. To avoid confusion, say what you mean, mean what you say, and make sure reporters get it. If you're investigating a rash of residential burglaries, make sure they don't turn that into "home invasions." If you don't have probable cause to get a warrant and arrest a "suspect" in your high-profile investigation, then your investigation is focusing so far only on a "person or persons of interest." Using that important alternate term reduces confusion on the part of the media, lowers their expectations, and reduces the pressure on you for an immediate arrest.

Use all of your communications tools. Maximize your effectiveness in managing the media in a high-profile case by going beyond the standard news briefing. SGT Larry King, Lee County (FL) Sheriff's Office PIO rightly recommends that the "service-minded PIO" utilize ". . . Internet, e-mail, office phone, cellular phone, voice mail, Nextel, wireless laptop computer. The PIO must be available to use the immediacy of these tools. There is no reason why an initial inquiry can't be answered within minutes rather than hours or 'when I get around to it'" (personal communication, July 2, 2007).

Conclusion

By definition, your high-profile investigation will draw significant media attention. You know that, right now, before you ever catch the next Big One. Plan for that reality by committing to working with the media, under the guidelines and recommendations that I've respectfully provided in this monograph. You won't hit a media relations home run every time you step up to the news briefing plate, but I guarantee you your batting average will go way up. Media coverage of your major case will never be perfect, but with the 'best efforts' strategies and tactics I've suggested here, you will have far greater input into—and far greater control of—media coverage of your major case. Choose and prepare for the route of collaboration rather than confrontation: "Feed the Animals!"

Bibliography

Commission on Accreditation for Law Enforcement Agencies (CALEA). (2001, November). *The standards manual of the law enforcement agency accreditation program* (4th ed.). Fairfax, VA: Author.

Federal Freedom of Information Act, Title 5 U.S.C., subsection b (7) A-F.

Noriega, C. The Versace/Cunanan Case: Individual case study, an unpublished seminar term paper.

Rick Rosenthal, award-winning veteran former Chicago radio and TV news anchorman and reporter, is now a nationally known law enforcement media relations trainer and consultant.

The Legality of Canine Sniffs and Motor Vehicle Stops Revisited

Barry M. Anderson, JD, MA, Associate Professor, Department of Law Enforcement and Justice Administration, Western Illinois University
Terry M. Mors, EdD, MA, Associate Professor, Department of Law Enforcement and Justice Administration, Western Illinois University

In the January 2006 special edition of *Law Enforcement Executive Forum*, the authors wrote about the legality of canine sniffs and motor vehicle stops immediately after the U.S. Supreme Court ruled in *Illinois v. Caballes*, 125 S.Ct. 834 (2005) that canine sniffs were not searches within the meaning of the 4th Amendment. At that time, the Illinois Supreme Court had not considered whether or not it was going to adopt the U.S. Supreme Court's decision.

A little background information would be appropriate here. The Illinois law in *Illinois v. Caballes* (2003) prior to the U.S. Supreme Court ruling in 2005 was that police needed at least some suspicion before using a canine unit at a motor vehicle stop. The authors' previous article was directed toward the possibility that the Illinois Supreme Court could have reconsidered the applicability of the "no-search" ruling of the U.S. Supreme Court and kept their requirement for some suspicion before using the canine unit. This could have been done, as individual states are not required to "lock-step" and adopt the rulings of the U.S. Supreme Court. They, in fact, can choose to give their citizenry more constitutional protection than the U.S. Supreme Court ruling. In other words and in this case, Illinois could have left the requirement for some suspicion before police could use a canine unit at a vehicle stop.

In May of 2006, however, the Illinois Supreme Court reviewed the *Caballes* decision and decided in a 4-3 decision to adopt the new rule (for Illinois) that canine sniff searches are not in fact searches and thus can be used at the officer's discretion in a motor vehicle stop [(see *Illinois v. Caballes*, 851 NE 2d 26 (2006)]. It should be noted that the first Illinois *Caballes* decision was a 4-3 verdict. A majority justice retired between the first and second *Caballes* decisions and was replaced by a justice who became a part of the new majority, and it was also a 4-3 decision in the opposite direction.

In reviewing the possible effects of the new ruling on Illinois law enforcement, the authors noted that "motor vehicle stops" not only cover stops for which there is suspicion or probable cause of a law violation, but they also include motor vehicle stops at checkpoints. These are vehicle stops (referred to as special needs searches) that the U.S. Supreme Court has allowed, in which checkpoint stops of all cars for a pre-designated time are allowable for reasons of vehicle safety, illegal aliens, and driving under the influence (DUI) investigations (see *Delaware v. Prouse*, 1979; *U.S. v. Martinez-Fuerte*, 1976; *Michigan Department of State Police v. Sitz*, 1990).

These special needs searches are allowed with no suspicion whatsoever by police officers in order to protect and better secure public safety. The Court in the rulings basically allows the lack of any suspicion by balancing the type of offense and the brevity of the stop with the need to protect the public from drunk drivers, protect people driving unsafe vehicles, or prevent illegal aliens from entering the country.

The authors decided to see what some law enforcement agencies were doing in light of the change in the law. It has been discovered that many law enforcement departments in Illinois are routinely using canine units at, for example, a DUI checkpoint and being used for every car proceeding through the checkpoint. Their support for this position is that the U.S. Supreme Court has ruled that canine sniffs are not searches within 4th Amendment guidelines because of their noninvasive nature. Additionally, it has been discovered that many smaller departments are now seeking funding to buy drug sniffing dogs for similar reasons.

In light of the above practice, and since the authors perceived a potential problem in the use of canine units at checkpoint vehicle stops, the authors felt that police administrators should be aware of a potential legal issue. The U.S. Supreme Court, in *Indianapolis v. Edmond* (2000), ruled that roadblock and checkpoint vehicle searches are not allowable when looking for drugs. Canine units were used in that case. The Court, in essence, said that law enforcement officers are not allowed to stop cars with no suspicion whatsoever using canine units because of the seriousness of the possible offenses involved and criminal nature of the investigation purposes. The public safety balancing portion was in essence gone in those instances, thus reverting motor vehicle stops for drug investigations to, at least, having some sort of suspicion of drug activity. The Court also drew a line regarding limiting the use of the special needs roadblock or checkpoint stops, and that line stopped with drug investigations.

The proponents for the use of canine units at such checkpoints argue the following:

- The canine sniffs are not searches and therefore not subject to 4th Amendment scrutiny.
- The apparent reason for the checkpoint stop is legal (DUI) according to the U.S. Supreme Court in *Sitz*.
- Even if the reason for the roadblock might subjectively be to find drugs, in addition to the DUI reason, the courts cannot look behind the actual stop for any subjective reasons according to *Whren v. U.S.* [517 U.S. 806 (1996)]. Pretextual vehicle stops are acceptable and legal, and the courts cannot look behind the actual reason for the stop to a subjective reason.

The following is a brief explanation of the facts involved in *Whren*. Undercover police officers in an unmarked car observed a car go by being driven by a known drug dealer. They had no reason to stop the car but felt certain there were probably drugs in the car. They decided to follow the car, and when, or if, the driver made a traffic violation, the police would pull the vehicle over. It also should be stated that traffic stops were prohibited by their department policy for undercover officers not in uniform and driving an unmarked car. After stopping the car, drugs were discovered in the car (in plain view), and the officers arrested the individuals. The pretextual issue was argued along with the subjective intent issue. The U.S. Supreme Court held that as long as the stop was legal (in this case for a motor vehicle violation), then the subjective intent of the officers was irrelevant. The drug conviction was upheld.

What the authors want police administrators to realize is the seemingly conflicting wordage of the U.S. Supreme Court in *Indianapolis v. Edmond*. The issue of *Whren* was addressed by the Court:

... While we do not limit the purposes that may justify a checkpoint program to any rigid set of categories, we decline to approve a program whose primary purpose is ultimately indistinguishable from the general interest of crime control. Petitioners argue that our prior cases preclude an inquiry into the purposes of the checkpoint program. For example, they cite *Whren v. U.S.* ... to support the proposition that “where the government articulates and pursues a legitimate interest for a suspicionless stop, courts should not look behind that interest to determine whether the government’s primary purpose” is valid. ... These cases, however, **do not** control the instant situation.

In *Whren*, we held that an individual officer’s subjective intentions are irrelevant to the 4th Amendment validity of a traffic stop that is **justified objectively by probable cause** to believe that a traffic violation has occurred. (emphasis added, pp. 45-46)

Clearly in the DUI checkpoint situations, there is no reasonable suspicion or probable cause needed to stop a vehicle. *Indianapolis v. Edmond* clearly directed that suspicionless drug checkpoint stops and the use of canine units are illegal.

For argument’s sake, assume that a department is going to run a DUI checkpoint, a clearly legal procedure to detect impaired motorists and to deter people from driving drunk. While running that checkpoint, an officer looks at the paperwork for the vehicle and the motorist’s driver’s license and finds something improper and illegal. There is no problem with writing a citation for, say, an expired driver’s license. This can be done even though this was a DUI checkpoint.

Using the same DUI checkpoint example, the driver opens his window, and the obvious smell of marijuana comes wafting out of the car. The police have a canine unit available. It is perfectly legal for the police to run the dog around the car, even though this is a DUI checkpoint. The police are obviously not precluded from arresting the person for whatever drug charge applies.

Using the same checkpoint situation in which there is no such “wafting” or any indication of drug activity, police run the canine unit around the car because they have been told that every car will be subject to the dog sniff even though this is a DUI checkpoint. The dog reacts; drugs are found in the car; and the officer arrests the driver. Is there any question as to the validity of the latter arrest?

What is the perception, or argument, in the case in which a canine unit is employed with every vehicle? Although purported to be a DUI checkpoint, the use of the canine unit arguably also makes this a drug search. That would, or could, arguably, violate the holding in the *Edmond* case.

A better policy, in the authors’ opinion, would be to conduct the DUI checkpoint within the guidelines of *Sitz*, and if something gives rise to the suspicion of drug activity, then use a canine unit, but not for every vehicle coming through the checkpoint. The authors do not believe the pretext allowances of a legitimate

vehicle stop on probable cause or reasonable suspicion are at all comparable to the special needs checkpoint stops, which the Court has clearly delineated.

The authors believe that *Edmond*, *Sitz*, and *Whren* are all good law, within their various factual and legal contexts; however, the mixing and matching of concepts from one case to another may not work because of their obvious different situations, both factually and legally.

In summary, the authors believe that a cautious and reasonable approach in the area of checkpoint vehicle stops and use of canine units is advisable. The authors firmly believe that the conflicting legal concepts will eventually be tested in the courts. It would be a shame to lose a large drug case, as there is a reasonable option. That option is to use canine units at checkpoints only when there is some suspicion of drug activity.

Works Cited

Delaware v. Prouse, 440 U.S. 648 (1979).

Indianapolis v. Edmond, 531 U.S. 32 (2000).

Michigan Department of State Police v. Sitz, 496 U.S. 444 (1990).

Illinois v. Caballes, 802 N.E. 2d 202 (2003).

United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

United States v. Place, 462 U.S. 696 (1983).

Barry Anderson, MA, JD, is an associate professor in the Law Enforcement and Justice Administration Department at Western Illinois University. Professor Anderson possesses an undergraduate degree from Grinnell University in Iowa, a master of arts degree from Western Illinois University, and a juris doctorate from the University of Iowa. Professor Anderson is a former prosecutor, defense attorney, and magistrate in the state of Iowa. He is a licensed practicing attorney in Illinois and Iowa and a nationally recognized expert on the death penalty. Professor Anderson has taught numerous police inservice training classes and made numerous presentations nationwide, and he is currently teaching undergraduate and graduate law classes.

Terry Mors, EdD, is an associate professor with the Department of Law Enforcement and Justice Administration at Western Illinois University. Dr. Mors received a baccalaureate degree from Roosevelt University, an MA in law enforcement and justice administration from Western Illinois University, and an EdD degree from Northern Illinois University in 2002. Having worked for the Gurnee, Illinois, Police Department in numerous positions ranging from patrol officer to commander, Mors possesses over 17 years of law enforcement experience. Professor Mors teaches criminal justice courses at the collegiate level and serves as a law enforcement and public safety consultant. He has made numerous presentations worldwide on various topics in law enforcement.

Our Panoptical Society Where the Invisible Becomes Visible¹

Jill Joline Myers, JD, Assistant Professor, Department of Law Enforcement and Justice Administration, Western Illinois University

Introduction

The “right to be left alone” was Louis Brandeis’ concept of privacy in 1890.² He believed that one of the primary purposes of the law was to protect private matters from public disclosure. Later, as a Supreme Court Justice, Brandeis elaborated on this belief by suggesting that the Constitution should afford protection against invasions of individual security. Brandeis predicted more than 75 years ago that the progress of science would furnish the government “with means of espionage . . . by which the Government . . . will be enabled to expose . . . the most intimate occurrences of the home.”³ Although Brandeis accurately predicted that scientific advances and technology would afford the government with the means to effortlessly surveil its citizens, even he would likely be astounded by the extent to which information, communication, and bodily and environmental privacy⁴ invasions exist today. Private sector and public surveillance is a way of life.

In the 18th century, a philosopher named Jeremy Bentham designed a circular prison whereby from a central tower, a watchman could always observe each individual cell, although not simultaneously. Because of the actual ability to do so, the perceived threat of surveillance became as great a threat as the surveillance itself.⁵ With the technological advances and new science of surveillance available in our society, a modern panopticon has morphed from Bentham’s central tower in a circular building into a global phenomenon allowing both synoptic (a general overview) and analytic (individual, detailed subject matter information) viewing.⁶ In other words, the ability to see without being seen exists on a global level.

Brandeis’ concept of a constitutionally protected right to privacy, although acknowledged, remains quite vague. The right to privacy has been recognized to exist in various facets of life, including the individual’s interest in avoiding disclosure of personal matters⁷ and “the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”⁸ This article focuses on the first facet and will discuss the right of the individual to be free in his or her private affairs from governmental surveillance and intrusion.

Right-of-privacy battle lines are evolving to define and defend the ability of individuals to protect what information about oneself is collected and how that information is used, stored, and disseminated.⁹ The abuses and breaches of data security¹⁰ created by this flow of personal information have spawned media coverage, lawsuits,¹¹ right of privacy legislation¹² requiring disclosure of information collection practices,¹³ correction procedures, opt-out opportunities,¹⁴ and extensive debate.

This article illuminates the legal and technological landscape surrounding privacy in light of new scientific and technological developments, recent policy agenda statements,

existing and envisioned legislative enactments, and judicial decisions. Initially, this article describes some recent technology used or acquired by the executive branch of the government for defensive crime and terrorism control purposes. Specifically, the research presented herein surveys some of the new scientific developments and technological tools available on the market today. The research begins with developments in biometrics and continues forth to discuss recent advances in surveillance mechanisms including audio, video (CCTV), cyber, and satellite surveillance systems; concealed weapon detectors; license plate identifiers; x-ray devices; thermal imaging equipment; and radio frequency identification tags. Next, the article focuses on statutes, policy statements, and legislative enactments pertaining to surveillance technology. Finally, the article discusses the judicial decisions that serve as a check and balance for the technology's collection, use, and dissemination of information.

Discussion

Surveillance is the backbone of law enforcement work. The ability to observe and gather timely and accurate information is the keystone to good policing. Knowledge is power, and massive amounts of information with powerful analytics that can conduct and return a search request almost instantaneously is "information that empowers."¹⁵ Technology greatly enhances surveillance capabilities. Machines have the capacity to surveil without interruption or distraction; unlike humans, surveillance technology does not need bathroom breaks, shift changes, or benefits. Machines can detect information through walls, reveal differences in biological matter, and observe objects from distances and in lighting conditions that humans cannot. Technology can discover, record, and analyze information more effectively and efficiently than most other law enforcement activities. Developments in transportation practices and systems, the banking industry, medical research and care, genetics, and communications in conjunction with computer and Internet advancements have created data dossiers on almost every person in the United States. Law enforcement personnel recognize these technological advantages and information resource centers and readily dip into the expanding treasure trove of information, and use the new developing technology, to assist in their work.

The thrust of this article stems from the fact that technology is exploding faster than either legislatures or courts can keep pace; thus, it is vital that law enforcement utilize new technology in a manner that respects basic rights of privacy and is consistent with Constitutional principles. This, of course, begs the question: Can the fox effectively guard the hen house? Or, can we really hope or expect that the executive branch will regulate itself? The founding fathers, who gave us the safeguard of checks and balances, would likely say "no."

Biometric Technology

Biometric technology is the most recent technology to capture the attention of the public, the government, and law enforcement. Biometrics is the identification or verification of an identity based on one or more intrinsic physiological or behavioral characteristics that can distinguish one person from another.¹⁶ Identification occurs when a physiological or behavioral characteristic is matched against all of the characteristics stored in a database. Verification occurs when the characteristics are authenticated. Identification is a one-to-many comparison; whereas, verification is a one-to-one comparison. The five most common examples

of biometric identification are (1) fingerprints, (2) facial recognition, (3) retina or iris scans, (4) voice recognition, and (5) DNA identification. As biometric technology continues to evolve (and more private companies and public utilities engage its use for identification purposes), growing concerns as to the misuse, tampering, and selling of biometric data (e.g., by criminals stealing, rearranging or copying the biometric data or using biometrics in unauthorized ways without the individual's express consent) will have to be addressed.

Fingerprint Optics

Fingerprints are the most common biometric system used by law enforcement agencies. The FBI itself maintains over 250,000,000 fingerprint records, and each day, it receives approximately 37,000 new records. Without biometric technology whereby each print is scanned, transformed into a template using complex algorithms, and then compared to the entire database of existing templates, a match could not be located in a timely fashion.¹⁷ The FBI's system, the Integrated Automated Fingerprint Identification System (IAFIS), provides "automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year," resulting in receipt of an electronic response within two hours and within 24 hours for civil fingerprint submissions.¹⁸

Fingerprint technology has improved considerably within recent years. Identix Incorporated, a Minnesota-based biometrics company with offices across the United States and in Australia and the United Kingdom, has created a system that through state-of-the-art optics, captures, stores, and wirelessly transmits high-quality fingerprint images to a central databank for on-the-spot identification called "live scan." This system uses a minutia-based fingerprint system. The minutia-based system analyzes the fingerprint image for endings, splits, and bifurcations in the ridge patterns. The benefit of this system is its ability to discern fingerprints over an extended period of time, regardless of some amount of dirt, moisture, or scars on the fingers themselves. The FBI's IAFIS system, which contains over 40 million records also uses these minutia-based fingerprint templates. The Identix live scan system can communicate with the FBI's expansive databank system for identification or verification.¹⁹

Fingerprint biometrics is no longer confined to law-enforcement-related activity. Thus, limitations and controls concerning its usage, storage, and dissemination may no longer be protected by Constitutional guarantees. Commercial applications for its use are being pursued in scenarios in which access control is important. For example, fingerprint biometrics is used to prevent unauthorized access to locations, workstations, personal computers, computer networks, smart cards, and the like. In 2004, IBM incorporated biometric capabilities into its ThinkPad T42 series of notebook computers. The company integrated a finger scanner directly into the PC or notebook, which controls access to the portable computer and its contents.²⁰ Furthermore, fingerprint biometrics is being used to replace keys as an entry device and to confirm identity before allowing transactions such as check cashing or banking transfers.²¹

Closely related to fingerprint technology is the growing trend toward using the biometric approach of hand geometry. Hand geometry uses the shape of the hand for authenticating a person's identity. Although individual hand features are not sufficiently unique to assure absolute verification, it is useful in less secure

settings and is easily and often combined with other biometrics like fingerprints. The technology involves using a powerful digital camera to record the hand's three-dimensional shape from silhouetted images projected within the scanner. The scanner ignores surface details such as fingerprints and disregards defects like lines, scars, and dirt, as well as fingernails, which may easily change.²² Because hand scan devices measure features like finger curves, length, thickness, distances between joints, and overall bone structure, the scan can be influenced by injury and swelling, thereby causing potential false positive matching or nonmatching.²³

For certain types of access-control situations requiring reasonably accurate, nonintrusive authentication (e.g., immigration and border control, which involve frequent international travelers, or some employer or business practices requiring entry/exit procedures for time/attendance or documentation like day care centers, athletic clubs, and maternity wards), hand geometry biometrics is the lesser intrusive (more privacy friendly) system. It is also an easier, faster, and simpler process to apply, and it provides sufficient verification for the project. Applications of hand scanning are on the rise. Hand geometry scanners verify identity at the entrances of over half of the nuclear power plants in the United States. Furthermore, the U.S. Immigration and Naturalization Service (INS) uses hand geometry scanners in its INSPASS program.²⁴ Walt Disney World uses a finger geometry scanner to control access into park entrances. Their scanner, "takes an image [of one fingertip], identifies a series of points, measures the distance between those points, and turns it into a numerical value." If the numerical value matches that of the entry pass, the guest easily and quickly gains access into the park.²⁵

Face Biometrics

Facial recognition is the method by which most identities are established. A glance at someone's facial features is all that is required to distinguish family from colleagues or strangers. Facial recognition technology uses the same methodology. Instead of the optic nerve, a computer software program analyzes the geometry of the face, measuring the distances between predefined features like the nose to the eyes, the mouth to the nose. One company has a face recognition program called Epitome.²⁶ The "epitome" of an image is its miniature, condensed version containing the essence of the textural and shape properties of the image.²⁷ The epitome is useful for such tasks as video processing and analysis, retrieval, recognition, and detection.

This technology leapt into public consciousness when it was used at the 2001 Super Bowl Game in Tampa, Florida, for security purposes; however, the technology was actually developed in the early 1990s as part of a Department of Defense initiative called the FERET program to determine the viability of using algorithms to measure faces. Early versions of the technology had been used to study crowds in casinos. Since then, it has been installed elsewhere. For example, Royal Palm Middle School in Phoenix, Arizona, installed two face recognition cameras in December 2003 for the purpose of ferreting out registered sex offenders and missing children. The cameras were linked to databases of sex offenders, missing children, and alleged abductors.²⁸ The technology has its limitations. It is not yet deemed scientifically reliable in that variables like lighting, facial expressions, weight, hair, and glasses may affect the accuracy of the equipment.

Department of Defense studies show the system is right approximately 50% of the time with outdoor lighting and 90% of the time with indoor lighting;²⁹ however, face biometrics combined with other biometric technology boosts the accuracy by significant levels. Identix has fused its face recognition system with skin biometrics³⁰ and claims that this combination of biometric techniques yields an unprecedented level of accuracy, improving face biometric technology's accuracy by at least 20% to 25%. Identix even boasts that the combination can distinguish between identical twins.³¹

Retina or Iris Scans

In 1987, after the discovery that no two individuals' irises were alike, Iridian Technologies was issued the Flom Patent, which provided the technology to identify people by their irises (the colored part of the eye surrounding the pupil).³² Since the development of the technology, iris scans are becoming more popular in a variety of settings. For example, New Egypt Elementary School in Plumsted, New Jersey, installed iris scanners and video monitors as a security measure. Preliminary findings from the Plumsted Project concluded that people reported feeling safer using this heightened security measure. The project also revealed one potential shortcoming in the project's implementation. To avoid the biometric security system, students and guests at the school engaged in "tailgating." Tailgating occurs when one person immediately follows another into the building without being subjected to an individualized iris scan.³³

Voice Prints

Alexander Graham Bell's father envisioned the idea that a person could be identified by the sound of one's voice. His idea was to create a visual representation of the spoken word based on subtle differences in pronunciation. In 1941, Bell Telephone in New Jersey produced a sound spectrograph for mapping a voice on a graph by analyzing sound waves based on frequency, intensity, and time.³⁴ The original purpose was to assist in enabling deaf people to speak. The purpose morphed during World War II when the government began using the technology to identify enemy voices on telephones and radios. Currently, the National Security Administration (NSA) uses the software to assist in electronic espionage cases.³⁵

Biometric identification using speech is particularly appealing because it is minimally intrusive. Analogous to fingerprints, one's voice can be compelled for the purpose of comparison without violating a suspect's 5th Amendment rights.³⁶ An individual's voice contains enough individually unique characteristics to distinguish it from others. In courts, the standard for admissibility of an opinion as to the identity of a speaker is merely that the identifier has heard the voice of the alleged speaker at any time.³⁷ The spectrogram assists the process by graphically displaying sound in three dimensions: (1) pitch, (2) resonating characteristics, and (3) rate of speech.

The identification process, however, suffers technological and biological difficulties. Voiceprints, unlike fingerprints, are not static. Fingerprint ridge details potentially exist from cradle to grave. The human voice, however, changes with factors such as age, stress, and health. Additionally, the process suffers when transmission quality is poor or when ambient noise is present. The accuracy of voice identification

depends upon the conditions under which the voice samplers were made, the characteristics of the equipment used, and the skill of the examiner.

DNA

DNA is a type of biometric datum in that it contains physiological characteristics to verify or determine identity. DNA can be used to accurately identify criminals when biological evidence exists, and it can exonerate persons mistakenly accused or convicted of crimes. Recently, Congress recognized the growing importance of DNA's use in the criminal justice system. On October 30, 2004, the "Justice for All Act of 2004" was created.³⁸ This Act establishes, among other things, enhanced DNA collection and analysis. Specifically, the purpose of the Act is to expand and improve the DNA testing capacity of local, state, and federal crime laboratories to eliminate substantial backlog, protect crime victims' rights, and provide post-conviction testing of DNA. Another aspect of the law that impacts privacy issues is the inclusion of funding to increase the capacity of the National DNA Index system (NDIS) of CODIS, which currently contains about 1.7 million DNA profiles, to a 50-million DNA profile database.³⁹ The increased capacity is designed to reduce the search time for matching DNA to microseconds and enable real-time searches of participating forensic laboratory databases.⁴⁰

Legal Analysis

All of the biometrics discussed above are extremely attractive to law enforcement because they provide an accurate measure of distinctiveness so that the government can identify an individual without the individual first claiming an identity (one-to-many search), provided that his or her biometric data is stored within the database. The only biometric discussed above, to date, that does not have the capacity to perform a one-to-many search is hand geometry because similarities between hands are more common.⁴¹ Hand geometry is still an attractive biometric because it is so user-friendly; it does not suffer from user failure because of smeared images or poor quality like fingerprints, and it does not require sufficient lighting like facial recognition.

As attractive as biometrics-based identification and verification systems are to law enforcement, their value and usage within the criminal justice arena is tempered by constitutional and legislative controls. Specifically, law enforcement must be mindful of privacy issues regarding the collection of biometrical data, the storage and dissemination of the data, and the ultimate use of the data as evidence in court cases. The collection of the data requires varying degrees of privacy invasions of an individual's body parts. Some, like facial recognition software, require no bodily contact; whereas, others, like retina and iris scans, require that the user come within inches of the equipment. Fingerprints require physical touching.

DNA collection and storage causes the most concern to privacy advocates particularly when samples are taken from individuals without consent. Concerns focus on . . .

the threat to the bodily integrity of citizens who are subject to the forced and nonconsensual sampling of their genetic material, the intrusion and denigration of privacy rights caused by the storage and use of tissue samples,

the potential for the future misuse of such samples held in state and privately owned laboratories, the prospect of long term bio-surveillance occasioned by the storage of genetic information in police databases and biological samples in forensic laboratories, and the possibility for the deceptive use of DNA forensic evidence in police investigations and criminal prosecutions.⁴²

Much of the DNA profile information comes from noncriminal and nonconsenting individuals like military personnel who are mandated to provide DNA samples for the purpose of identifying soldiers lost in combat.⁴³ Since these samples and DNA profile information are collected and preserved, it is possible that they may be used for purposes related to research or law enforcement for which no consent had been given at the outset⁴⁴ or that exceed the scope of a permissible search.⁴⁵ Some worry that biometric data given for an innocent purpose, such as health-related issues, will be used by the government or corporations for other, unrelated purposes like employment or insurance denial or discrimination.⁴⁶ Another concern is the potential capturing or acquiring of biometric data over the Internet or through identity theft by criminals who would then use it to defraud individuals and institutions.

Some of these issues have been addressed already. Currently, on the federal level, there are several anti-discrimination laws that prohibit some degree of genetic discrimination;⁴⁷ however, on the state level, a complex assortment of genetic discrimination laws exists. Some states have laws that protect against genetic discrimination in both employment and insurance services, and other states have no laws prohibiting genetic discrimination in either area. Regardless, weaknesses or holes exist in the current legislation that must be addressed.⁴⁸

The admission of biometric data in court procedures is not as controversial as the privacy implications in its collection and storage. The rules of evidence apply equally to hard evidence and scientific evidence. The Constitution applies to scientific searches as well as physical searches. There are, however, differences in the application of the legal principles. Chain of custody issues, retrieval practices, and scope of a search take on new meaning when applied to biometric data. Furthermore, scientific evidence may influence the criminal justice system differently or more dramatically than other evidence. Forensic biometric evidence may induce or encourage a defendant to plead guilty, may influence trial strategies,⁴⁹ and may be responsible for the push toward requiring conclusive scientific evidence corroborating guilt in capital cases.⁵⁰

A study conducted in 1988 conservatively estimated that 77,000 suspects per year in the United States become defendants on the basis of eyewitness identification.⁵¹ Interestingly though, the unreliability of eye witness identification and human testimony is becoming more well-known and well-documented.⁵² The use of biometric identification and verification techniques is one method by which the criminal justice system is responding to the problem. The use of DNA testing technology, in particular, is proving invaluable in the court's search for truth. In fact, DNA technology has proven eyewitness identification as well as other forensic sciences, long accepted by courts as scientific proof of identification in criminal cases, wrong. Specifically, DNA tests have shown that individuals convicted on the basis of expert forensic testimony on comparisons of bite marks, hairs, voiceprints, ear prints, and fingerprints were wrongly convicted.⁵³

Biometric evidence is not the panacea that the popular television show, *CSI*, would have one believe. Not all cases contain biometric evidence, and those that do depend on the technology working and the skill, qualifications, expertise, and attention to details of those who use it. For example, for a fingerprint identification to be made, data of good quality must be entered and drawn upon. For face recognition technology to work, the cameras must pan, tilt, and focus in the appropriate direction and on the specific subject under sufficient lighting. The captured forensic data must then be monitored and analyzed pursuant to acceptable procedures while a chain of custody is maintained assuring uncontaminated biometric evidence. Those applying the technology need the competence, resources, motivation, and ethical standard to use it properly. Certification of examiners and accreditation of laboratories are becoming part of the norm in terms of the qualification package for admissibility.

The court's acceptance of scientific biometric evidence varies per jurisdiction and to a certain extent, on a case-by-case basis. The seminal case discussing whether an expert may testify about novel technology that does not lie within the range of common experience that relates to an issue at trial was *Frye v. U.S.*⁵⁴ Frye, the defendant, wanted to introduce testimony from an expert as to the result of a deception test (i.e., polygraph precursor). The court refused to allow the testimony holding that an expert may testify as to his or her opinion only if the opinion is deduced from a well-recognized scientific principle or discovery that is sufficiently established to have gained general acceptance in the particular field in which it belongs. Since the systolic blood pressure test had not gained such scientific recognition, no expert testimony was allowed.

Three recent Supreme Court cases have since discussed the use of scientific testimony,⁵⁵ but the results are not entirely conclusive or unanimously controlling. In *Daubert v. Merrell Dow Pharmaceuticals*, a product liability case, the Court considered whether the "general acceptance" principle underlying scientific evidence necessary as a precondition to admissibility of expert testimony outlined in *Frye* was still appropriate in light of the new Federal Rule of Evidence, Rule 702.⁵⁶ The *Daubert* Court held that a general acceptance in the field to which the science belongs is no longer the standard precondition to admissibility. Federal Rule of Evidence 702⁵⁷ is more liberal.

The *Daubert* case set forth new guidelines for admissibility in federal court. First, the Court established the role of the judge as a gatekeeper. In that role, the judge will conduct a hearing to determine whether the methodology underlying the testimony is scientifically valid. The judge will consider such factors as whether the theory can be tested, whether the theory has been subjected to peer review or publication, the known rate of error, whether there are standards controlling maintenance of its operation, and whether the theory has acceptance within the relevant scientific community. Furthermore, the judge will determine whether the reasoning or methodology was properly applied to the facts at issue and if so, whether the testimony would assist the trier of fact to understand the evidence or to determine a fact in issue. Finally, as the gatekeeper, the judge will determine whether its prejudicial effect outweighs its probative value.

*Kumho Tire Company v. Carmichael*⁵⁸ expanded the *Daubert* holding to apply to opinion testimony of non-scientist expert witnesses. Therein, the Supreme Court unequivocally

held that in order to fulfill its gatekeeping responsibility, a court may use the factors identified in *Daubert*, if they can be appropriately utilized to determine reliability of either the underlying technique or the expert's conclusions. The gatekeeping function is flexible and by necessity must be tied to the facts of the case. The factors highlighted in *Daubert* are not a definitive list, a talisman, or a litmus test.

Although the *Daubert* decision establishes that *Frye* was superseded by the Federal Rules of Evidence, the change does not result in a universal admissibility or free-for-all for all junk or pseudoscientific assertions. In fact, in both *Daubert* and *Kumho*, the judge refused to allow the expert's testimony because there was an insufficient nexus between the scientific studies conducted and the actual issue before the court.⁵⁹ In the case of *Kumho Tire Company*, there were insufficient indications of the reliability concerning the expert's methodology of tire failure analysis.

The *Frye* standard of general acceptance still applies in 18 states including Arizona, California, Florida, Illinois, New York, Pennsylvania, and Washington.⁶⁰ Hence, population wise, *Frye* is the governing law at most state trials. Additionally, there is also no consensus on whether the introduction of novel scientific applications applies to all biometric technology. While most courts use a *Frye* or *Daubert* analysis to decide admissibility of biometric techniques, in *U.S. v. Lauder*, the court concluded that "whether an electronic fingerprinting machine generated an accurate image was not a question for a "*Daubert*" type hearing. It goes to the authentication of the image."⁶¹ Finally, even within *Frye* or *Daubert* jurisdictions, differences in opinion prevail as to whether or when certain biometric technologies like the polygraph are admissible. Despite the clear trend to exclude polygraph evidence since enactment of Military Rule of Evidence 707 (a)⁶² and the *U.S. v. Scheffer*⁶³ decision, courts still admit polygraph evidence in certain situations including rebutting a claim by a defendant that his or her confession was the result of coercion.⁶⁴ For the most part, excluding the polygraph issue, biometric evidence is admissible under the appropriate standard.⁶⁵

Other Surveillance Technology

Although it is the nature of technology to progress, technological wizardry should not obviate the Constitutional right to privacy. The government may employ scientific innovations to secure their goals; however, the use of these modern technological advancements should be strictly evaluated in light of the 4th Amendment because the advancements in science have exposed to scrutiny objects, ideas, conversations, and secrets that society once believed were protected from the observation or perception of the government. As Brandeis warned in 1928, . . .

Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court. . . .⁶⁶

Currently, the science of surveillance has progressed to the extent that an individual's activities, associations, and conversations may be intrusively monitored remotely,

unknowingly, and without any physical penetration of the traditional privacy shields. The applicable two-part inquiry of whether a person has a constitutionally protected reasonable expectation of privacy⁶⁷ is strained by the surge of advances in surveillance science. Furthermore, concepts like, “knowing exposure,” “voluntary abandonment,” “sensory-enhancement,” “location privacy,” and “the third-party doctrine,”⁶⁸ contribute to the stressed legal framework that now defines our technology-altered conception of a “reasonable expectation of privacy.”

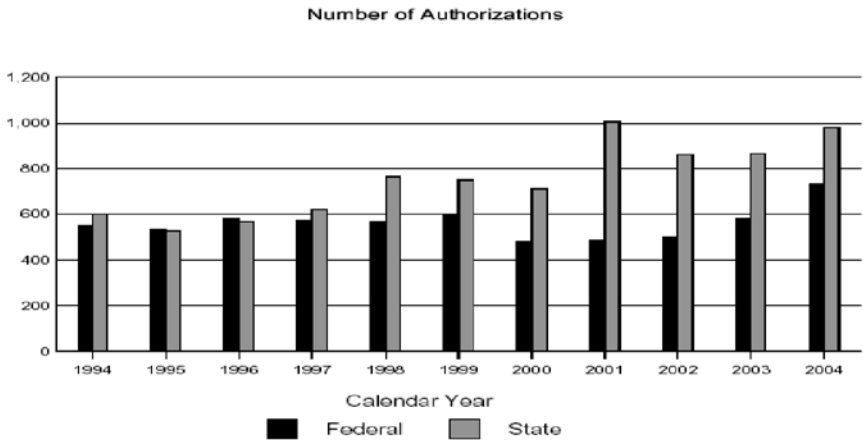
Before an intelligent discussion of the legislative and judicial limitations of scientific surveillance can be undertaken, one must first comprehend the basics of current surveillance technology. The surveillance technology to be discussed herein includes audio, electronic, and video surveillance; CCTV; surveillance drones; Radio Frequency Identification (RFID) technology; satellite tracking; black boxes; key loggers; concealed weapons detectors; thermal imaging; through-the-wall x-ray technology; and mobile license plate readers. First, each type of technology are briefly described as to its frequency of use and its capability to surveil. Then, legislative controls and judicial decisions restricting or limiting the technology’s use for law enforcement purposes are explained.

Audio and Electronic Surveillance

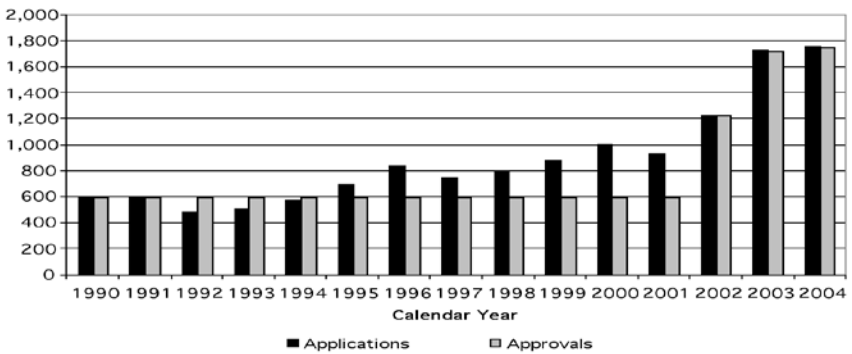
The concept of audio and electronic surveillance is not new. Oral, electronic, and wire communications have been intercepted for years.⁶⁹ Electronic surveillance is a significant tool in modern law enforcement bringing dimension to dialogues, minimizing interpretation ambiguity, and making recollection issues obsolete. When used appropriately, it has the power to bring down the most elusive of “bad guys.” There is little wiggle room for a defendant whose words are captured on tape. If used inappropriately, however, the surveillance has the power to seriously invade our privacy, stifle creativity for fear of being exposed as different, and expose our secrets to those who have no need to know. The legislature was mindful of the balance that needed to be struck between law enforcement’s need to intercept and an individual’s right to be free of unwarranted eavesdropping. Hence, the Electronic Communications Privacy Act (“ECPA”) of 1986,⁷⁰ the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”),⁷¹ the Communications Assistance for Law Enforcement Act (“CALEA”),⁷² the Foreign Intelligence Surveillance Act of 1978 (“FISA”),⁷³ and the Omnibus Crime Control and Safe Streets Act of 1968⁷⁴ (and their comparable state counterparts) were enacted to both permit and presumably limit these types of surveillances.

The extent to which audio and electronic communication surveillance occurs is reported annually to Congress through the Administrative Office of the United States Courts.⁷⁵ The 2004 report concluded that 1,710 intercepts were authorized in 2004 by state and federal courts, which amounted to an increase of 19% compared to the number in 2003. Of the 47 jurisdictions (state, federal, the District of Columbia and the Virgin Islands) that currently authorize this type of surveillance, 20 jurisdictions reported using this surveillance during 2004 as an investigative tool.⁷⁶ No wiretap applications were denied in 2006, and 2003 and 2004 were the only years that more secret surveillance warrants (FISA) were granted⁷⁷ than federal wiretap warrants, which require a more stringent legal standard.⁷⁸ The following charts summarize the rising trend in using wiretap surveillance.

State and Federal Wiretap Authorizations



FISA



New-Fangled Audio Surveillance Systems

In addition to the traditional “wiretap” or “bug” devices one typically imagines, new technology and software has been developed that can be trained to recognize and distinguish sounds that are indicators of a security breach or a safety hazard. The software is based on mathematical models that mimic the way the brain interprets sound, but it can distinguish between two similar sounds far more precisely than the human ear. For example, Chicago police implemented Safety Dynamics LLCs software to monitor certain types of criminal activity. The new audio surveillance devices are mounted on streetlight poles to listen for gunshots.⁷⁹ When gunshots resound, the devices guide surveillance cameras toward the source of the sound. The technology, formally known as Smart Sensor Enabled Neural Threat Recognition and Identification (SENTRI), uses four microphones to pinpoint the source, turns a surveillance camera toward the shooter, and places a 911 call⁸⁰ The technology used in Chicago has the capacity to recognize the sound of a gunshot within a two-block radius. Since Chicago has implemented this technology to crack down on guns and gang violence, several other cities are investigating its use as well.

A similar system designed in 2003 and 2004 called “Boomerang” is being used by troops in Iraq. This system is mounted on the back of a moving vehicle to locate hostile gunfire. The expansion of this type of audio surveillance has tremendous potential for large-scale security; conceivably an array of detectors could be placed along a deserted border to listen for specific activity. If the sensors detected specific sound indicators, the detectors could then notify a central location of any suspicious activity.⁸¹

Video Surveillance

Video surveillance cameras are ubiquitous. The use of closed circuit television (CCTV) to monitor locations around the world has exploded during the last decade.⁸² The United Kingdom (UK) leads the world in the deployment of CCTV technology. According to research studies,⁸³ the network of cameras in England is so dense (e.g., one camera for every 14 people) that in many urban areas, people may be monitored and filmed as often as 300 times per day.⁸⁴

Although the use of CCTV technology in the United States is less prevalent than in the United Kingdom, it is steadily increasing. For example, in 2002, the U.S. National Park Service installed surveillance cameras around national monuments in Washington, DC.⁸⁵ Other cities including Baltimore, Chicago, and New Orleans have installed camera surveillance networks with financing from the Department of Homeland Security.⁸⁶ Chicago, for example, added 2,250 cameras in its Homeland Security Grid.⁸⁷ These cameras are linked to a \$43-million operations center constantly monitored by police officers. Baltimore used federal grants to finance cameras and its \$1.3 million Watch Center, and New Orleans planned on deploying a 1,000-camera surveillance system by the end of 2005 as a result of federal dollars.

In October 1999, there were an estimated one million video cameras in operation in the United States for the purpose of promoting public safety and security.⁸⁸ In 1998, New York Civil Liberties Union volunteers conducted a project to produce a comprehensive map of surveillance cameras (public and private) in Manhattan. The group reported 2,397 CCTVs with only 55 cameras in use by the Department of Transportation as part of their vehicular traffic control system.⁸⁹ Minneapolis⁹⁰ and Washington, DC,⁹¹ have conducted similar projects. Although no one tracks actual numbers of surveillance cameras in the United States, the Carnegie Mellon Data Privacy Lab estimates that there are 10,000 publicly available online webcams displaying public places in the United States.⁹²

Cameras are used routinely in public and quasi-public places to deter shoplifting, prevent crime and terrorism, and record illegal acts. Persons in public venues are not the only subject for the camera. Items, activities, and events are all subject to the scrutinizing eye of video surveillance, even in seemingly remote locations. In *California v. Ciraolo*,⁹³ the Supreme Court held that an aerial observation of a home from 1,000 feet by police looking for drugs did not violate the 4th Amendment because private and commercial flights in the public airways are routine. Thus, no reasonable expectation of privacy would exist. In domestic settings within a home, CCTV usage is also legally acceptable. For instance, nanny cameras do not violate privacy rights;⁹⁴ however, the use of cameras in places where a person has a reasonable expectation of privacy, like a bathroom or bedroom, would likely violate privacy statutes or be subject to a tortious invasion of privacy claim.⁹⁵

In *United States v. Knotts*,⁹⁶ the Supreme Court found no expectation of privacy when the government attached a radio-tracking device to a canister of chemicals subsequently traced to the defendant's house. Specifically, the Court held that a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his or her movements from one place to another. Surveillance is acceptable in virtually all places where a potential for visual observation (i.e., plain view) exists.

CCTV cameras and video recordings were initially installed to deter theft and monitor traffic. Now video surveillance is routinely used to detect undesirable behavior, such as public order transgressions, and deter violence and vandalism in public parks. CCTV is becoming an integral part of a government's crime control policy and social control theory. It is promoted as the primary solution for urban dysfunction. In fact in Britain, CCTV is the single most heavily funded crime prevention measure, accounting for three-fourths of the total spending on crime prevention by their Home Office.⁹⁷ In the United States, the National Institute of Justice (NIJ) has funded research to study the effect of using CCTV cameras to monitor public spaces.⁹⁸ Furthermore, the trade organization for security professionals, ASIS International, commissioned the Carnegie Lab to assess the number and nature of webcams that observe people in public spaces. Ultimately, the goal is to analyze and propose related policies and best practices that measure the relationship between technology and privacy for the security industry.⁹⁹

With the explosive growth in video surveillance,¹⁰⁰ concerns have arisen with regard to the implications of CCTV and video surveillance effects on privacy rights and civil rights. Some governmental uses of the technology spark little controversy like CCTV usage in correctional facilities. Other venues, however, raise serious constitutional privacy concerns. Even though the effectiveness of these cameras on identifying crime and terrorism and their efficiency as a deterrent and deployment tool is still up for debate, CCTV proponents seem to be gaining support.¹⁰¹ The displacement of crime to a different location is one factor that clouds the findings of the study. The Electronic Privacy Information Center (EPIC), a watch group for privacy concerns, reports that although millions are spent on CCTV systems, studies show that they have little effect on criminal activity.¹⁰² EPIC also reports that studies show that there is a serious risk of racial discrimination with the use of camera surveillance networks. They are concerned that the Homeland Security camera systems will be misused or abused and cite several examples of such abuse from private industry.¹⁰³ With the increase in CCTV use, coupled with the new technology making them active as opposed to passive viewing vessels,¹⁰⁴ instances of abuse could grow exponentially.

The change from analog to digital devices and the ease of video enhancement for clarification purposes creates a new set of legal issues. Historically, when a convenience store surveillance camera caught a crime on video, the analog tape was seized as evidence, and the item was admitted if properly authenticated. Now, the first question raised is what must be seized as evidence: the digital recording produced off the hard drive or the hard drive itself. Each time a digital image is created in a new format, it has the potential to be altered. Thus, a new field of science known as forensic video analysis has emerged. Forensic video analysis is the scientific examination, comparison, and evaluation of video in legal matters. A lack of legal precedent and scientific authority exists within this novel field,

so the extent to which a recognized expert can clarify, enhance, reproduce, and accurately retrieve information is all relatively new and uncharted territory.¹⁰⁵

Although forensic video comparison evidence analysis is a relatively new field, the use of comparison evidence in many other scientific disciplines is widely accepted. Comparison evidence has been used in the biometric areas previously discussed herein (e.g., fingerprint analysis, DNA examination, footwear and hand print comparison, facial mapping, and ear prints). Comparison evidence is also used in tool mark identification, firearm and bullet matching, chemistry of paint matching, duct tape matching and drug samples. It is also used in questioned document, fiber, and hair examinations.¹⁰⁶ Questions as to potential tampering, best evidence (hard drive versus a digital reproduction), and the use of comparison analysis by a reverse projection image method are current concerns. Furthermore, questions related to time-lapse photography, compression, and scan conversion processes, aspect ratio to calibration, and issues concerning retrieval of digital information in remote storage (particularly, storage outside of the United States) highlight additional evolving issues.¹⁰⁷ In essence, the same types of admissibility challenges that face biometric technology and novel sciences are relevant here.

Silent video surveillance is largely ungoverned by statute. Courts have held that silent video surveillance is not covered under the ECPA.¹⁰⁸ Silent video surveillance is not an “aural transfer” because it does not involve the transfer of the human voice and therefore is not regulated under the legislation.¹⁰⁹ For the most part, there are almost no federal regulations, no state statutes covering video surveillance, and no express statutory provision for the interception of nonverbal communications. Some states, like Missouri and Washington, and the federal government, however, provide a limited restraint to video surveillance in that they have adopted statutes prohibiting the use of video surveillance for peeping or voyeurism purposes.¹¹⁰

Radio Frequency Identification (RFID) Technology

RFID is a technology that allows companies and governments to implant tiny and virtually undetectable microchips or “tags” with antennas into almost any product or animal, including humans. RFID tags are commonly used to track inventory in a fast, efficient, and cost-effective manner. The basic design consists of two main elements: (1) the RFID tag itself and (2) a scanner. The tag is a microchip with a data storage capability wired to an antenna coil that uses radio transmitted codes to uniquely identify itself. The RFID scanner is a transmitter that interacts with the microchips’ writings to modify the information on the chip.¹¹¹

The RFID tags are either passive or active. Active units contain their own power supplies and can transmit the information either continuously or on a predetermined schedule. Active units are more common and are found in such items as cell phones and aircraft transponders. Passive units are tiny and do not require an internal power source but rely on the antenna’s electrical current coming in contact with an incoming radio frequency. Even the most basic RFID tags, passive ones with no independent power source and no re-writing capability, enable the real-time tracking of an object and the individuals that carry them.¹¹²

RFIDs are basically a “first class” optical bar code like those used to scan groceries and other products¹¹³ with two critical advantages: (1) each microchip is assigned

its own unique electronic identifier (as opposed to the limited one-dimensional bar code that allows only a broad category identification) and (2) the RFID data can be read outside the line of sight and through objects like walls, within a briefcase, or in a trunk of a car if a powerful enough scanner were used. Additionally, with the use of wireless technology linked to existing Global Positioning Satellite (GPS) networks, RFID tags could be used to track any item, anywhere, and at any time.¹¹⁴ The technology is attractive due to its low price (20 to 40 cents per passive tag¹¹⁵), its passivity (not requiring an external power source), and its very small size. The small size and its placement (as well as the novelty of the technology) makes the device theoretically invisible and disablement free.¹¹⁶

The extent of usage is mind-boggling. The State Department has embedded all United States passports issued after October 2006 with RFID chips,¹¹⁷ and the Mexican government has implanted certain workers with RFID chips as a means of permitting access to restricted areas inside government buildings.¹¹⁸ Retail giants like Wal-Mart® currently endorse and utilize this technology as does Delta Airlines in tracking passenger luggage.¹¹⁹ The technology is used in the EZ-Pass system, in the medical arena, and for gas payments and security engineering.¹²⁰ RFID technology provides an enhanced means of tracking products and profiling consumers by conveying information about key areas where consumers live and work to data processing systems. Developments in RFID technology are yielding systems with larger memory capacities, wider reading ranges, and faster processing. The market for RFID tags is growing explosively and is projected to reach \$10 billion annually within the decade.¹²¹

RFID technology raises huge privacy implication issues. EPIC asserts that when RFID technology is used to track people, it breaches basic human dignity boundaries and treats people like livestock or shipment pallets.¹²² At a minimum, RFID technology impacts a person's "location privacy."¹²³ The tags have the potential to become far more invasive than the highly criticized USA PATRIOT Act provision, which allows the government to track the books people check out of the library.¹²⁴ The FBI, or the Department of Defense, or a rogue law enforcement person could use RFID technology linked with GPS networks to conduct potentially unrestrained surveillance. The surveillance could track a person's purchases against computer databases for signs of suspicious activity (like purchases of mannitol, kitchen scales, glassine bags, rubber gloves, etc. to acquire information sufficient to obtain an arrest warrant for drug manufacturing), or the surveillance could be used to simply locate or track a person's whereabouts based upon an item purchased containing an "invisible" RFID tag. The government could potentially covertly rate or score people based upon the items they have acquired containing RFID tags.¹²⁵

As of October 2006, 9 states have enacted legislation that deal with some aspects of the emerging uses of RFID technology, 6 states have pending RFID related bills, and 16 states failed to pass RFID related legislation.¹²⁶ For example, California proposed legislation to restrict state government's use of RFID tags, but that legislation failed to pass.¹²⁷ South Dakota's legislature failed to pass its bill prohibiting the implanting of the device in people,¹²⁸ Rhode Island was unsuccessful in seeking restraint from the government's use of RFID tags to track movement or identity of a person (employee,¹²⁹ student, or client) as a condition of obtaining a benefit or service,¹³⁰ and Missouri failed to pass notification legislation requiring RFID tags to be labeled so an individual is aware of their existence.¹³¹

Although no federal RFID specific legislation exists, the FCC already regulates the use of electromagnetic spectrum in RFID applications. In other words, the FCC places limits on the power and spectrum allocation of RFID readers, which in turn limits the read range of a particular tag. The FCC's limitation power or control, however, has already been reduced for the Department of Homeland Security (DHS) so that it can improve the effectiveness of scanning shipping containers when they reach U.S. ports.¹³²

United States Visitor and Immigrant Status Indicator Technology (US-VISIT)

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is the DHS system to "keep America's doors open and our nation secure." The system requires visitors to the United States to submit a biometric (fingerprint and photograph) identifier to the government. The biometric information is then checked against 20 interfacing government databases to determine the likelihood that the visitor is a criminal or terrorist. Currently, US-VISIT entry procedures are operating at 115 airports, 15 seaports, and 50 secondary ports of entry and 12 airport and 2 seaports as exit procedures. The system planned to be fully functional at every entry point by December 31, 2005.¹³³

The US-VISIT system uses RFID technology combined with biometric technology and as of September 2005, the program has processed 30 million visitors and stopped 700 potential entrants who were either arrested or deported.¹³⁴ Critics of the system say that the RFID and biometric technology employed includes more information than is necessary for its purpose of preventing terrorism.¹³⁵ EPIC's report of January 2005 complains that of the more than 16.9 million visitors to the United States that have been processed by US-VISIT screening, 372 individuals have been identified for crimes or immigration violations. None have been caught as wanted terrorists.¹³⁶ The government claims that EPIC reads the program's goals too narrowly and believes US-VISIT goals are to enhance the security of American citizens, permanent residents and visitors; facilitate legitimate travel and trade; ensure the integrity of the immigration system; and safeguard the personal privacy of visitors.¹³⁷

Satellite Tracking

All states monitor activities of convicted sexual offenders and require that they register within the jurisdiction wherein they reside;¹³⁸ now, however, monitoring of offenders has escalated to a new level. Across the United States, satellite tracking is being used to monitor the movements and whereabouts of convicted sex offenders.¹³⁹ Global positioning systems are monitoring these individuals. The sophisticated systems can create exclusion¹⁴⁰ and inclusion zones that alert law enforcement officers and other individuals if a sex offender has entered a prohibited zone or is where he or she should be.

Sex offenders are not the only individuals being considered for monitoring through satellite surveillance. In Charleston, South Carolina, global positioning satellite monitoring is one of the suggested solutions for jail overcrowding, with home detection bracelets as another. Home detention requires regular call-in contact, as that system lacks real-time tracking. The new satellite technology offers several advantages. The system would alert officers if an inmate went into a restricted area.

South Carolina advocates believe the GPS technology will be valuable beyond the mere tracking of offenders and keeping the community safer. The technology will also assist in eliminating the monitored felons as suspects in new crimes.¹⁴¹ Crime specific monitoring, such as discussed for sexual predators, and category offenders like felony prisoners, makes other per se monitoring easier. Once you go down the slippery path, the easier it is to continue to monitor other per se crimes or offenders.¹⁴²

The Legal Constraint on Wire, Electronic, and Oral Surveillance

Electronic surveillance, whether it be by audio, video, RFID, or satellite technology, is a powerful yet ominous tool in modern law enforcement's arsenal of weapons. Hence, several statutes were enacted to control or limit its usage. The primary statutes are the Omnibus Safe Streets and Crime Control Act of 1968, the Electronic Communication Privacy Act (ECPA) of 1986 ("Title III")¹⁴³ and the Foreign Intelligence Surveillance Act (FISA).¹⁴⁴ Most audio (wire and oral) and electronic surveillance is governed by these statutes.

The ECPA is subdivided into three subtitles¹⁴⁵ and covers three specific types of communications: (1) wire, (2) oral, and (3) electronic. A wire communication involves aural transfers, which are communications containing the human voice that travel through a wire or cable device at some point during their transmission. A landline or mobile telephone conversation that is intercepted in real time is an example of this type of communication. An oral communication is a communication uttered by a person under circumstances such that the person has a reasonable expectation that the communication will not be overheard. In other words, the communicator must have a reasonable expectation of privacy in his or her conversation, and it must be one that society is willing to protect. This definition applies to communications intercepted through bugs or other recording devices like tape recorders that do not involve a wire transmission. Finally, electronic communications are all non-wire and non-oral communications (i.e., signals, images, and data that are transmitted through a medium such as wire, radio, electromagnetic; and photo-electronic). The prime examples of electronic communications are an e-mail message, a fax, a page, or a text message.

Historically, wiretap laws required the consent of all parties before a communication could be intercepted. Now, federal law and 35 states allow for the interception of wire communications if only one of the parties to the communication has given prior consent. Even then, however, the situations for interception vary significantly from jurisdiction to jurisdiction.¹⁴⁶ Furthermore, the ECPA requires law enforcement to obtain a court order with an accompanying affidavit based on an extensive laundry list of legal requirements¹⁴⁷ before capturing the content of a communication. The list is extensive because wiretap surveillance poses greater threats to privacy than the physical searches and seizures covered by the 4th Amendment. Interception of communications inherently captures some communications of non-targets regardless of whether the communication is relevant to the investigation. Additionally, not every communication of a criminal suspect (target) is criminal in nature, and unlike the typical search warrant for which officers announce, enter, search, and exit, electronic surveillance is conducted surreptitiously and continues in an ongoing fashion until the goals and objectives of the investigation are met. At times, the monitoring continues for months and involves thousands of communications.

All electronic surveillance statutes require the issuing judge to review the affidavit to determine whether normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or are too dangerous. To satisfy this requirement (commonly referred to as the exhaustion/necessity requirement), the affidavit cannot be merely a boilerplate recitation of the difficulties of gathering usable evidence.¹⁴⁸ The affidavit must include a “full and complete” statement providing detailed information about all prior interceptions on the named interceptees and the facility or device to be intercepted. It also must include all pertinent information relevant to the investigation, including possibly exculpatory information. There is, however, some discretion to disclose the evidence in less than entirety to establish probable cause provided there is no effort to mislead the court in approving a warrant that might otherwise not have been issued.¹⁴⁹ For example, it has been held acceptable for the government to withhold information to protect the confidentiality of informants.

The ECPA also requires that the interception of oral communications through wiretapping must be conducted in such a way as to minimize the interception of communications not otherwise subject to interception. Interception is proper only as long as it is necessary to achieve the goals of the authorization. This does not require that all innocent or nonrelated communications remain unmonitored. Rather, the statute requires that unnecessary intrusions upon the privacy of the individuals being lawfully monitored should be minimized to the greatest extent possible. Minimization is satisfied if, on the whole, the agents have shown a high regard for the rights of privacy and have done all they reasonably could to avoid unnecessary intrusion.¹⁵⁰

The wiretap statute contains its own exclusionary rule that provides no intercepted communications, wire or oral, can be received in evidence if the communications were unlawfully intercepted, the order was insufficient, or the interception was not made in conformity with the order.¹⁵¹ Due to this clear legislative intent to limit surveillance to protect privacy issues and control law enforcement surveillance, a substantial compliance standard is mandated by most courts for each provision of the statute that is deemed to be a central or functional safeguard factor.¹⁵² In short, only surveillances that are narrowly focused with constitutionally acceptable preapproved judicial blessings based on special showings of need are permissible.

Foreign Intelligence Surveillance Act (FISA)

In 1978, the Foreign Intelligence Surveillance Act (FISA) was passed. Its purpose was to provide a statutory structure to govern electronic and physical surveillance (e.g., wiretapping, pen registers, and physical searches) in national security cases when foreign intelligence information is sought.¹⁵³ This act authorizes the government to carry out electronic surveillance in the United States upon obtaining a judicial order from a special panel of judges designated by the Chief Justice based upon a probable cause finding that the target is a foreign power or an agent of a foreign power.¹⁵⁴ FISA was intended to be used primarily in foreign intelligence and counter-intelligence cases in which threats to national security were of prime importance; therefore, the act does not have the same lengthy laundry list of requirements and restrictions as does the ECPA.

FISA does not contain the EPCA provision requiring notification to each target or aggrieved person (interceptee) within 90 days after the electronic surveillance has been terminated.¹⁵⁵ FISA does not require probable cause because FISA deals with “special needs” such as terrorism and espionage threats directed by foreign powers. Thus, the act focuses on dealing with extraordinary crimes as distinguished from ordinary crime control.¹⁵⁶ In fact, for individuals who are not U.S. citizens or permanent resident aliens, the statute does not even require probable cause to believe that the target is engaged in criminal conduct. It is enough that the target is an agent of a foreign power.¹⁵⁷ For U.S. citizens, the statute allows surveillance when there is probable cause to believe that the person is engaged in clandestine intelligence activities on behalf of a foreign power, which “. . . involve or *may involve* a violation of the criminal statutes of the United States.”

One of the primary concerns of critics is that virtually all FISA applications are approved, and the numbers are steadily increasing at an alarming rate.¹⁵⁸ Furthermore, although little is specifically known about these investigations, the complaint is that FISA has been used increasingly in criminal cases for which it was not designed.¹⁵⁹ The government does this by claiming that it is conducting parallel intelligence and criminal investigations and proceeds under the new FISA standards that the person is engaged in clandestine intelligence activities on behalf of a foreign power, which “. . . activities involve or *may involve* a violation of the criminal statutes of the United States.”

Passive Sensory-Enhanced Surveillance Technology

Passive sensory-enhanced surveillance technology allows law enforcement personnel to collect information enhancing the officer’s senses without physical intrusion and often without the suspect’s knowledge. Typically, the device passively measures emissions, such as visible light, infrared radar, radio waves, heat, sound, smell, etc., from the target. The most basic such passive sensory-enhanced surveillance techniques and technologies include flashlights, tracking devices, binoculars, and startrons,¹⁶⁰ and to a certain degree, canine sniffs.¹⁶¹ More recent technology includes concealed weapons detectors, x-ray devices,¹⁶² mobile license plate detectors, and thermal imaging technology.

Concealed Weapons Detectors

Several companies have developed concealed weapons detectors. One company brags about its development of an ultrasound sensor that can remotely detect and image concealed weapons on a human body from ranges up to 8 meters.¹⁶² Another company touts that by using its millimeter wave technology and a camera system, concealed weapons can be detected and identified under a person’s clothing regardless of whether the weapon is metal, plastic, or composite in real-time outputs from a range of up to 45 feet in distance.¹⁶³ An Ohio developer has patented a sensor that could be used to detect concealed weapons or help pilots see better through rain and fog by technology that measures how brightly the objects reflect the natural radiation in the environment. The theory behind the technology is that every object (e.g., the human body, a gun, a knife, or an asphalt runway) reflects a certain amount of ambient radiation. This sensor just illuminates the radiation through a camera system revealing the items in an x-ray type relief image. This technology claims as a benefit that it can scan people or luggage without subjecting

them to X-rays or other radiation and “if the sensor were embedded in an airplane nose, it might help pilots see a runway during bad weather.”¹⁶⁴

X-Ray Technology

Since the September 2001 attacks, enormous amounts of money and effort have been invested in updating the U.S. government’s people screening and transportation security measures from 1960s era magnetometers and CAT scan equipment to state-of-the-art technology.¹⁶⁵ Currently, the Transportation Security Administration (TSA) is field testing a noninvasive x-ray system known as a backscatter portal¹⁶⁶ that can see items hidden on a person’s body, concealed in vehicles, or secretly stashed in cargo containers. The system’s signals interact with explosives, plastics, and metals, revealing their shape and form thereby making them easy to visually identify.

The backscatter technology works by measuring the solar radiation reflected by persons or objects under scrutiny. The system is sensitive enough to discover metal objects, plastic explosives and weapons, non-metallic handguns, and drugs. In vehicle inspections, the driver briefly exits while the screening van slowly passes by the target screening for contraband. When a person is screened, the individual steps into the refrigerator-sized machine, and the technology performs a virtual strip search, which provides inspectors with a clear view of what is underneath the person’s clothes—skin or weapons.¹⁶⁷ The more remote inspections system may also be used to screen persons. In that scenario, the system scans the moving individual for contraband. If detected, the system, which is linked to a closed-circuit television camera system with object-tracking capabilities, will automatically pick out and follow the suspect until he or she can be stopped and questioned. Whether the technology is used to screen a vehicle or a person, the process takes less than a minute and claims to be physically harmless; however, the signal strength of detected backscattered x-rays allows such a highly realistic image of the human form to be reconstructed, it potentially causes emotional or privacy damages.¹⁶⁸

The devices are currently used by U.S. Customs agents at 12 airports to reduce the long queue, reduce security threats posed by vehicles containing explosives, and screen drug carrying suspects. Backscatter technology is also used at London’s Heathrow Airport,¹⁶⁹ and since the July 2005 bombing, the system is also employed in London’s underground subway tube.¹⁷⁰ Furthermore, the backscatter technology is being used as part of the Secure Automobile Inspection Lanes (SAIL) test project to conduct explosives screening on automobiles boarding the Cape May-Lewes Ferry in Cape May, New Jersey; the Golden Gate Ferry in San Francisco, California; and several other designated locations.¹⁷¹ Despite the privacy implications, many governments worldwide are highly interested in this aviation security technology,¹⁷² including TSA.¹⁷³

Mobile License Plate Readers

“Deny the Road to Criminals” is G2 Tactics, Inc.’s mantra for promoting their mobile license plate recognition technology. The product called GLAVID or Plate Finder uses an infrared camera with a high-powered processor to read the license plate and compare it to specific databases in real time. The technology allows an officer to read license plates (60 times per second) while mobile or stationary,

in daylight or at night. The equipment can be operated to cover a single lane or multiple lanes of traffic and operates on its own without an external trigger.

The impact to law enforcement of this technology is far reaching. The system checks all plates against a specially created “vehicle of interest” database.¹⁷⁴ This database may include state or federal (NCIC) databases for stolen autos or plates, as well as any other database, including outstanding parking or traffic fines. Auto theft recovery and identification, an important law enforcement task, is just one of its potential uses. With links to other databases, the equipment could assist with AMBER alerts, outstanding warrants, terrorist lists, library fines, etc. The benefit of the system is that the device does not racially profile. The negative aspect again relates to the automatic accessibility of private information to others. The device is rapidly gaining popularity among law enforcement agencies.¹⁷⁵

Thermal Sensors

A thermal imaging device, often called a FLIR (forward-looking infrared radar), is used to detect activity and movement via heat patterns on the surface of a selected target by identifying temperature differentials. The device provides a visual image of objects that are warmer or cooler than the baseline. A thermal imager is capable of locating a human in the dark from a distance in excess of 7 kilometers. Although thermal imaging devices are incapable of seeing through an object, activity or hot spots may be detected if heat from the activity passes through an intermediate object like a window or a porous wall.¹⁷⁶

Thermal imagers are a prized commodity¹⁷⁷ and have been applied in a variety of circumstances. The U.S. Border Patrol uses the device for military surveillance and detection of illegal immigrants. FLIRs have been used to save persons trapped in smoke ridden buildings as well as many other search-and-rescue operations. The imager has assisted in locating countless individuals including missing children, lost Alzheimer’s patients, fleeing suspects, and escaped convicts. The devices are used in drug cases to locate hydroponics laboratories. As a result of the refined sensibility of the equipment, the devices have been used recently to detect and identify fugitive gas emissions and hazardous air pollutants that are harmful to the environment.¹⁷⁸

The usefulness of the technology cannot be denied. These devices allow law enforcement to collect otherwise unavailable information passively without a physical intrusion. Thus, for the most part, the suspect has no knowledge that the equipment has been used. Because thermal imagers operate by observing and recording waste heat radiated through the surface of a structure, concerns were raised that 4th Amendment privacy protection would be analogized to a garbage search inquiry approved by the Supreme Court in 1988 in *California v. Greenwood*.¹⁷⁹ The concern centered on the collection of private information without notice as well as the acquisition of confidential data in areas where privacy is highly protected like within a residence. Although the FLIR technology supposedly cannot penetrate walls, it actually does to a certain extent. Without adequate control, this infrared technology could allow the government to search and surveil inviolate of the right to privacy.

The issue is temporarily resolved by the 2001 Supreme Court decision in *Kyllo v. United States*.¹⁸⁰ In *Kyllo*, the litigants debated whether the information retrieved from the search was recovered through the wall, as abandoned property, or discovered in view from the exterior of the home's walls. The Court, however, sidestepped that debate and focused its decision instead on how the thermal imager was used under the *Katz*¹⁸¹ two-pronged test. First, did the person have an actual subjective expectation of privacy? Second, was that expectation one that society was prepared to recognize as reasonable? The Court concluded that *Kyllo* did have a subjective expectation of privacy in the heat emissions within his home since the technology had the potential of revealing more than the contraband hydroponics marijuana growing operation. Protected information, such as when the lady of the house was bathing, could also be revealed. Furthermore, the subjective privacy expectation was one that society would be willing to recognize. This latter conclusion was reached on the basis that thermal imagers are not devices commonly available to the general public. Hence, the interiors of houses are off limits to any technology, no matter how unobtrusive the technology may be, provided that the technology is not in general use. This decision offers minimal or temporary protection to privacy advocates, as new technology is a continuing phenomenon and more and more of the technology is being made available to the general public.

Policies

Brandeis' version of privacy, the right to be secluded from the observation or company of others (i.e., "right to be let alone") seems abandoned in light of the information captured, gleaned, analyzed, and disseminated by the use of the technological breakthroughs mentioned above. The government believes that these domestic surveillance activities or techniques are justified under the guise of national security (i.e., protection of citizens from crime, cyber or otherwise, and from street punks and dealers) and terrorism. To that end, the government has made significant use of the technology available. The formulation, development, and use of new technologies and strategies has been formally part of the government's agenda since the creation of the Advanced Research Projects Agency (ARPA), by Public Law 85-325 and Department of Defense Directive 5105.41 in February 1958. Its creation was directly attributed to the Soviet's Sputnik project and its implicit threat to national security. Although ARPA has been renamed DARPA (Defense Advanced Research Projects Agency), it still functions as the facilitator for developing and implementing programs to address national security needs. Its accomplishments and mission "to leverage ingenuity and research to develop transformational technologies that give our armed forces a decisive edge" are vast and impressive.¹⁸²

Despite the noble goal stated in its mission statement, some of DARPA's recent technology-based projects have received major criticism from privacy activists. In 2002, one project, Combat Zones that See (CTS) was heavily attacked. The Combat Zones That See Project was developed for use in combat zones and utilized the technology involved with smart CCTVs with event detection, object tracking, and notification systems.¹⁸³ Its obvious and intended purpose was to identify and track enemy combatants. Privacy advocates feared its exploitation and deployment on civilian populations. The potential for creating a big brother surveillance state was perceived so highly likely that the project was eventually scrapped in 2003.

Checks and Balances: Legislative Controls

As a result of the significant privacy concerns generated by the use of the new technology and other governmental programs and the awareness raised by privacy groups like EPIC, the Department of Defense formed the Technology and Privacy Advisory Committee (TAPAC) to address these concerns. TAPAC's 2004 report¹⁸⁴ concluded that statutory and regulatory frameworks were needed to regulate collecting and disseminating data on individuals. Currently, the Privacy Act of 1974¹⁸⁵ and to a certain extent, the E Government Act of 2002¹⁸⁶ are the primary limitations on the collection and disclosure of this type of information. Other legislative enactments such as ECPA,¹⁸⁷ the USA PATRIOT ACT,¹⁸⁸ CALEA,¹⁸⁹ and FISA¹⁹⁰ address some of the other privacy surveillance issues discussed herein, but all of them are woefully outdated, strained beyond recognition, or fundamentally inadequate when it comes to the new technology.

Checks and Balances: Judicial Review

So far, the research has discussed some of the new technologies; certain new governmental policies and practices; and to a lesser extent some of the major legislation that exists to oversee these activities. It is now time to review the judiciary's spin (check and balance) on these executive decisions and legislative mandates. This spin will have to envelop the world as it exists today including all the changes, events, and beliefs that have occurred and control the American people of today. The ever-evolving advancements in communication and surveillance technology have fundamentally altered the way individuals conduct their affairs. People no longer live in brick or wood homes; they now reside in cyberspace or virtual homes. They do not just exist as flesh and blood mammals; they exist as bits of biometric materials. Their private papers and effects are no longer confined to physical documents; they are bytes of electronically stored information forming blocks of ones and zeroes stored on some remote computer. Communications and activities are no longer geographically bound. Information is available to everyone almost anywhere within a nanosecond. Despite all this, the core belief, as espoused by Brandeis, to be left alone, still stands. It is the judiciary's task to strike the proper balance between an individual's privacy and law enforcement's need to know.

As the judiciary needs a real case in controversy to act, the judicial reviewing process is by design, mostly reactionary and tends to be somewhat piecemeal. There are, however, certain basic principles that act as guidance concerning the constitutionality and legality of the use of new technology by the government (e.g., the concepts of location privacy, public/third party disclosure, and cognition enhancement).

Location privacy is defined as an individual's freedom from having his or her movements monitored without consent. Currently, the concept is not incorporated into the 4th Amendment. Neither is it protected by the ECPA or by any other explicit legislation. In fact, the ECPA specifically exempted technology that by "[an] electronic or mechanical device" tracks the movement of a person or object.¹⁹¹ The rationale behind this exclusion stems from the fact that Congress sought primarily to protect contents of communications as opposed to non-content material. By using a postal mail analogy, only the letter was protected; the envelope or the physical means by which the content arrives is not protected.

The results of a no location privacy mentality are far reaching in light of today's technology and are under considerable pressure to change. The early decisions are easy to reconcile with the rule. No location privacy existed outside of a home because whatever a person did outside of the home was done in the public's view. Thus, one had no reasonable expectation that actions, conducted in public, would be private. For instance in 1983, the Supreme Court found that the government's attaching a radio-tracking device to a canister in an automobile to track the defendant did not violate the Fourth Amendment because, "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."¹⁹² The rule allowing no location privacy branched off or combined with the knowing exposure rule. The knowing exposure rule essentially states that when one knowingly exposes information to others (third persons), one cannot then claim a reasonable expectation of privacy in that information.

These decisions led the way to the conclusion that electronic surveillance is acceptable in virtually all places where a potential for visual observation exists, including aerial observation of a home from 1,000 feet by police looking for drugs.¹⁹³ The natural progression next led to the acceptability of certain enhancement technology to better expose that which is in the public's view, like flashlights and high-powered, high-resolution cameras.¹⁹⁴ Satellite tracking is the next potential expansion, and its acceptability is a potential for concern. In the Dow Chemical Company case, the court commented that a line might be drawn in the sand for satellite tracking. "[S]urveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."¹⁹⁵ To date, however, more and more states are moving toward the use of satellite tracking, particularly in the areas of sexual offenders and border patrol monitoring. So the line may have been moved.

RFID technology took this lack of location privacy and knowing exposure doctrine to a new dimension. RFID tags are now a household item. They are implanted in cellular phones, automobiles, items of merchandise at Wal-Mart®, luggage tags by Delta Airlines, tickets at Disney World, E-Z passes and governmental and private identification cards. RFID tags turn regular items into tracking devices. Last year, the Court of Appeals for the 6th Circuit found that the DEA's use of the device to transform the suspect's cell phone into a tracking device was acceptable and not unreasonable or in violation of either the 4th Amendment or the ECPA.¹⁹⁶ In October 2005, two courts, one in Texas and one in New York, found that the tracking of locations of cell phones without showing probable cause that a crime occurred or was in progress violates the right to privacy. Those courts found that cell phones are tracking devices, and even if they are, a showing more than the fact that the information is relevant to an ongoing investigation is needed.¹⁹⁷ As these differences in holdings indicate, the courts are having difficulty reconciling and interpreting location privacy with the new technology.

Video cameras are also a common piece of surveillance equipment used in public arenas. Red light cameras, motion-sensing video recorders, object tracking, and cyber bugs are watching with their unblinking eyes. Silent video surveillance is not covered under the Electronic Communications and Privacy Act or under the 4th Amendment. The 4th Amendment is not invoked because the surveillance

is occurring in a public area or in an area where no reasonable expectation of privacy exists. The ECPA is inapplicable because, video does not involve an “aural transfer,” the transfer of the human voice.¹⁹⁸

The concept of privacy from tracking devices and video cameras is not without some control. Location privacy is sometimes recognized within the zone of privacy in one’s home. It appears that here, in one’s castle, the 4th Amendment would require a warrant. A warrant is required to monitor a tracking device in a private home because it is withdrawn from public view.¹⁹⁹ The Supreme Court found that the monitoring of a beeper within a home was the functional equivalent of an entry to determine whether the container was there, and thus a warrant was necessary to ensure that the use of beepers was not abused and that agents demonstrated in advance their justification for the desired search.²⁰⁰

Location privacy also exists to the extent that certain physically invasive inspections are more intrusive than other purely visual inspections.²⁰¹ Although visual surveillance is lawful, a continuous surveillance by a video camera on a power pole to record the activities in a suspect’s backyard was too intrusive a search; thus, it required 4th Amendment protection.²⁰² Perhaps this was the concept that the Texas and New York courts were attempting to protect²⁰³ when they declared a cell phone not to be a tracking device, or if it is, maybe it is a continuous surveillance worthy of protection.

Location privacy also exists when “peeking technology” is used to look inside a home when the view is not exposed. For example, in *Kyllo v. U.S.*, the Supreme Court held that the insides of the house are off limits to any technology, no matter how “unobtrusive” the technology may be, provided, however, that the technology used is not in general use. Thus, the use of thermal imagers (devices not generally available to the public) to measure the amount of heat emanating within a home (clearly an unobtrusive surveillance) was forbidden.²⁰⁴ The *Kyllo* decision raises questions as to what ultimate result will prevail concerning RFID technology. RFID technology, unlike thermal imagers, is in general use and is fairly unobtrusive; however, the technology does reveal both legal and illegal activity. As the *Kyllo* court reiterated, however, the expectation of privacy is linked to prevailing social conventions and the commonplace nature of the technology involved. Thus, the proliferation of RFID technology and the post-911 shift in social attitudes about privacy will have to be factored into the decision.

The concern here is that everything that now contains an RFID tag (and everything that does not) is potentially a tracking device. Most people are unaware, due to the size of the device, and the recent advancements in technology, that this super bar code has the capacity to track their movements. The passive tags are reactivated when they come into contact with a scanner. Although the technology today for most RFID tags requires that the object be within a few feet of the scanner, that obstacle will soon be overcome. Satellite tracking of sexual offenders is a clear indication of the trend for the future.

The only piece of legislation that remotely acknowledges location privacy is the Communications Assistance for Law Enforcement Act (CALEA).²⁰⁵ CALEA was designed to ensure that the new technology developed by telephone companies would not impede law enforcement’s ability to intercept communications. CALEA

was intended to preserve the status quo of the FBI's surveillance capabilities, not to expand them. The goals of CALEA were to require telephone companies to design or make their existing networks compatible to law enforcement's electronic surveillance needs, so that law enforcement could intercept call content and call identifying information as needed and as specifically authorized. In other words, the carriers had to make all the information available to the FBI, but the information had to be made available in individual pieces (e.g., pen register information, call content information, call location information, etc, so that the information could be dispensed depending on the particularized need in the order.²⁰⁶

CALEA was also responsible for ensuring that telecommunication carriers developed the software that allowed the Emergency 911 to operate, thereby allowing the tracking of cell-phone users at all times.²⁰⁷ Although this information is readily available in 911 situations, CALEA is mandated to protect the privacy and security of communications not authorized to be intercepted. Thus, call location information is not to be provided routinely without proper legal authority. CALEA was designed so that first, the common carriers and the private technology creators would be allowed to develop their own mechanisms for implementation of the act. If the private companies failed to make their equipment surveillance savvy, then the Federal Communications Commission (FCC) would intervene to develop an appropriate standard. Thus, the interpretation and enforcement of the statute was delegated to the FCC. The FCC has since then interpreted CALEA to require telecommunications carriers to provide call-identifying, including cell site information to all law enforcement agencies.²⁰⁸ The FCC has already allowed the DOD to extend the scanning power for RFID chips. As a result, privacy advocates argue that FCC was threatening civil liberties by giving the federal government new tools for surveillance.

*Katz v. United States*²⁰⁹ was a landmark decision that addressed technological invasions into areas in which a reasonable expectation of privacy exists and one that society is willing to protect. In *Katz*, law enforcement agents obtained evidence of a gambling operation by bugging and recording conversations of a bookie from outside of a public phone booth. The Court rejected the long standing rule that a trespass to a traditional zone of privacy (like the home or the person) was needed to violate expectations of privacy that society was willing to recognize as reasonable. The technologically savvy Court held that "the fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."²¹⁰ The new expectation of privacy requires that a person exhibits an actual (subjective) expectation of privacy and, that the expectation is one that society is prepared to recognize as "reasonable."

Although the *Katz* decision was a tremendous victory for privacy advocates, its impact has been largely limited to content versus non-content material like the bookie's conversation therein. Envelope or non-content materials do not get the same extension to the zone of privacy protections. For example, pen register devices, which capture addressing materials, not content, are outside the scope of the 4th Amendment.²¹¹ Cell site location data is somewhere in the middle of content and non-content material. Privacy advocates consider it content material because it is not specifically included in the list of information accessible by subpoena under the Stored Communications Act (SCA) provisions.²¹² Law enforcement argues that cell site information is merely a tracking device; therefore, it is clearly

non-content information. Furthermore, this information is typically collected by the cellular companies as part of their basic business records. Companies do not collect content information as part of their regular business practice.²¹³

Likewise, the *Katz* decision did not afford 4th Amendment protection from the government's recovery of information from third parties,²¹⁴ or information that is knowingly exposed even from great distances by aerial surveillance.²¹⁵ Account information in banks,²¹⁶ telephone companies,²¹⁷ and Western Union²¹⁸ has been declared by the courts to be unprotected material because the customer voluntarily conveyed the information to the company and "exposed" that information to its equipment or personnel in the ordinary course of business. In so doing, (the customer) assumed the risk that the company would reveal the information to police or others.²¹⁹

The burgeoning acceptance of this "knowing exposure to third parties" practice exception to 4th Amendment protection has been promoted wholeheartedly by the Bush administration. Under the USA PATRIOT Act, the FBI can issue National Security Letters, which allow for the disclosure of personal records about ordinary Americans without getting approval from a prosecutor, grand jury, or judge. Simply by issuing the letter, the FBI can direct companies, libraries, banking institutions, financial entities, Internet service providers, universities, and other institutions to turn over customer records. Once disclosed to the government, the records are then scrutinized and deposited into government data banks, allowing access for "state, local, and tribal governments and for appropriate private sector entities."²²⁰ These national security letters are used routinely to seek information that is "relevant to an investigation to protect against international terrorism or clandestine intelligence activities." No longer are specific and articulable reasons needed to justify the gathering of the information. In fact, the FBI now issues more than 30,000 national security letters per year without any check or balance from an impartial authority.²²¹ The dramatic increase in the letter's usage is a direct result of the Justice Department's new guidelines, which provide that the FBI should consider (not require) less intrusive means and should not hesitate to use any lawful techniques even if intrusive when investigators believe them to be more timely, particularly in investigations relating to terrorist activities.²²² A few organizations have challenged the constitutionality of a national security letter, and the outcome is currently up on appeal in the United States Court of Appeals for the Second Circuit; however, the lower court did find the letters violative of the 1st and 4th Amendments under the theory that "democracy abhors undue secrecy."²²³

Internet Service Providers (ISPs) are also considered to be third parties that hold and process a user's information on the user's behalf; thus, the 4th Amendment provides little to no protection of information revealed to ISPs. With little constitutional protection, Internet surveillance restrictions must come from statutes. The ECPA's Wiretap Act protects if a communication is being transmitted from its origin to a destination; the SCA applies if the communication is stored electronically with a computer service provider. Only the Wiretap Act, with its inclusive exclusionary rule, offers real privacy protection to third parties. The SCA subjects the information to disclosure, with a minimum showing requirement that the information will be relevant to a law enforcement investigation.

To invoke the Wiretap Act and thereby obtain its protection, the information sought must fit precisely within the definition. For example, when the Secret Service seized a computer from a company that produced role-playing games and collected e-mail information held within the computer, the Wiretap Act did not apply. Since the e-mails were temporarily housed or stored within the computer, they were not intercepted "in transit."²²⁴ The same holding applied to the use of keylogger devices. When the FBI used its keylogger system to record the defendant's keystrokes on his computer to ascertain his password, there was no interception because the keylogger did not record keystrokes while the defendant's modem was operating. Thus, the keystrokes were not intercepted in transit, and the Wiretap Act did not apply.²²⁵

The advent of e-mail has created an interesting quagmire in communication privacy. The ECPA was created as a protection from unwarranted surveillance of communications. The content of the communication was the focus of the protection. Content at the time was of an evanescent nature. If one did not capture the words when spoken, they would be gone forever. E-mail changed that. Contents of communications are captured, both read and unread, for a period of time. Even when deleted, they are not really gone. The Wiretap Act offers little protection to the content of these communications; all that is needed is to wait for a mere instant, beyond its "in-transit stage," and one can capture the same information in a stored capacity without all the privacy protection rigmarole. Fortunately, some courts have not bought into the third party disclosure rule with regard to e-mails and believe that what the ECPA does not protect, the 4th Amendment does.²²⁶

Sensory Enhanced Surveillance

Closely related to the cognition enhancement concept is the concept of sensory enhanced surveillance. This type of surveillance extends the natural sensory perception of individuals beyond normal ranges. Sensory enhancement is employed when flashlights, binoculars, telescopes, CCTVs with or without object tracking, thermal imagers, biometric devices, K-9s,²²⁷ electronic surveillance audio devices,²²⁸ x-ray, tracking devices,²²⁹ etc. are used. Most of these devices use passive, non-intrusive, non-trespass methods to engage in surveillance, but regardless, the technology allows the detective to search in areas beyond his or her physical potential. The *Kyllo* decision provides the only real guidance concerning this issue;²³⁰ however, as described above, this decision offers minimal protection to privacy advocates because new technology is a continuing phenomenon, and more and more of the technology is being made available to the general public. Take computers and Internet access or cell camera phones as an example. A few years ago, few people possessed them; now they are commonplace items.

Conclusion

As technology continues to develop, the burden will be on law enforcement officials to convince courts that the new device or the new technological program does not threaten individual privacy and that its use complies with fundamental 4th Amendment principles and existing statutory mandates. As evidenced by many of the examples discussed herein, today's technology is evolving faster than either the legislature or the courts can predict; thus, it is imperative that the executive

branch, including law enforcement, control their own conduct and guard their own hen houses.

James Madison, the author of the 4th Amendment captured the heart of this issue when he wrote the following:

But what is government itself but the greatest of all reflections on human nature? If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controuls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to controul the governed; and in the next place, oblige it to controul itself. Who will watch the watchers?²³¹

Madison's solution to controlling government power was to separate the power of the government into different branches so they could check each other. In recent times, however, the speed with which technology is advancing and the immediate application of these devices by law enforcement (the executive branch) has tilted this system of checks and balances. The concern is that the implementation of new technology and resources by law enforcement has not been adequately subjected to any checks by the judicial or legislative branches. Law enforcement must, therefore, be responsible and carefully monitor and control its own behavior.

There is substantial evidence cited herein that the protections initially established by the Constitution and the statutory enactments are stretched beyond recognition or are not working as intended. It is increasingly apparent that Brandeis' concept of a balanced government to protect our fundamental rights, including the right to privacy, has been severely challenged by the invasion of the new technology. The executive branch's lack of self control, the legislature's diluted or inadequate regulations, and the judiciary's creative twisting and bending of historical principles coupled with slowness in embracing a virtual world is of serious concern to privacy proponents.

As the technology continues to develop and improve and as society demands more and more protection from the executive branch, the concepts of privacy will most certainly be redefined. The right to be left alone will be difficult to maintain. Even with strict legislative controls, ever watchful privacy groups, and a demanding judiciary, the executive branch will push the envelope. It will be the task of the legislative and judicial branches to keep the executive branch in check.

Endnotes

¹ "Where the invisible become visible" was Seisint's description for its Multi-State Anti-Terrorism Information Exchange (MATRIX) system. Seemingly insignificant data analyzed against billions of data bits will make the invisible, visible.

² Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5).

³ *Olmstead v. United States*, 277 U.S. 438, 474 (1928), J. Brandeis dissenting.

- ⁴ Privacy International. (2004). PHR2004 – Overview of privacy. Available online at [www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-82589](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589)
- ⁵ Bentham, J. (1969). *Panopticon papers: A Bentham reader* (pp. 194-208). In M. P. Mack (Ed.). New York: Pegasus.
- ⁶ Foucault, M. (1972). *The archeology of knowledge & the discourse on language*. New York: Pantheon Books.
- ⁷ In *Griswold v. Connecticut*, 381 U.S. 479, 484, the Court, *citing* Lord Camden in *Entick v. Carrington*, 19 How. St. Tr. 1029 said, “Specific guarantees in the Bill of Rights have penumbras formed by emanations from those guarantees that help give them life and substance . . . affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man’s home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.”
- ⁸ In *Whalen v. Roe*, 429 U.S. 589, 605-06 (1977), the Supreme Court acknowledged the “threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures . . .”
- ⁹ Many commercial websites utilize “cookies” to gather personal information from visitors. This collected information is then distributed or sold to third parties (companies and the government) for marketing or profiling purposes. Seisint sells its proprietary repository of billions of public records to the government. (See *Seisint Delivers Advanced Investigative Tool for Law Enforcement* at www.accurint.com/news/news_5_18_2004.html). The government also sells its databases to private companies. The state-operated MATRIX program was sold to Lexis/Nexis for \$775 million in July 2004 (See www.billingsgazette.com/index.php?id=1&display=rednews/2004/07/16/build/business/54-lexis-nexis.inc).
- ¹⁰ ChoicePoint’s March 2005 leak resulted in 750 known cases of identity fraud. Additionally, in February 2005, the Bank of America reported that it lost 1.2 million customer records (See http://news.com.com/ChoicePoint+Were+sorry+for+data+leak/2100-1029_3-5618515.html and http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=nl). These leaks influenced U.S. Senator Feinstein (CA) to propose a bill (S-751) that would require federal agencies and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information.
- ¹¹ The Electronic Privacy and Information Center (EPIC), a watchdog for privacy groups, filed a lawsuit against the Transportation Security Administration (TSA) for TSA’s criteria

for putting people on lists (No Fly and Selectee) that bar some passengers from flying and subject others to extensive scrutiny (See www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html).

- ¹² Privacy Act of 1974, 5 U.S.C. § 552a, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801-6809; the Fair Credit Reporting Act (15 U.S.C. §1681); Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501-06; etc.
- ¹³ For example, in July 2004, RFID legislation seeking to set privacy standards for the technology in California was defeated by the Committee on Business and Professions (See www.rfidjournal.com/article/articleview/1015/1/1).
- ¹⁴ The Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227 and the Federal Trade Commission (FTC) established a national Do-Not-Call Registry. The registry is nationwide in scope, applies to all telemarketers (with the exception of certain nonprofits), and covers both interstate and intrastate calls. (See www.fcc.gov/cgb/donotcall/#relatedrules).
- ¹⁵ See www.equifax.com
- ¹⁶ <http://search.msn.com/results.aspx?q=biometric+definition&FORM=SSRE>; Danielyan, E., Danielyan Consulting LLP. The lures of biometrics. *The Internet Protocol Journal*, 7(1). Available online at www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-1/lures_of_biometrics.html
- ¹⁷ See www.peoplekey.com.au/biometrics_tutor/law.htm
- ¹⁸ IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects. The fingerprints and corresponding criminal history information are submitted voluntarily by local, state, and federal law enforcement agencies (See www.fbi.gov/hq/cjisd/iafis.htm).
- ¹⁹ See www.11id.com/index.php?option=com_content&task=view&id=208&Itemid=216
- ²⁰ Shor, S. (2004, October 5). IBM integrates biometrics into ThinkPad. *Tech News World*. Available online at www.technewsworld.com/story/IBM-Intergrates-Biometrics-into-ThinkPad-37100.html
- ²¹ See www.jackwe.com/sagem.htm
- ²² Jain, A. K. (1998, November). A prototype hand geometry-based verification system: MSU-CPS-98-31.
- ²³ See www.biometricsinfo.org/handgeometry.htm
- ²⁴ INS Passenger Accelerated Service System (INSPASS) is an automated system created to reduce immigration inspection processing time for authorized travelers by combining automation with a hand geometry biometric image to validate the claimed identity of an individual (See www.biometrics.org/REPORTS/INSPASS2.html).
- ²⁵ Disney claims they do not store the entire fingerprint image, but only numerical information about certain points. Harmel, K. (2006, September). Walt Disney World: The government’s

tomorrowland? Available online at http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments

²⁶ See <http://research.microsoft.com/~jojic/epitome.htm>

²⁷ See <http://research.microsoft.com/~jojic/epitome.htm>

²⁸ See www.usatoday.com/news/nation/2003-12-12-facial-scans_x.htm

²⁹ NSIT, DARPA, & DOD. (2003). Face recognition vendor test. Summary. Available online at www.itl.nist.gov/iad/894.03/face/face.html#FRVT2002

³⁰ The surface of the skin is as unique a characteristic of an individual as one's fingerprints. By using a common, household digital camera, the dermal surface of the skin can be classified and imaged in an automated manner using an algorithm called Surface Texture Analysis. "The surface texture of the skin is analyzed for random features, and a skin template is extracted," which can then be viewed on its own or fused with other biometric systems like fingerprints or facial recognition applications (See www.identix.com/trends/skin.html).

³¹ See www.11id.com/index.php?option=com_content&task=view&id=208&Itemid=216

³² See www.businessweek.com/technology/content/jul2005/tc2005075_4115_tc119.htm

³³ The National Law Enforcement and Corrections Technology Center System. (2004, Summer). *Tech Beat*.

³⁴ Ramsland, K. (2005, December 9). The origin of voiceprints. Available online at www.crimelibrary.com/criminal_mind/forensics/voiceprints/

³⁵ Stokes, J. (2005, December 20). The new technology at the root of the NSA wiretap scandal. Available online at <http://arstechnica.com/news.ars/post/20051220-5808.html>; Deputy Director for National Intelligence Michael Hayden reports that the voice/word recognition software provides new opportunities to intercept overseas calls that pass through U.S. switches. The trigger is a phrase included on a watch list or a call with an abnormally high volume of a certain type of vocabulary. Hayden defends the software stating it is only used on international calls, and the period of interception, in most cases, is far less than that which would be gained by getting a court order. NSA's usage of the software has been analogized to Echelon, another government-run, high-volume, automated intelligence-gathering project that looks for certain words or phrases in samples of electronic communications.

³⁶ *United States v. Wade*, 388 U.S. 218, 222-23 (1967). The privilege against self-incrimination protects an accused person only from being compelled to testify against him- or herself or otherwise provide the state with evidence of a testimonial or communicative nature. Submitting to fingerprinting, photography, or measurements; writing or speaking for identification; appearing in court; standing, assuming a stance, walking, or making a particular gesture do not become testimonial activities within the scope of the privilege against self-incrimination because activities such as these, including the use of one's voice involve only identifying a physical characteristic, not to speak his or her guilt. Furthermore,

in this case, compelling Wade to speak within hearing distance of the witnesses and even to utter words purportedly uttered by the robber, was not of a “testimonial” nature.

³⁷ United States v. McMillan, 508 F.2d 101 105 (8th Cir. 1974) cert. denied, 421 U.S. 916 (1975) quoting from United States v. Rizzo, 492 F.2d 443 (2d Cir.), cert. denied, 417 U.S. 944, (1974), which held, “The standard for the admissibility of an opinion as to the identity of a speaker is merely that the identifier has heard the voice of the alleged speaker at any time.”

³⁸ H.R.5107 Justice for All Act of 2004; Public Law 108-405.

³⁹ In December 2004, the ACLU of Northern California filed a lawsuit to challenge the government’s seizure of DNA samples from people who were never convicted of any crime (See <http://aclunc.org/pressrel/041207-dna.html>). New Jersey ACLU also filed a lawsuit in January 2004 challenging the collection of juveniles’ DNA (See www.aclu-nj.org/pressroom/aclufileslawsuitchallengein.htm).

⁴⁰ See www.dna.gov/info/solve

⁴¹ Signature/handwriting analysis and keystroke analysis are other examples of biometric technology that look at behavioral characteristics that contain patterns of unique characteristics such that verification (one-to-one authentications), not necessarily identifications can be made. Signature/handwriting verification correlates how a user signs his or her name, the pressure he or she asserts, the strokes and patterns of the lines, the speed, and the order of strokes used to create the document. Keystroke analysis assesses the typing style of the user including speed, pressure, error rate, and timing of the keystrokes. The keystroke recognition technology then compares the user’s typing pattern against the pattern contained in the database template.

⁴² Williams, R., & Johnson, P. (2005, Fall). Inclusiveness, effectiveness and intrusiveness: Issues in the developing uses of DNA profiling in support of criminal investigations. *Journal of Law, Medicine, and Ethics*, 33, 545.

⁴³ Mayfield v. Dalton, 901 F.Supp. 300 (D. Haw. 1995), vacated as moot, 109 F.3d 1423 (9th Cir. 1997) (Mandatory collection of DNA from military service members did not violate the 4th Amendment protection against unreasonable searches and seizures.)

⁴⁴ See <http://aclunc.org/pressrel/041207-dna.html>; <http://www.epic.org/privacy/genetic>

⁴⁵ Since general searches are impermissible, the extent and nature of the information revealed through certain biometric technologies may violate the 4th Amendment. A warrantless toxicological testing that exceeded the scope of the prior authorized private search “by employing chemical or mechanical means to reveal the hidden nature” violated the Fourth Amendment. *State v. Von Bulow*, 475 A.2d 995, 1018 (R.I. 1984).

⁴⁶ Szekely, P. (2002, May 8). Burlington Northern Santa Fe Corp. Railroad to pay \$2.2 million in DNA test case: Illegally testing workers for genetic defects. Reuters. Available online at www.mindfully.org/GE/GE4/Railroad-Workers-Genetic-Defects8may02.htm

⁴⁷ Americans with Disabilities Act, 42 U.S.C. §§12111-117 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in sections

of 26 U.S.C., 29 U.S.C., and 42 U.S.C.); and Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e (2000); and Executive Order 13145 codified at 3 C.F.R. 235 (2001), reprinted in 42 U.S.C.A. §2000e-1b (West, 2003) (prohibits discrimination in employment based on genetic information; however, it applies only to federal employees.)

- ⁴⁸ The Americans with Disabilities Act bars employment discrimination against people who currently have an injury or disease but can still do the job, but people carrying genes making the disease or injury potential in the future may not be not protected from discrimination by employers or insurers because they are not currently disabled.
- ⁴⁹ In cases in which DNA evidence or fingerprints are recovered, some criminal defendants may alter their defense from not guilty to consensual activities defense or allege that the evidence was planted by law enforcement.
- ⁵⁰ Darehshori, S., Kirchmeir, J. L., Quinn Brady, C., & Mandery, E. (2006, March 4). Empire state injustice: Based upon a decade of new information, a preliminary evaluation of how New York's death penalty system fails to meet standards for accuracy and fairness. *Cardozo Public Law, Policy & Ethics Journal*, 85.
- ⁵¹ Wells, G. L., Small, M., Penrod, S., Malpass, R. S., Fulero, S. M., & Brima Combe, C. A. E. (1998). Eyewitness identification procedures: Recommendations for lineups and photospreads. *Law and Human Behavior*, 603, 609.
- ⁵² The U.S. Department of Justice found that mistaken eyewitness identification was a factor in 85% of the 28 cases studied (See U.S. Department of Justice. (1996). *Convicted by juries, exonerated by science: Case studies in the use of DNA evidence to establish innocence after trial*, 15-17]. Another study found that mistaken eyewitness identification was present in 86% of the first 60 DNA exonerations in the United States [See Scheck, B., Neufeld, P., & Dwyer, J. (2000). *Actual innocence: Five days to execution, and other dispatches from the wrongly convicted*. New York: Doubleday.]. A Huff study found that mistaken eyewitness identification occurred in 60% of the 500 wrongful convictions studied. A Borchard study found that eyewitness error occurred in 45% of 65 cases of wrongful conviction, and a Rattner study found that eyewitness error occurred in 52% percent of the 205 wrongful convictions studied. Gross, S. R., Jacoby, K., Matheson, D., Montgomery, N., & Patil, S. (2005). Exonerations in the United States: 1989 through 2003. *The Journal of Criminal Law & Criminology*, 95(2), 523. Northwestern University, School of Law. Available online at www.law.umich.edu/newsandinfo/exonerations-in-us.pdf
- ⁵³ The Innocence Project (See www.innocenceproject.org).
- ⁵⁴ *Frye v. U.S.*, 54 App. D.C. 46 (1923).
- ⁵⁵ *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, (1993); *General Electric Company v. Joiner*, 522 U.S. 136, 1997); and *Kumho Tire Company v. Carmichael*, 526 U.S. 137 (1998).
- ⁵⁶ Jan. 2, 1975, P.L. 93-595, § 1, 88 Stat. 1937.
- ⁵⁷ Rule 702. Testimony by experts if scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient

facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

⁵⁸ *Supra*.

⁵⁹ In *Daubert, supra*, the court ruled that since no prior study had found Bendectin to be a human teratogen or substance capable of causing malformation in fetuses, the expert testimony would not assist the jury and should be excluded pursuant to the court's gatekeeping function.

⁶⁰ See e.g., *Grady v. Frito-Lay, Inc.*, 839 A.2d 1038, 1044-45 (Pa. 2003); *Logerquist v. McVey*, 1 P.3d 113, 124-34 (Ariz. 2000); *Hadden v. State*, 690 So. 2d 573, 577 (Fla. 1997); *People v. Leahy*, 882 P.2d 321, 324-31 (Cal. 1994); *People v. Basler*, 740 N.E.2d 1 (Ill. 2000).

⁶¹ *U.S. v. Lauder*, 409 F.3d 1254 (CA10 NM 2005).

⁶² Military Rule of Evidence, Rule 707 (a) "Notwithstanding any other provision of law, the results of a polygraph examination, the opinion of a polygraph examiner, or any reference to an offer to take, failure to take, or taking of a polygraph examination, shall not be admitted into evidence." Executive Order 12,767 (July 1, 1991, President George Bush).

⁶³ *U.S. v. Scheffer*, #523 U.S. 303 (1998). The Court stated, "There is simply no consensus that polygraph evidence is reliable. To this day, the scientific community remains extremely polarized about the reliability of polygraph techniques. We cannot conclude that the control question polygraph has been generally accepted within the scientific community." Furthermore, preserving the jury's core function of making credibility determinations will permit the court to limit a defendant's right to present evidence and will save the court time.

⁶⁴ *U.S. v. Kampiles*, 609 F.2d 1233 (7th Cir. 1979).

⁶⁵ Although there is disagreement within the scientific community on the accuracy of voice verification authentication, voiceprint technology has advanced to the degree that several circuit courts now allow comparisons of the spectrogram of an unidentified speaker with that of an identified speaker in order to find similar patterns as admissible scientific evidence (See www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00258). See *United States v. Smith*, 869 F.2d 348, 351-53 (7th Cir. 1989) citing *United States v. Williams*, 583 F.2d 1194, 1198-1201 (2d Cir. 1978), *cert. denied*, 439 U.S. 1117, (1979); *United States v. Baller*, 519 F.2d 463, 465-67 (4th Cir.), *cert. denied*, 423 U.S. 1019, (1975); *United States v. Franks*, 511 F.2d 25, 32-34 (6th Cir.), *cert. denied*, 422 U.S. 1042, (1975).

⁶⁶ See *Olmstead supra*, at 473, 474-79 (Brandeis, J., dissenting).

⁶⁷ *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). First, does the individual have a reasonable subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as objectively reasonable?

⁶⁸ Each of these concepts will be discussed more fully in the judicial section of this article.

⁶⁹ *Olmstead, supra*.

- ⁷⁰ Pub. L. No. 99-508, 100 Stat. 1848. 18 U.S.C. 2510(12) (2004) (codified as amended in scattered sections of 18 U.S.C.).
- ⁷¹ USA PATRIOT Act of 2001, Pub. L. No. 107-56, 215, 115 Stat. 272, 287, 50 U.S.C. 1861-1862 (2004).
- ⁷² 47 U.S.C. 1002-121
- ⁷³ 50 U.S.C. 1801-1811
- ⁷⁴ 18 U.S.C. Chapter 19
- ⁷⁵ Specifically, the Omnibus Crime Control and Safe Streets Act of 1968 requires that certain information, including the number and nature of state and federal applications for orders authorizing or approving the interception of wire, oral, or electronic communications, the offenses under investigation, the location of the intercept, the cost of the surveillance, and the number of arrests, trials, and convictions that were a direct result of such surveillance, be reported annually.
- ⁷⁶ Administrative Office of the United States Courts. (2004). Wiretap report. Available online at www.uscourts.gov/wiretap04/contents.html
- ⁷⁷ FISA surveillance results are required to be submitted annually to the United States Department of Justice, Office of Legislative Affairs. FISA warrants do not require the same degree of court supervision or notice requirements as do ECPA wiretap orders. The discrepancies in the numbers between applications sought and applications approved are accountable to the reviewing court's denial of the application, the withdrawal of the application, or the fact that the application was submitted in a prior year and approved the following year.
- ⁷⁸ Electronic surveillance at an all-time high. (April 29, 2005). Available online at www.epic.org/privacy/wiretap
- ⁷⁹ SENTRI is programmed to recognize only gunshots, not record conversations or bug private homes. The system in Chicago has no "mechanism for other sounds like human voices" (See www.usatoday.com/travel/2005-07-05-electroniccrime_x.htm).
- ⁸⁰ "System sensors detect stimuli based on intelligent neural-based rules to pinpoint the location of the stimuli, pan the camera to the stimuli location, send the alarm (audible and visual) to the Control Center, send real-time images and audio to the Control Center, and activate the system strobe light or beacon" (See www.usatoday.com/travel/2005-07-05-electroniccrime_x.htm and <http://govtsecurity.com/mag/listen>).
- ⁸¹ The technology was created to monitor and recognize a sound signature using multiple points and patterns of reference such as security breaching noises like gun shots, chain link fences being cut, and human voices in unauthorized areas. Currently, it can recognize sound signatures as short as a gunshot or as long and varied as a diesel truck.
- ⁸² See e.g., NYCLU Surveillance Camera Project 2397 cameras in Manhattan at www.nyclu.org/surveillance.html or the Minneapolis Surveillance Camera Project at [120](http://www.mpls-</p></div><div data-bbox=)

watched.org; See also, <http://privacy.cs.cmu.edu/dataprivacy/projects/camwatch/index.html>

- ⁸³ McCahill, M., & Norris, C. (2003, June). Working paper No. 6, CCTV in London: On the threshold to urban panopticon? Analyzing the employment of CCTV in European cities and assessing its social and political impacts. Available online at www.urbaneye.net/results/ue_wp6.pdf
- ⁸⁴ Electronic Privacy Information Center (EPIC). (2005, March). Observing surveillance project. Available online at www.observingsurveillance.org
- ⁸⁵ Fahrenthold, D. A. (2002, July 3). Cameras to oversee festivities for Fourth. *Washington Post*, A1; Hsu, S. S. (2002, April 10). D.C. police offer rules for video surveillance. *Washington Post*, B1.
- ⁸⁶ EPIC. (2005, May). Spotlight on surveillance, more cities deploy camera surveillance systems with federal grant money. Available online at www.epic.org/privacy/surveillance/spotlight/0505.html
- ⁸⁷ Chicago's cameras were financed by a \$5.1 million grant from DHS.
- ⁸⁸ Security Industry Association (SIA) and International Association of Chiefs of Police (IACP) Informational Brief for Guideline Closed Circuit Television (CCTV) for Public Safety and Community Policing (Revision Number 7; 10/31/99). (See www.workplace-security-got-sued.com/CCTV.htm).
- ⁸⁹ NYCLU Surveillance Camera Project. (1998). Available online at www.mediaeater.com/cameras/overview.html
- ⁹⁰ Minneapolis Surveillance Camera Project (See www.mpls-watched.org).
- ⁹¹ EPIC. (2005, March). Observing surveillance project. Available online at www.observingsurveillance.org
- ⁹² Carnegie Mellon Data Privacy Lab. (2003, Fall). Surveillance of surveillances. Available online at <http://privacy.cs.cmu.edu/dataprivacy/projects/camwatch/index.html>
- ⁹³ *California v. Ciraolo*, 476 U.S. 207, 215 (1986).
- ⁹⁴ *State v. Diaz* 706 A.2d 264, 268 (N.J. Super. Ct. App. Div. 1998).
- ⁹⁵ *Miller v. Brooks*, 123 N.C. App. 20 (1996).
- ⁹⁶ *United States v. Knotts*, 460 U.S. 276 (1983).
- ⁹⁷ Welsh, B. C., & Farrington, D. P. (2002). *Home Office Research Study 252, Crime prevention effects of closed circuit television: A systematic review*. Available online at www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf
- ⁹⁸ CCTV: Constant cameras track violators. (2002). *NIJ Journal*, 249. Available online at www.ncjrs.org/pdffiles1/jr000249d.pdf

- ⁹⁹ Carnegie Mellon Data Privacy Lab. (2003, Fall). Surveillance of surveillances. Available online at <http://privacy.cs.cmu.edu/dataprivacy/projects/camwatch/index.html>
- ¹⁰⁰ The government, private citizens, and businesses are utilizing CCTV technology to protect themselves, monitor specific activities, or send images via their mobile camera phones. Cell phone camera popularity reportedly grew from just under 9 million shipped to the United States during 2003 to 27 million in 2004 and is estimated to reach 100 million in 2008. (See www.pcworld.com/news/article/0,aid,117035,00.asp).
- ¹⁰¹ The United States General Accounting Office's Report to the Chairman, Committee on Government Reform, House of Representatives. (2003, June). Video surveillance information on law enforcement's use of closed circuit television to monitor selected federal property in Washington, DC. Available online at www.gao.gov/atext/d03748.txt; see also, A review of current research into the effectiveness of CCTV systems in reducing crime. (2002, June 28) (hereinafter "NACRO Study"). Available online at www.epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf
- ¹⁰² NACRO Study. (2002, June 28). Available online at www.epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf
- ¹⁰³ Examples include when the manager of a Florida newspaper improperly extended a legitimate surveillance camera system to include a hidden camera in the employee bathroom; when a JC Penney employee discovered that a guard was showing videotape in which he zoomed in on a woman's breasts using the store's ceiling cameras; and when B-grade filmmakers raided footage from public video cameras to make risqué movies featuring unsuspecting persons. Pompano, A. J. (2005). Privacy in the age of video surveillance: This is not your father's candid camera. Yale-New Haven Teachers Institute. Available online at www.yale.edu/ynhti/curriculum/units/2000/3/00.03.05.x.html#f
- ¹⁰⁴ Now cameras can be remotely controlled by police to pan, tilt, and zoom in on specific persons, activities, or items. Cameras also have night vision capabilities and wireless technologies. A full range of viewing, recording, and storage connections can be integrated with the cameras. Digital video recorders developed for use with CCTV surveillance systems have hard drive capacities to store up to 10 weeks of recordings with retrieval and video content analysis. Other technological advancements include conversion from analog to digital, development of smart cameras with event detection, and notification for networked video systems. Object tracking, another new innovation, enables a viewer to follow a subject from camera to camera in order to monitor the target of interest even with movement through the field of view. There are also advances in imaging with reduction of field pattern noises, remote streaming video recording, and viewing capability from hand held devices. Cyber Bug, a three-pound pilot-less aircraft surveillance drone operated by remote control, sends streaming video to officers on the ground. Although the use due to cost (\$8,500 each), additional training, and variable weather conditions pose challenges, the machines would be beneficial for monitoring risky situations like low flights over wooded areas to look for missing persons or to investigate a chemical or biological attack. [See Partlow, J. (2005, June 28). High-as-the-sky tech at drone show. *Washington Post*, p. 85. Available online at www.washingtonpost.com/wp-dyn/content/article/2005/06/27/AR2005062701643.html]. The Coast Guard is developing similar drones that can be vertically launched and provide 16 continuous hours of surveillance. Other improvements include wireless connectivity and access through the Internet, cost reductions, outdoor automatic day/night adjusting cameras, and tapeless systems that

allow storage capacities in excess of one million gigabytes (see www.surveillance-source.com/CCTV_Surveillance_System.htm).

- ¹⁰⁵ Forensic video analysis is the scientific examination, comparison, and evaluation of video in legal matters per the Law Enforcement and Emergency Services Video Association (LEVA). Hak, J. W. (2005, October 6-7). *The legal basis for forensic video comparison evidence. Video and the law: A practitioner's guide to admissibility*. LEVA 2005 Training and Development Conference.
- ¹⁰⁶ The technical basis for all comparison evidence requires the identification and analysis of (1) a class characteristic (an identifiable feature that assists in narrowing down the statistical probability that a person or object belongs to the same group as a known person or object that shares the same features) and (2) a unique characteristic (identifiable features found on a specific person or object that is found on no other person or object of a similar class.) For example, a forensic video analysis of car headlight spread can be performed since all cars display unique headlight patterns.
- ¹⁰⁷ Hak, J. W. (2005, October 6-7). The legal basis for forensic video comparison evidence. LEVA 2005 Training and Development Conference. *Video and the law: A practitioner's guide to admissibility*.
- ¹⁰⁸ United States v. Koyomejian, 970 F.2d 536, 540 (9th Cir. 1992).
- ¹⁰⁹ See e.g., United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 540 (9th Cir. 1992); United States v. Biasuci, 786 F.2d 504, 508 (2d Cir. 1986).
- ¹¹⁰ Mo. Rev. Stat. § 565.253; Wash. Rev. Code § 9A-44-115; Video Voyeurism Prevention Act of 2003, 18 U.S.C. § 1801 et seq. (See www.theorator.com/bills108/hr24.html). The bill makes it a crime "to capture an improper image of an individual" if the perpetrator "knowingly does so under circumstances violating the privacy of that individual" (See www.pcworld.com/news/article/0,aid,117035,00.asp).
- ¹¹¹ See www.aimglobal.org/technologies/rfid/what_is_rfid.asp
- ¹¹² Predicted by MIT researchers to become the most pervasive computer technology in history, most RFID tags do not require any external power source and can transmit information via radio waves when the tag enters the reception field of the nearest scanner (See www.ftc.gov/bcp/workshops/rfid).
- ¹¹³ Optical bar-code technology is currently used in five billion scans per day. RFID technology may replace and surpass this limited technology.
- ¹¹⁴ Cisco Systems has already designed a system that can track RFID tags to a few meters and display the location on a central map. While the current range of the scanners is limited to two to five feet on passive tags, this range could be greatly increased by developing more powerful and sophisticated scanners. Thus, RFID tags never die. They are merely dormant until a scanner awakens them.
- ¹¹⁵ The cost of a passive read-only tag has been steadily decreasing and ranges about 20 to 40 cents each (See www.rfidjournal.com/article/articleview.1098/1/1/).

- ¹¹⁶ Cell phones may be turned off or ESNs may be exchanged. GPS devices can be deactivated. Passive RFID chips, however, cannot be turned off.
- ¹¹⁷ The State Department has required Radio Frequency Identification chips on all American passports issued after October 2006 (See www.washingtontechnology.com/news/1_1/daily_news/27294-1.html).
- ¹¹⁸ Gardner, W. D. (2004, July). RFID chips implanted in Mexican law-enforcement workers. Available online at www.techweb.com/wire/story/TWB20040715S0001
- ¹¹⁹ Retail giants drive RFID deployment. (2005, June). Available online at www.eweek.com/article2/0,1895,1490912,00.asp
- ¹²⁰ Tucson, Arizona, jail uses Smart Band® RFID wristbands for prisoner identification and officer access (See www.ti.com/rfid/docs/news/eNews/enewsvol23.htm#var).
- ¹²¹ See www.epic.org/privacy/rfid
- ¹²² See www.epic.org/privacy/rfid/children.html
- ¹²³ *Location privacy* is defined as the freedom of an individual from having his or her movements monitored without consent. This concept will be discussed at length in the judicial restraint section of this article.
- ¹²⁴ USA PATRIOT Act of 2001, Pub. L. No. 107-56, 215, 115 Stat. 272, 287, 50 U.S.C. 1861-1862 (2004) (allows the FBI to compel production of library circulation records as a part of its business records).
- ¹²⁵ This technique is similar to the “terrorist quotient” score developed for airline security under the MATRIX and CAPPS II programs.
- ¹²⁶ American Legislative Exchange Council. RFID State Legislative Activity, October 2006. (See <http://downloads.heartland.org/20144.pdf>; www.contactlessnews.com/library/2005/11/01/a-number-of-state-legislatures-consider-rfidrelated-issues).
- ¹²⁷ A California bill introduced in February (SB 682) would prohibit public entities from issuing RFID identity documents, such as library cards, that can broadcast personal information. Identity Information Protection Act of 2005.
- ¹²⁸ South Dakota H.B. 1114 (See www.contactlessnews.com/library/2005/11/01/a-number-of-state-legislatures-consider-rfidrelated-issues).
- ¹²⁹ An in-depth look by the RAND Corporation (Santa Monica, CA; 310-451-7002; www.rand.org) at six corporate uses of RFID found that records from RFID access control systems typically link with personnel records, often integrate with CCTV systems, and occasionally link to medical records [See Balkovich, E., Bikson, T. K., & Bitko, G. (2005, January). *9 to 5: Do you know if your boss knows where you are? Case studies of radio frequency identification usage in the workplace*. Santa Monica, CA: RAND.].
- ¹³⁰ Rhode Island H-5929 (See www.contactlessnews.com/library/2005/11/01/a-number-of-state-legislatures-consider-rfidrelated-issues).

- ¹³¹ Missouri SB 128 (See www.contactlessnews.com/library/2005/11/01/a-number-of-state-legislatures-consider-rfidrelated-issues).
- ¹³² Victory, J., Lewis, M., Dombrowsky, Jr., T. S., & Hike, C. M. (2005, August). Homeland security and communications: A compendium of federal programs, FCC section. Woley, Rein & Fielding, LLP. Available online at www.wrf.com/docs/publications/12285.pdf
- ¹³³ See www.millermayer.com/resources/usvisit.html
- ¹³⁴ Bischoff, G. (2005, September 1). U.S. border crossings go high tech. See http://mrtmag.com/mag/radio_us_border_crossings/
- ¹³⁵ The information collected from the individuals subjected to this search include complete name; date of birth; gender; country of citizenship; passport number and country of issuance; country of residence; travel document type (e.g., Visa) number; date and country of issuance; complete U.S. address; arrival and departure information; and for the first time, a photograph and fingerprints (See www.epic.org/privacy/us-visit_pia.pdf, US-VISIT Program Increment and Privacy Impact Assessment, December 13, 2003). Concerning the complaint that the RFID tag contains more biometric information than is necessary or required by the program, the government's response is that the complaint is unfounded. The passive RFID tags used for the program only have a read range of about 3 inches; however, critics contend that RFID technology is currently evolving and the range of the passive reading will improve (See www.eweek.com/article2/0,1895,1746423,00.asp, Defense Department Tests Hybrid Active/Passive RFID, Jacqueline Emigh, December 30, 2004).
- ¹³⁶ Another complaint from EPIC is that US-VISIT did not substantially comply with the E-Government Act of 2002, which requires federal agencies to conduct privacy impact assessments before developing and purchasing new technologies that will collect personal information electronically. The purpose of the act is to ensure that privacy considerations are built into the technology in the planning stages. DHS did release a privacy impact assessment for the program's biometric technology, but they did so just days before the technology was deployed at the airports and ports, thereby providing insufficient time to review the privacy impact before implementation (See www.epic.org/privacy/us-visit).
- ¹³⁷ US-VISIT program increment and privacy impact assessment. (2003, December 13). Available online at www.epic.org/privacy/us-visit_pia.pdf
- ¹³⁸ The U.S. Congress passed three laws that require states to monitor child offenders: (1) the Wetterling Registration Act, (42 USC § 14071), (2) the Lynchner Tracking and Identification Act and (3) Megan's Law. On March 5, 2003, the Supreme Court ruled that information about registered child offenders may be posted on the Internet. Megan's Law mandates that a county be notified of child offenders residing there and residents must have access to that information (See www.registeredoffenderslist.org/megans-law.htm?engine=overture!3510&keyword=megans+law).
- ¹³⁹ The State of Florida now mandates the tracking of convicted sexual offenders who have committed "lewd and lascivious" acts against a child. The act, entitled the Jessica Lunsford Act took effect in September 2005 and requires those who molest children younger than 12 to wear satellite offender tracking devices for life once they leave prison (See www.gps-practice-and-fun.com/offender-tracking.html). Additionally, in May 2005,

Massachusetts launched a tracking program. Oklahoma and New Jersey have already passed laws requiring monitoring of offenders for the rest of their lives. Pennsylvania is also considering monitoring “sexually violent predators” through satellite tracking systems (See www.gps-practice-and-fun.com/offender-tracking.html).

¹⁴⁰ Typically, exclusion zones include a victim’s home and workplace.

¹⁴¹ Behre, R. (2005, September 30). GPS weighed to ease jail overcrowding. *Charleston Post and Courier*, p. 1B. Available online at www.nlectc.org/justnetnews/weeklynews.html

¹⁴² See 117 S. Ct. 1416 (1997) wherein a unanimous court held in an analogous situation that a per se exception (to the knock-and-announce rule) based upon a category of cases is prohibited by the 4th Amendment. If one blanket exception is made, it would be easy to cut out other exceptions.

¹⁴³ See Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, § 802, 82 Stat. 212 (codified at 18 U.S.C. § 2510-20) and Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§ 2510-21, 2701-10, 3121-26).

¹⁴⁴ 50 U.S.C. § 1801 et seq.

¹⁴⁵ The three subtitles are (1) Title I, the Wiretap Act, which deals with the interception of communications that are in transmission, 18 U.S.C. §§ 2510-2522 (2000); (2) Title II, the Stored Communications Act, which covers the accessing of stored electronic communications and records, 18 U.S.C. §§ 2701-2711 (2000); and (3) Title III, the Pen Register Act, which applies to pen registers and trap and trace devices, which record phone numbers or addressing information (such as the “to” and “from” lines on e-mail) 18 U.S.C. §§3121-3127 (2000).

¹⁴⁶ For example, jurisdictions may define the term *party* as anyone privy to a conversation or as law enforcement personnel only. Jurisdictions may limit the offenses for which interception is permissible to certain select crimes. Some jurisdictions limit the ability to record the intercepted communications. Some jurisdictions may allow interception for officer safety but for no other purpose including use as evidence in criminal or civil matters. Some jurisdictions may allow the communications to be intercepted as part of a videotaped car stop.

¹⁴⁷ The list of legal requirements includes such things as proper authorization from the appropriate official, identifying the investigators, the crimes, and the parties to be intercepted with specificity, tri-partite probable cause, a full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that the order should be issued, the goals and objectives of the interception, as well as the length of time for the interception including when it will begin, end, the actual hours of interception per day, and the days of the week of interception, exhaustion and necessity, minimization and the equipment and technology to be employed.

¹⁴⁸ *United States v. Leavis*, 853 F.2d 215, 221 (4th Cir. 1988), quoting *United States v. Kerrigan*, 514 F.2d 35, 38 (9th Cir.), *cert. denied*, 423 U.S. 924 (1975).

- ¹⁴⁹ United States v. Ferrara, 771 F.Supp. 1266, 1305 (D. Mass. 1991) *aff'd sub. nom.*, United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993).
- ¹⁵⁰ United States v. Clerkley, 556 F.2d 709, 716 (4th Cir. 1977), *cert. denied sub. nom.* London v. United States, 436 U.S. 930 (1978). See also, Scott v. United States, 436 U.S. 128 (1978). The burden of proof for minimization is initially on the government to make a *prima facie* showing of compliance, and then the burden switches to the defense for production and persuasion. United States v. Rizzo, 491 F.2d 215, 217-18 (2d. Cir.) *cert. denied*, 416 U.S. 990 (1974). The standard for compliance for minimization is the overall reasonableness of the totality of the conduct of the monitoring agents in light of the purpose of the wiretap and the information available to the agents at the time of the interception. The more complex and widespread the investigation, the wider latitude of eavesdropping is allowed. United States v. Hoffman, 832 F.2d 1299 (1st Cir. 1987); United States v. Dumes, 313 F.3d 372 (7th Cir. 2002); United States v. Lopez, 300 F.3d 46 (1st Cir. 2002); United States v. Merton, 274 F.Supp. 1156 (D. Col. 2003); United States v. Hernandez-Sandejas, 268 F. Supp. 2d 1295 (D. Kansas 2003). Factors involved in this reasonableness determination include the sophistication of the suspects and counter-surveillance methods, whether coded conversations are used, the location and operation of the target telephone or device, the extent of judicial supervision, the duration of the wiretap, the purpose of the wiretap, and the length of the calls monitored. Two minutes is "too brief a period for an eavesdropper even with experience to identify the caller and characterize the conversation." United States v. Capra, 501 F.2d 267 (2d Cir. 1974) *cert. denied*, 420 U.S. 990 (1975); United States v. Malekzadeh, 855 F.2d 1492 (11th Cir. 1988); United States v. Apodaca, 820 F.2d 348 (10th Cir. 1989); United States v. Dumes, 313 F.3d 372 (7th Cir. 2002); United States v. Wright, 121 F. Supp. 2d 1344 (Kansas, 2000). The existence, or lack thereof, of a pattern of pertinent calls; the absence of privileged interceptions; and the proper handling of interception of windfall, or "other" offenses. Clerkley *supra*, 556 F.2d at 716; Salzman, Spease and Ross v. State, 275 Md. 88 (1975); United States v. Hyde, 574 F.2d 856 (5th Cir. 1978).
- ¹⁵¹ United States v. Bianco, 998 F.2d 1112 (2nd Cir. 1993).
- ¹⁵² There are three states where a strict compliance approach is applied and directs that any violation of the regulatory scheme would result in the complete suppression of all surveillance evidence. State v. Siegal, 266 Md. 256 (1972); State v. Bailey, 289 Md. 143 (1980) (The omission from the order that the intercept would terminate upon attainment of the objectives rendered the order invalid *ab initio*, and all evidence was suppressed despite the fact that the police complied with the missing provision by terminating surveillance early.); State v. Pottle, 677 P.2d 1 (Ore. 1984) (Because of the inherent dangers of abuse and an inherently more intrusive process than a traditional search and seizure, strict compliance with all statutory requirements is necessary. Substantial compliance is inadequate.); State v. Sitko, 460 A.2d 1 (R.I. 1983); State v. Luther, 116 R.I. 28 (1976).
- ¹⁵³ 50 U.S.C. § 1801 et seq.
- ¹⁵⁴ 50 U.S.C. § 1805(a)(3)(a).
- ¹⁵⁵ Under FISA, notice need only be given if criminal charges are filed and, if after an emergency search is authorized, the order is subsequently denied.

- ¹⁵⁶ CRS Report for Congress. The Foreign Intelligence Surveillance Act: An overview of the statutory framework and recent judicial decisions. (2004, September 22). Available online at www.fas.org/irp/crs/RL30465.pdf
- ¹⁵⁷ Foreign Intelligence Surveillance Act: Oversight hearings before the subcommittee on courts, civil liberties, and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong. 2-18 (1983) (testimony of Mary Lawton). (As cited in www.cdt.org/publications/lawreview/1997albany.shtml#I).
- ¹⁵⁸ Refer to the chart shown previously and referenced in endnotes 76-78 above.
- ¹⁵⁹ McGee, J., & Duffy, B. (1996, June 23). Someone to watch over us. *Washington Post*. (As cited in www.cdt.org/publications/lawreview/1997albany.shtml#I).
- ¹⁶⁰ Startrons are night scopes with magnification capacity and are acceptable as surveillance enhancers that do not constitute a “search” within the meaning of the 4th Amendment. *Commonwealth v. Williams*, 396 A.2d 1286, 1289-90 (Pa. Super. 1971); See also, *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (\$22,000 mapping quality camera that took aerial photos was considered mere enhancement technology, not a search).
- ¹⁶¹ In *United States v. Place*, 462 U.S. 696, 707(1983), the Supreme Court permitted canine sniffs as a non-intrusive and limited “type of sensory-enhanced search” because “the sniff discloses only the presence or absence of narcotics, a contraband item.” See also, *Illinois v. Caballas*, 125 S. Ct. 834 (2005).
- ¹⁶² See www.jaycor.com/web-content/eme_sens_ultra.html
- ¹⁶³ See www.securtex.com/wds_overview.asp
- ¹⁶⁴ See <http://researchnews.osu.edu/archive/bakdiode.htm>
- ¹⁶⁵ Singel, R. (2004). *New screening technology is nigh*. Available online at www.wired.com/news/privacy/0,1848,65366,00.html?tw=wn_story_page_prev2. In addition to x-ray type technology referred to as the backscatter portal system, TSA is also field testing Smart identity cards and a device to be used at passenger-screening portals that shoots puffs of air at passengers to loosen particles, which the machine then quickly tests for explosive residue.
- ¹⁶⁶ Electronic Privacy Information Center. “Backscatter” x-ray screening technology. Available online at www.epic.org/privacy/airtravel/backscatter/default.html
- ¹⁶⁷ TSA is aware of the revealing nature of the images and is working with companies to create software that would substitute a generic body but leave in place the outlines of the suspected contraband; however, that software has not been developed [See *Airports roll out high-tech security*. (2005, May 15). Available online at www.usatoday.com/travel/news/2005-05-15-xray-inside_x.htm].
- ¹⁶⁸ See www.epic.org/privacy/airtravel/backscatter/default.html

- ¹⁶⁹ Security Solutions Network. (2005). Smiths detection presents Tadar—a new people screening system based on millimeter-wave technology—at Inter Airport Europe. Available online at www.smithsdetection.com/eng/1025_1193.php
- ¹⁷⁰ Webster, B. (2005, July 8). Body scan machines to be used on tube passengers. *Times Online*. Available online at <http://technology.timesonline.co.uk/article/0,,20409-1686151,00.html>
- ¹⁷¹ Secure Automobile Inspection Lanes Pilot (SAIL). (2004, October 21). TSA to conduct first real-world test of cutting-edge backscatter technology. Available online at www.tsa.gov/press/releases/2004/press_release_0527.shtm. Secure Automobile Inspection Lanes Pilot (SAIL); SAIL II Home. (2005, August 29). Available online at www.tsa.gov/what_we_do/layers/sail/editorial_multi_image_0092.shtm
- ¹⁷² Improving Aviation Security – Cherif Rizkalla. Statement of Cherif Rizkalla, President, Smiths Detection, Americas. (2005, July 13). Available online at www.smithsdetection.com/eng/1025_1185.php
- ¹⁷³ See www.usatoday.com/travel/news/2005-05-15-airport-xray-bottomstrip_x.htm
- ¹⁷⁴ See www.g2tactics.com/glavid.html and www.g2tactics.com/bootfinder.html
- ¹⁷⁵ The device has been sold to the New Haven, Connecticut, Police Department; numerous Maryland law enforcement agencies; the Arlington, Virginia, Parking Authority among others, and has been tested by the Chicago Police Department.
- ¹⁷⁶ *United States v. Cusumano*, 83 F.3d 1247, (10th Cir. 1996) (dissent by J. McKay).
- ¹⁷⁷ Schwab, J. (2005, September 28). New Athens chief gets training with thermal camera. *Belleville, News Democrat (IL)*. Available online at www.nlectc.org/justnetnews/10062005.html#story2. See also www.flirthermography.com/news/news_item/1067/
- ¹⁷⁸ See www.flirthermography.com/news/news_item/1067
- ¹⁷⁹ *California v. Greenwood*, 486 U.S. 35 (1988).
- ¹⁸⁰ *Kyllo v. United States*, 533 U.S. 27 (2001).
- ¹⁸¹ *Katz v. United States*, 389 U.S. 347 (1967).
- ¹⁸² See www.darpa.mil/grandchallenge/overview.html
- ¹⁸³ See http://dtsn.darpa.mil/ixo/solicitations/CTS/file/BAA_03-15-CTS_PIP.pdf
- ¹⁸⁴ U.S. Department of Defense. (2004, March). Safeguarding privacy in the fight against terrorism: Report of the technology and privacy advisory committee.
- ¹⁸⁵ 5 U.S.C. § 552a; See www.usdoj.gov/04foia/privstat.htm. The Privacy Act of 1974 gave individuals the right to know and correct the information that the government was maintaining, collecting, using, or disseminating about them. Individuals have the right to review all information collected on oneself, request corrections, and be informed of

any disclosures. The Freedom of Information Act facilitates these processes. Additionally, the law restricted the government from building databases unless the information (as to education, financial transactions, medical history, criminal or employment history, name or identifying number or symbol including finger or voice print or photograph, etc.) about the person was directly relevant and necessary to an agency's mission. The act also requires the government, to the extent practical and possible, to collect the information directly from the subject, to inform the subject of the principal purpose for which the information will be used and the routine uses which may be made of the information, and to advise the individual of the effects of not providing the requested information. A huge limitation of the Privacy Act is that it controls only the government's collection of records not private industry's collection. By collecting information from nongovernmental sources, the government sidesteps the Privacy Act. The government does not have to correct the information, go to the source, or meet some of the other privacy protection limitations concerning disclosure practices provided within the act. Private sources are performing the dirty work for the government without the governmental mandated restraints. Big brother's little helpers. Available online at www.epic.org/privacy/choicepoint/cp_article.pdf

¹⁸⁶ Public Law 107-347—Dec. 17, 2002 116 Stat. 2899; http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

¹⁸⁷ Electronic Communications Privacy Act ("ECPA") of 1986, Pub. L. No. 99-508, 100 Stat. 1848. 18 U.S.C. § 2510(12) (2004) (codified as amended in scattered sections of 18 U.S.C.

¹⁸⁸ USA PATRIOT Act of 2001, Pub. L. No. 107-56, 215, 115 Stat. 272, 287, 50 U.S.C. 1861-1862 (2004)

¹⁸⁹ Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. 1002-121 (2004).

¹⁹⁰ Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801-1811 (2000).

¹⁹¹ The ECPA explicitly excludes tracking devices or any communication from a tone-only paging device [18 U.S.C. § 2510(12) (2004)].

¹⁹² *United States v. Knotts*, 460 U.S. 276 (1983).

¹⁹³ *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (holding that "in an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his . . . [actions or contraband] were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.")

¹⁹⁴ *Dow Chemical Co. v. U.S.*, 476 U.S. 227, 238-39 (1986) (using aerial mapping camera does not violate 4th Amendment since the area surveilled was an open field).

¹⁹⁵ *Id.* at 238

¹⁹⁶ *United States v. Forest*, 355 F. 3d 942 6th Cir. 2004), vacated by 125 S.Ct. 1050 (2005).

¹⁹⁷ Krim, J. (2005, October 28). FBI dealt setback on cellular surveillance. Available online at www.washingtonpost.com

- ¹⁹⁸ *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994).
- ¹⁹⁹ *United States v. Karo*, 468 U.S. 705 (1984); *United States v. Gbemisola*, 225 F.3d 753 (D.C. Cir. 2000); *United States v. Knotts*, 460 U.S. 276 (1983).
- ²⁰⁰ *United States v. Karo*, 468 U.S. 705 (1984).
- ²⁰¹ *United States v. Nerber*, 222 F.3d 597, 601 (9th Cir. 2000).
- ²⁰² In *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987), the court ruled that the installation of a surveillance camera on a power pole to videotape activities in a suspect's backyard constitutes a "search" within the meaning of the 4th Amendment, cited in *United States v. Nerber*, *supra* at 601. In *Bond v. United States*, 529 U.S. 334 (2000), the Court reaffirmed the general principle that the nature of the intrusion by the government can have an effect on whether a citizen has a legitimate expectation of privacy. There, a Border Patrol agent boarded a bus traveling between California and Arkansas, checked the immigration status of its passengers, randomly squeezed the defendant's canvas bag that was stored in the overhead compartment, and discovered a brick of methamphetamine. This action violated Bond's 4th Amendment right to privacy. *United States v. Nerber*, *supra*; The Court will consider the severity of the governmental intrusion in determining whether a citizen has a legitimate expectation of privacy. Hidden video surveillance is extremely intrusive, particularly when a video search is directed straight at a person, rather than a location.
- ²⁰³ See endnote 197 above.
- ²⁰⁴ *Kyllo v. United States*, 533 U.S. 27 (2001). (Using thermal imaging technology to peek inside a home to observe heat emissions consistent with a hydroponics marijuana growing operation constituted a search within the meaning of the 4th Amendment.)
- ²⁰⁵ 47 U.S.C. §§ 1002-121 (2004).
- ²⁰⁶ For example, the CALEA provisions require telecommunication carriers to make their equipment capable of transmitting call content and call-identifying information. Regarding call content information, CALEA was instrumental in forcing Verizon to comply with the law concerning their push to talk and Voice Over IP technology in 2004. CALEA won the battle in October 2004, and Verizon will now make the technology for surveillance available to law enforcement. The VOIP Regulatory Freedom Act § 2281, Senate Commerce Committee Hearings, June 16, 2004. Historically, Internet Service Providers (ISP's) in the United States were exempt from CALEA requirements. The FBI wants to expand the law to include voice over IP.
- ²⁰⁷ See www.fcc.gov/911/enhanced/releases.html
- ²⁰⁸ In re Communications Assistance for Law Enforcement Act, Third Report and Order, 14 F.C.C.R. 16794, 16815 (1999).
- ²⁰⁹ *Katz v. United States*, 389 U.S. 347 (1967).
- ²¹⁰ *Id.* at 353.

²¹¹ *United States v. NY Telephone Co.*, 434 U.S. 159 (1977).

²¹² 18 U.S.C. §§ 2701-2711 (2000).

²¹³ Cell site location information is typically collected by cellular companies in the course of processing calls while the device is activated; however, activation (the making or receiving of a call) is not a prerequisite to the recovery of this information. Cell site information may be retrieved even if the phone is off or not actively being used. The technology is such that cell site information reveals caller location within a 40-foot radius of longitude, latitude, and altitude, thereby providing location information within a potentially protected zone of privacy like a residential dwelling in a high rise building. Cell site information also must be available even if the advanced features of the mobile wireless technology creates complexities for providing even basic 911 service. For example, this location information must be available regardless of whether the 911 caller is a subscriber of the wireless provider with coverage in the area or when the calls are blocked. In re *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling System*, FCC Docket No. 94-102, Report and Order and Further Notice of Proposed Rulemaking (See www.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt).

²¹⁴ See e.g., *Couch v. United States*, 409 U.S. 322, 335 (1973). A restaurateur who has given bank statements, payroll records, and reports of sales and expenditures to his or her accountant for the purpose of preparing his or her income tax returns may not invoke his or her 5th Amendment privilege or claim a 4th Amendment privacy interest). *Hoffa v. United States*, 385 U.S. 293, 302 (1966). "Neither this Court nor any member of it has ever expressed the view that the 4th Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."

²¹⁵ *California v. Ciraolo*, 476 U.S. 207, 215 n.3 (1986). The aerial surveillance of an enclosed backyard by the naked eye was not a search; however, using technology that "discloses . . . intimate associations, objects or activities" may be a search. *Dow Chemical Company v. United States*, 476 U.S. 227, 238 n.5 239 (1986). Since the aerial surveillance revealed, "[n]o objects as small as 1/2-inch in diameter (such as a class ring) . . . nor are there any identifiable human faces or secret documents captured in such a fashion," serious privacy concerns were not implicated. What now will be the result with the enhanced capabilities of mapping cameras coupled with face recognition software? Have we finally reached a point where serious privacy concerns are implicated?

²¹⁶ *United States v. Miller*, 425 U.S. 435, 442-43 (1976). An individual has no legitimate 4th Amendment expectation of privacy in original checks and deposit slips, financial statements, and monthly statements maintained, pursuant to the record-keeping requirements of the Bank Secrecy Act of 1970 (12 USCS 1829b(d)), by banks with which the individual had accounts. Federal agents may, by means of subpoenas *duces tecum*, acquire this information since the checks were not confidential communications but negotiable instruments to be used in commercial transactions, and all of the documents obtained, including financial statements and deposit slips, contained only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.

²¹⁷ *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

- ²¹⁸ In re Grand Jury Proceedings, 827 F.2d 301, 305 (8th Cir. 1987). Western Union customers have no privacy interest in Western Union records, as they are not the customers' property.
- ²¹⁹ Smith v. Maryland 442 U.S. 735, 744 (1979) citing, United States v. Miller, *supra*.
- ²²⁰ Executive Order 13388, October 2005.
- ²²¹ Gellman, B. (2005). The FBI'S secret scrutiny. Available online at www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html
- ²²² Gellman, B. (2005). The FBI'S secret scrutiny. Available online at www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html
- ²²³ National security letters gag Patriot Act debate. Available online at www.aclu.org/nsl
- ²²⁴ Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).
- ²²⁵ United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001). The government's key stroke capturing device, Carnivore later known as Magic Lantern, does not fit within the language of the ECPA. The technology behind Magic Lantern does not fit within the statute's definition of electronic storage. The device is installed on a target's hard drive on a personal computer, not on "a facility through which an electronic communication service is provided" such as an ISP. Cookies software, which is similar to the Magic Lantern technology, has been determined not to fit within the ECPA definition of electronic storage because the cookies are implanted on the user's hard drive, and the section defining "electronic storage" "is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission," which infers the statute's intent to control ISP communications, not private person's communications.
- ²²⁶ United States v. Maxwell, 45 M.J. 406, 417 (1996 C.A.A.F. Lexis 116). This case rejected the disclosure rationale and held that a defendant maintains 4th Amendment protection in remotely stored e-mails. The military court found that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. Once the transmissions are received by another person, however, the transmitter no longer controls its destiny. In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.
- ²²⁷ In United States v. Place, 462 U.S. 696, (1983), the Court declared that a canine sniff of luggage in a public place was not a search. Although an individual has a protected privacy interest in the contents of personal luggage, since a canine sniff "does not require opening the luggage and exposing non-contraband items, which would remain hidden from public view, this less intrusion is not a search within the meaning of the 4th Amendment.
- ²²⁸ Smith v., Maryland 442 U.S. 735 (1979). A "pen register" was not held to be a search.

²²⁹ *United States v. Knotts*, 460 U.S. 276 (1983). Placing beeper in container to track movements of vehicle to a remote cabin in the hills was not considered a search.

²³⁰ *Kyllo v. United States*, 533 U.S. 27 (2001).

²³¹ Madison, J. *The Federalist* No. 51, at 349 J. E. Cooke (Ed.), 1961.

Acknowledgments

Anne Burton, JD, deserves special recognition and thanks for her contributions in reviewing and critiquing my thoughts and research.

Jill Joline Myers, JD, is an assistant professor of Law Enforcement and Justice Administration at Western Illinois University. Prior to joining the faculty at Western, she served as a state prosecutor in Baltimore, Maryland, for over 20 years. Leading their Electronic Surveillance and Special Investigation Division, she was responsible for litigating or overseeing all complex drug and gang electronic surveillance investigations. Researching and lecturing extensively on 4th Amendment matters, Professor Myers concentrates her work in the area of technological developments by examining their subsequent application to law enforcement investigations.

The Process and Utility of Psychological Fitness-for-Duty Evaluation in Law Enforcement

Marva Dawkins, PhD, President and CEO, Center for Applied Psychology and Forensic Studies

Marvin P. Dawkins, PhD, Professor of Sociology, Department of Sociology, University of Miami

Amanda Reyes, PsyD, Former Psychological Intern, Center for Applied Psychology and Forensic Studies

Stephen Griffin, PsyD, Post-Doctoral Associate, Center for Applied Psychology and Forensic Studies

This article is based on an earlier presentation at the 113th annual conference of the International Association of Chiefs of Police (IACP) in Boston, Massachusetts, October 16, 2006.

Introduction

Police officers in the United States are charged with fulfilling many functions, including keeping the peace, ensuring public safety, providing assistance in times of emergencies, investigating crimes, and apprehending criminal perpetrators. Given these many responsibilities, law enforcement is often portrayed as a potentially stress-provoking career. Police officer candidates must, therefore, undergo extensive screening and training procedures prior to assuming their positions and, when necessary, evaluation and possible treatment during their careers to assess and maintain fitness for effectively fulfilling their responsibilities in law enforcement (Beutler, Nussbaum, & Meredith, 1988; Hiatt & Hargrave, 1988). Pre-employment screening often includes psychological assessment, in addition to physical exams, written tests, physical Fitness and drug use tests, and background investigations. The intent of these pre-employment screenings is to detect any potential difficulties that may impede a prospective officer from properly discharging duties and to preemptively deal with these difficulties.

The possibility exists, however, that in the course of one's career, an officer may become incapable of performing job responsibilities or begin performing inadequately, thus, producing the potential for placing the public at risk. As a preventive measure, police departments have adopted procedures to address possible officer incompetence. Increasingly, these procedures involve referral to a psychologist for psychological evaluation, a process commonly known as the fitness for duty evaluation or FFDE (Fischler, 2001; Rostow & Davis, 2004; Grossman, Haywood, Ostrov, Wasyliv, & Cavanaugh, 1990; Stone, 2000). Police officers may be referred for an FFDE for a variety of reasons, including, but not limited to the following: a pattern of citizen complaints against them, allegations of egregious infractions, allegations that officers perpetrate violence, incidents involving officers as victims of violence, or when there is suspicion of on-the-job alcohol intoxication or impairment due to other substances. An FFDE may also be ordered when there are observable decreases in an officer's level of fitness involving negative changes in demeanor or such job performance behavior as a pattern of arguments with coworkers, a high proportion of on the job

errors, insubordination, or even peculiar or threatening behavior (Fischler, 2001). Although the psychological FFDE has been previously described (Benner, 1997; Fischler, 2001; French, 2002; Rostow & Davis, 2004), there continues to be a need for better understanding of how the FFDE process works and its potential utility in the context of law enforcement. For example, FFDEs are used to assist police executives in making decisions to ensure that officers returned to regular duties are able to resume responsibilities without placing the public at risk; however, misunderstanding or misperceptions may sometimes exist, both inside and outside of police departments, regarding the meaning and role that FFDEs play in the functioning of police departments. Consequently, there are few reports in the research literature of how the FFDE process actually operates in terms of its implementation by police departments. Such unanswered questions as the following are sometimes the basis of misunderstanding in regard to the FFDE process and its utility:

- What relevant background information is collected?
- What types of behavioral observations are made?
- How are mental status exams, test results, and psychological evaluators' conclusions used in decisions regarding the fitness of referred officers?

Since enforcement of strict confidentiality rules must be maintained for the protection of officers, these questions and others have led to suspicions, such as the view that the primary function of FFDEs is to use this process as part of disciplinary action to remove officers or force them to leave their position. Consequently, few examples of FFDEs and their use by police departments can be found in the law enforcement research literature (Benner, 1997; Fischler, 2001; Stone, 2000). Therefore, a detailed description of the FFDE process and how police departments can use FFDE results to carry out the responsibility of maintaining "fitness" of officers will enhance knowledge and understanding, while dispelling misconceptions that may exist in law enforcement and the wider community (Super, 1997). The purpose of this article is to extend the literature by more fully describing the FFDE process and examining the potential utility of FFDE results in assisting police departments in maintaining "fitness" of the police force. We shall begin with a review of the relevant literature to assess the state of knowledge on the FFDE process and its use.

Review of Related Literature

Fitness for Duty and Characteristics of Police Officers

Although once debated, it is now generally accepted that there is not a single type of police officer who possesses traits of "the good police officer." Rather, police officers are increasingly heterogeneous and possess a wide variety and combination of traits. One of the more consistent findings, however, has been that officers who possess a high level of the personality dimension called conscientiousness are generally successful police officers. Conscientiousness refers to the ability to organize, control, and motivate around goal-directed behaviors (Sarchione, Cuttler, Muchinsky, & Nelson-Gray, 1998). Sarchione et al. (1998) found that officers who had high levels of conscientiousness were rated as reliable, organized, hard working, and capable of self direction. Additionally, police officers rated as "good" officers by their superiors are characteristically self

disciplined, extraverted, emotionally sturdy, and report low amounts of anxiety (Lorr & Strack, 1994). Other personality characteristics that are often found in highly rated police officers include being energetic, persistent, self sufficient, having a dominant stance, and being independent while maintaining flexibility (Hargrave, Hiatt, & Gaffney, 1986; Lawrence, 1984). In addition, police officers with the least amount of disciplinary problems are also able to remain emotionally detached and critical of situations without falling into the pathological range of detachment or criticalness (Lawrence, 1984). Although police officers can possess some combination of the above mentioned qualities, there are also factors that have been found to be associated with negative personality traits. For instance, for some officers, longer time spent as an officer is associated with increased reports of becoming overly suspicious, cynical, and distrustful, in addition to exhibiting emotional detachment and acting out (Adlam, 1982; Ostrov, 1986).

Among physiological characteristics that may affect police officers' fitness for duty, some studies have reported that, in comparison to many other professions, police officers are at higher risk for cancer and cardiovascular disease, while others have disputed such associations (Anderson & Bauer, 1987). Some evidence indicates that subsets of police officers are prone to gastrointestinal disease and headaches (Lawrence, 1984). Within the police officer population, the rates of suicide and alcoholism are higher than those of the general public (Anderson & Bauer, 1987; Beutler et al., 1988). These studies, therefore, suggest that, for some officers, increased time on the police force can lead to negative physical and psychological characteristics, which, in turn, may decrease the ability to effectively perform required duties.

The Need for FFDEs: The Role of Stress and Personality Factors

One of the most important factors in the functionality of police officers, in terms of its effect on job performance and fitness, is the attendant stress of law enforcement work (Alkus & Padesky, 1983; Burke, 1993; Graf, 1986; Morton, 2004). Research in this area has not yielded consistent results. For example, while some studies find that persons who enter law enforcement are adversely affected by their jobs (Morton, 2004), other studies indicate that police officers as a population are better equipped to deal with stressors such as violence and emotional distress and report increased self confidence and assertiveness (Adlam, 1982; Burke, 1993; Hart, Wearing, & Headey, 1995). One of the factors that may increase an officer's stress and maladaptive behavior is exposure to violent situations and actual involvement in violence. Officers' self-reports indicate that they experience several types of violence, including witnessing violence toward other victims, using force or violence against suspects, and having violence directed at them (Anderson & Bauer, 1987). When asked to rank the most severe stressors inherent in their jobs on a continuum of the least to the most stressful events, male officers reported that verbal threats, followed by violence directed at them, witnessing violence against a child, and, finally, their use of deadly force as the most stressful occurrences in their work (Anderson & Bauer, 1987). Some of the most severe work-related reactions displayed are in response to having used deadly force. Many officers who survive deadly force encounters report depression, guilt, and symptoms consistent with Post Traumatic Stress Disorder, such as nightmares, anxiety, and flashbacks (Anderson & Bauer, 1987). In such cases, support of the police department where they are stationed is an important buffer; therefore, in most instances, officers are able to return to work after the appropriate investigations are completed and the officers receive counseling. Notwithstanding the importance of

deadly force encounters and the attention generated by the media regarding such encounters, in general, since exposure to violence is an extreme situation relative to the overall aspects of police work, other sources of stress are more often investigated and reported in the literature.

More common, day-to-day, sources of stress for officers fall under the category of "organizational" stressors. Organizational stressors encompass events such as shift rotations, lack of support from supervisors, boredom between assignments, and the adverse effects of police work on family life (Ostrov, 1986). Indeed, police officers have described the most stressful parts of their job as having to deal with the organizational structure of the police department, the rigid evaluation they undergo by administration and the public, and the rigid schedules they must follow (Hart et al., 1995; Lawrence, 1984; Violanti & Aron, 1993). Additionally, many minority and female police officers report negative social interactions on the job, such as discrimination and social barriers to organizational integration (Morris, 1996), which contribute to their overall perceptions of stress. Occupationally inherent stressors, including the need to balance contradictory roles such as giving orders and obeying orders and the rapid shifts between tedium and danger (Beutler et al., 1988), are ranked as significant stressors for officers. These stressors contribute to the amount of perceived stress for male police officers, which is, in turn, correlated with physical symptoms experienced and dissatisfaction with work and coworkers (Norvell, Hills, & Murrin, 1993). Although officers' reactions to stress in and of themselves do not indicate that they are unfit for duty, a pattern of negative responses could indicate a pre-emptive need for treatment before significantly negative behaviors occur. Thus, being attuned to sources of police stress can lead police executives to make organizational changes that may decrease the levels of negative stress that officers experience.

The research literature on police stress, therefore, gives valuable insight concerning antecedents of officers' maladaptive behaviors, although not all officers who have negative reactions to stress reach a level at which their fitness for duty comes into question. While environmental factors and stressors contribute to problem officers' negative behaviors, these factors alone do not account for all of the dysfunctional behaviors that are displayed. More recent exploration of personality structures that predispose police officers to problem behaviors have been investigated in terms of questions regarding fitness. For example, lower levels of measured dimensions of conscientiousness have been found to be associated with a tendency to be lazy, careless, impulsive, and irresponsible in relation to job performance (Sarchione et al., 1998). Accordingly, in keeping with the belief that personality structure influences behavior, forensic assessment providers have included personality measures as part of their FFDE assessment procedures.

Personality Assessment Instruments Used in FFDEs

Evaluators report using many instruments in FFDEs, and there is overlap with instruments used in police officer candidate selection (i.e., screening), including the Minnesota Multiphasic Personality Inventory (MMPI), the California Personality Inventory (CPI), the Inwald Personality Inventory (IPI), and others. Among the objective tests used in police officer evaluation, the MMPI-2 and the CPI are among the most validated tests for police candidate selection (Ostrov, 1986). As such, they are the most widely included measures in FFDEs, although the literature regarding the use of these instruments in the FFDE arena is limited. What is known is that

the MMPI-2 and CPI look promising as valid instruments for use in assessment of fitness for duty (Cross & Burger, 1982; Gough, 1995; Pugh, 1985; Saxe & Reiser, 1976; Schmit & Stanard, 1996; Schneider, 2002; Scogin, Schumacher, Gardner, & Chaplin, 1995). It should also be noted that, though the MMPI and CPI are the most widely used objective measures in FFDEs, overall, the scores on these measures cannot predict whether an officer will be a problem officer or a conforming officer (Wells, 1992). Rather, their predictive validity is attributed to predicting certain subsets of behavior that are relevant to the concepts of fit (conforming) versus unfit (problem) officers. As the research in this area continues to develop, the few studies directly addressing the results of MMPI and CPI measures in FFDEs will be highlighted.

Results on the MMPI have differentiated between fit and problem officers when evaluations were conducted after officers developed problem behaviors. For instance, male officers with characteristics such as being more dysphoric, conventional, and behavior conforming were more likely to have higher performance ratings, lower numbers of suspensions, and lower numbers of grievances filed against them (Beutler et al., 1988). Conversely, the likelihood of an officer being suspended was highly correlated with general elevations on the MMPI clinical scales (Beutler, Strom, Kirkish, Scogin, & Gaines, 1985; Hiatt & Hargrave, 1988). Additionally, for Caucasian officers in university police settings, there is a correlation between longer time on the job and an increased vulnerability to addictive behaviors and stress-related neurotic psychopathology (Beutler et al., 1988). One of the pitfalls in using MMPI data to assess overall character traits, however, is that it is difficult to generate meaningful descriptions from MMPI data unless there are clinical elevations of the scales. Thus, it has been challenging to generalize results from MMPI profiles, as sworn officers often do not score in the clinically significant ranges of pathology.

Since its inception, the CPI has been touted as a measure of "normal" personality characteristics and has been used in a variety of occupational assessment settings, including the screening of potential police officers and the evaluation of police officers. An early study using the first version of the CPI found that scores on eight scales of the CPI were discriminative between police officers who were rated average and those rated highly by their superiors (Hogan, 1971), providing a basis for the use of the CPI during psychological evaluations of police officer populations. The CPI is also useful in assessing police officer characteristics as these relate to assessments of their psychological suitability by independent investigators (Hargrave & Hiatt, 1987). Additionally, officers' CPI profiles have a consistent, and often direct, relationship with supervisors' ratings of their leadership abilities and suitability for their jobs (Hargrave & Hiatt, 1987; 1989). For instance, officers who were rated by their superior officers as doing well tended to have elevated scores on the dominance, functional intelligence, and autonomous achievement scales of the CPI (Mills & Bohannon, 1980). These CPI results are consistent with previous research findings in which fit-for-duty police officers were described as organized, goal directed, self motivated, and emotionally sturdy. Such officers also score high on the CPI measures of socialization and self control, and are typically regarded as dependable and rule abiding individuals who are able to control their emotions when necessary (Sarchione et al., 1998).

On the other hand, as measured by the CPI, problem police officers are less dependable, less willing to conform to social norms, less disciplined, and less likely to plan than officers without a history of disciplinary problems. Additionally, problem officers are regarded as prone to being careless, impulsive, and showing a lack of regard for

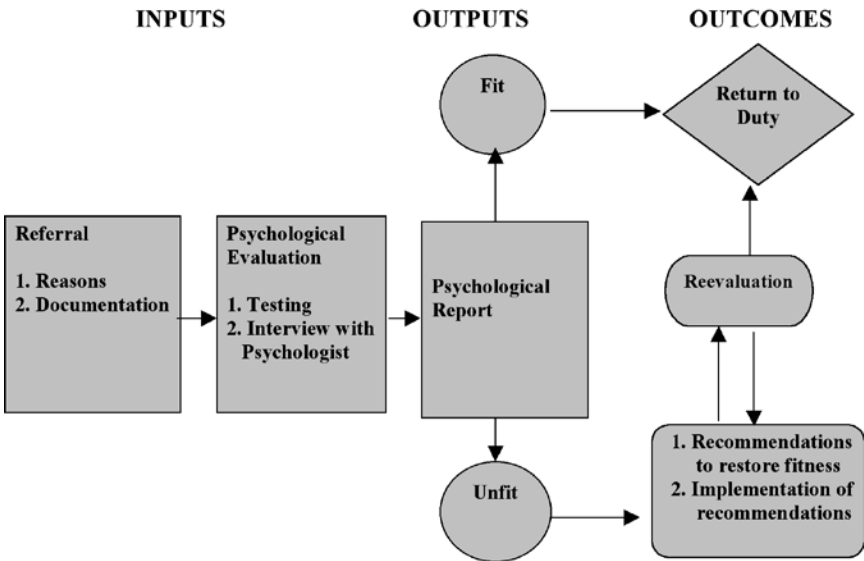
their assigned duties (Hargrave & Hiatt, 1989; Sarchione et al., 1998). These behaviors correspond with low scores on the self control and socialization scales, scales that measure traits such as impulsivity, risk-taking, lack of objectivity, and willingness to break rules (Hargrave & Hiatt, 1987). Also, low scores on communality, good impression, responsibility, self-control, socialization, and tolerance scales of the CPI are associated with officers who have been responsible for unnecessary use of force (Hargrave & Hiatt, 1989). While these results do not provide a predictive personality constellation for unfit officers, they highlight the types of traits that might be intuitively expected in officers who have difficulty conforming to the rigid codes of police behavior.

To conclude, the literature on FFDE has been primarily devoted to addressing the need for psychological evaluations to identify environmental stressors and psychological factors that may affect police officers' performance of duties and responsibilities. Less attention has been given to addressing the need of the law enforcement community and the general public for a better understanding of how the psychological FFDE process actually operates. We will turn, now, to address this need to extend the literature by presenting a depiction and discussion of how the FFDE process actually operates, with the aim of clarifying its inputs, outputs, outcomes, and associated activities. In addition, we will examine the potential utility of FFDE results as internal feedback to police departments, with the aim of informing decisions of police chiefs regarding strategies to maintain optimal levels of fitness of police officers.

Conducting FFDEs: The Process

The FFDE can be depicted as a process involving inputs, outputs, and intended outcomes (see Figure 1). A description and discussion of activities associated with each stage of the process follows.

Figure 1. Fitness for Duty Evaluation Process



Inputs

Two types of inputs in the FFDE process can be identified: (1) referrals and (2) psychological tests. FFDEs begin when a referral is made by a police department for an officer to be evaluated. The referral procedure involves two activities: (1) providing reasons for the referral and (2) providing documentation to support the decision to refer. Reasons for referrals can usually be characterized as emotional distress, behavioral concerns, or somatic concerns. Emotional distress involves allegations of anxiety, depression, problems with attention, concentration, mood swings, impulse control, anger outbursts, suicidal or homicidal concerns, and emotional reactions to situational stressors (e.g., death of a loved one, marital or spousal separation and divorce, shift changes, problems getting along with assigned partner, or financial concerns). Emotional distress may be related to alcohol or other substance abuse. This can include allegations of substance abuse, a pattern of excessive alcohol use, or relapse into drinking after past treatment for alcoholism, along with the problems described above under the emotional distress category. Behavioral concerns as reasons for referrals can include allegations of excessive force, disruptive behavior in the workplace, failure to follow a supervisor's directive, consistent patterns of absenteeism or tardiness, multiple reports of complaints registered by citizens, arrests for driving under the influence of alcohol or other drugs, multiple auto accidents, child abuse and neglect, or any other serious display of behavior contrary to the standards set forth by the police department. Behavioral concerns may be related to domestic violence involving allegations of abuse/violence directed at a significant other. Somatic concerns include allegations of physical condition complaints by officers with or without objective findings from a physician or other healthcare provider to support such complaints. Somatic concerns that lead to referrals are usually accompanied by an emotional overlay involving emotional distress. The documentation provided to support a referral decision includes an officer's performance ratings, reports of registered complaints against the officer, Internal Affairs investigative reports, and supervisors' comments.

After the referral of an officer for a FFDE is made, the officer must undergo psychological evaluation. This evaluation involves two activities: (1) psychological testing and (2) a psychological interview by a licensed psychologist. The psychological tests are designed to assess personality dynamics, behavior functioning, cognition, symptoms complaints, anger and temperament concerns, and patterns of alcohol use. Tests administered as part of a typical battery include the CPI, the Personality Assessment Inventory (PAI), the State-Trait Anger Expression Inventory-2 (STAXI-2), and the Shipley Institute of Living Scale (SILS), among others. The CPI is a self-administered, pencil-and-paper, objective personality measure consisting of 434 items. There are 20 scales, and the median reliability for test-retest of the individual scales is .70 (Gough, 1987; 1996). The form of the CPI used in the FFDE compares a subject's scores to known norms for police and public safety professionals. The scales of the CPI can be divided into overall groupings that assess for the areas of interpersonal adequacy, poise, self-confidence, socialization, responsibility, achievement potential, and intellectual modes (Hargrave & Hiatt, 1989). Depending on a subject's constellation of scores on subscales, subjects can be classified according to one of four "vectors" (1) Alpha, (2) Beta, (3) Gamma, and (4) Delta. The positive traits associated with Alphas include, being enterprising, dependable, and outgoing (Roberts, 2004). The positive traits

associated with Betas include being reserved, responsible, and moderate. Gammas tend to be adventurous and pleasure seeking, while Deltas tend to be withdrawn and private (Roberts, 2004). The PAI is comprised of 344 items and 22 scales. It was designed to aid in clinical diagnosis and screening for psychopathology. For the normative sample, a range of internal consistency alpha coefficients of .45 to .90 with a median of .81 has been found. For the clinical sample, alpha coefficients of internal consistency range from .23 to .94 with a median of .86 (Morey, 1991). The overall test-re-test reliability ranges from .31 to .92 with a median of .82, while the subtest test-retest reliability ranges from .68 to .85 with a median of .78 (Morey, 1991). When used in conjunction with the CPI, scores on the PAI are better predictors of when an officer will meet problem criteria than predictions based on the CPI and MMPI-2 used separately (Roberts, 2004). The STAXI-2 is a self-administered, 57-item inventory designed to measure the experience, expression, and control of anger. The internal consistency reliability for the STAXI scales ranges from .73 to .95, and for the subscales the range is between .73 and .93 (Drummond, 2001). The construct validity of the STAXI has also been supported via factor analysis of test items (Forgays, Forgays & Spielberger, 1997). The SILS is a self-administered, 60-item measure designed to assess general intellectual functioning in adults and adolescents. It is also intended for use as a screening device to detect cognitive impairment in individuals with previously "normal" intelligence (Deaton, 1992). Reliability tests have found that for total scores, the reliability ranges from .62 to .82, with a median reliability of .78. The split-half reliability for total scores is .92. Validity coefficients for SILS scores range from .70 to .80 (Deaton, 1992).

After administering and scoring, a report of the results of these tests is prepared for the psychologist who conducts the face-to-face interview with the officer. In this interview, the psychologist is able to gain further insight regarding the officer's fitness based on direct observation and in-depth discussion of areas of concern based on referral information and test results.

Outputs

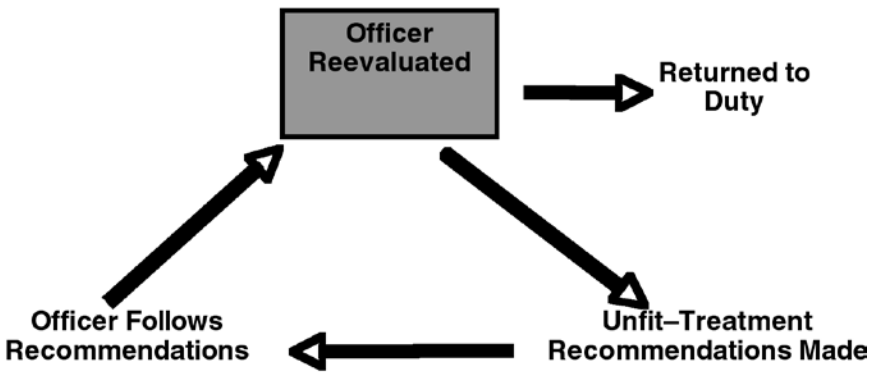
The documented output in the FFDE process is the psychologist's written report, which includes an assessment of an officer's fitness-for-duty status. Specifically, the written report includes an officer's relevant background information, reasons for referral, behavioral observations, mental status examination results, testing responses, and conclusion as to whether an officer is "fit" or "unfit" for duty, along with treatment deemed necessary to restore an officer declared unfit to fitness. Treatment recommendations require that sessions must be held with licensed mental health professionals only. The typical recommendations are for individual counseling/therapy sessions, group counseling/therapy sessions, psychiatric evaluation and psychotropic treatment, participation in outpatient rehabilitation programs, and participation in inpatient programs. Some of the areas of focus of treatment include domestic violence, eating disorder, anger management, current life stressors, alcohol abuse, grief, depression, job issues, and romantic relationships.

Outcomes

The outcome of the FFDE process for a police officer found "fit" is that the officer is returned to duty; however, an officer found "unfit" must, first, follow the recommendations for treatment to restore fitness and, then, undergo re-evaluation

through which a psychological assessment of “fit/unfit” is made, once again, to determine whether that officer should be returned to duty or recommended for further treatment. The fitness-for-duty re-evaluation sequence is depicted in Figure 2 to illustrate how this stage of the process operates. Note that this sequence is repeated each time an officer who has been previously found to be unfit is found unfit upon re-evaluation. Even after an officer has been found fit and returned to duty, however, there is a possibility that at a later time, a referral for an FFDE can be made, whereby, this referred officer must begin the process at the initial (input) stage rather than the re-evaluation sequence stage of the process.

Figure 2. FFD Reevaluation Sequence*



* Sequence is repeated each time an officer is found unfit upon reevaluation.

The diagrams depicting the flow of stages through which FFDEs pass (Figures 1 and 2) can also be useful in identifying areas of strength and weakness in a police department’s planning, in terms of developing and assessing the effectiveness of its FFDE process. We turn now to describe the potential uses of FFDE results beyond their primary intent.

FFDE as Feedback to Police Departments: Potential Utility

As a specific action taken in response to behaviors that indicated a potential for an officer to be unable to properly carry out required duties and responsibilities, the officer is referred for a psychological FFDE. Although the results of the evaluation are used in making decisions regarding the fitness for duty of an individual officer, aggregated FFDE results accumulated over time may reveal patterns that can inform strategies developed by police departments aimed at reducing referrals or preventing the actions that lead to referrals altogether. Thus, FFDE results may reveal patterns, which can serve as important feedback to police departments and be used in creating structural changes with the aim of preventing the behaviors that lead to referrals for psychological evaluation of officers. Some examples of potential uses of FFDE results to prevent or reduce referrals for psychological

evaluations in a police department may illustrate the untapped utility of this data as internal feedback:

- To identify patterns that indicate a need for developing prevention and early intervention strategies related to alcohol and other substance abuse, domestic violence, or other behaviors that place officers at high risk of being referred for a psychological evaluation
- To identify patterns that indicate a need to address possible over-representation of officers being referred for psychological evaluations based on demographic factors (e.g., age, gender, ethnicity, length of time in a department, etc.)
- To examine and address the extent to which there is a disproportionately higher rate of certain types of referrals (e.g., environmental stress-related) in police departments based on their location
- To develop a system of monitoring and feedback in reporting aggregate FFDE results to police departments so that regular assessment of the fitness of officers in a department, overall, can be made and, when necessary, changes can be implemented on a timely basis
- To educate police chiefs and other police executives regarding the importance of using psychological FFDEs as “tools” to ensure fitness of officers, rather than using them to exact punishment or to withhold making referrals out of loyalty to dedicated police officers

While there may be other uses, these examples illustrate the potential utilization of FFDE referral data by a police department in meeting the fitness needs of its officers. Caution must always be taken to ensure that guidelines for the protection of privacy rights of officers and other protections are adhered to and that the use of FFDE results for evaluative feedback to police departments is carried out by competent specialists in evaluation research.

Conclusion

Since the psychological FFDE has become widely recognized in law enforcement as a process intended to ensure the mental health, safety, and effectiveness of police officers and the departments in which they work, it is important that the functioning and utilization of this process is neither misunderstood nor undervalued. In addressing these needs, this article provided an extensive review of the research literature related to the assessment of police officers’ fitness; presented the FFDE in the context of a diagrammatic depiction to clearly identify its major components and the flow of actions through which referred cases follow, leading to a final evaluation of an officer being declared “fit to return to duty”; and presented a brief discussion of the potential of FFDE results as feedback to police departments to illustrate the value and utilization of these results in planning and strengthening a police department’s efforts related to FFDEs. As more police departments utilize the FFDE process, it is important that procedures that are put in place are not haphazardly planned and follow systematic and logical steps, such as those suggested in this article. Since some departments provide FFDEs on an in-house basis, rather than through the use of external psychological services,

it is especially important for the FFDE to be perceived as nonpunitive in these departments and for police officers who are referred for psychological evaluation in such departments to understand that the role of the FFDE process is to ensure their fitness for duty rather than serve as a prelude to disciplinary action. Finally, more use should be made of FFDE results in planning for the needs of police officers and the departments in which they serve, especially in developing psychological support services and prevention strategies.

References

- Adlam, K. R. C. (1982). The police personality: Psychological consequences of being a police officer. *Journal of Police Science and Administration, 10*, 344-349.
- Alkus, S., & Padesky, C. (1983). Special problems of police officers: Stress-related issues and interventions. *Counseling Psychologist, 11*(2), 55-64.
- Allen, M. G., Hibler, N. S., & Miller, R. (2000). Fitness for duty evaluations of law enforcement officers in accordance with federal occupational health procedures. In D. Sheehan (Ed.), *Domestic violence by police officers* (pp. 27-35). Washington, DC: U.S. Department of Justice, Federal Bureau of Investigation.
- Anderson, W., & Bauer, B. (1987). Law enforcement officers: The consequences of exposure to violence. *Journal of Counseling and Development, 65*, 381-384.
- Benner, A. W. (1997). Determining the need for fitness-for-duty evaluations. *Police Chief, 54*, 141-143.
- Beutler, L. A., Nussbaum, P. D., & Meredith, K. E. (1988). Changing personality patterns of police officers. *Professional Psychology: Research and Practice, 19*(5), 503-507.
- Beutler, L. E., Storm, A., Kirkish, P., Scogin, F., & Gaines, J. A. (1985). Parameters in the prediction of police officer performance. *Professional Psychology: Research and Practice, 16*(2), 324-335.
- Burke, R. J. (1993). Work-family stress, conflict, coping, and burnout in police officers. *Stress Medicine, 9*(3), 171-180.
- Cross, D. T., & Burger, G. (1982). Ethnicity as a variable in responses to the California psychological inventory items. *Journal of Personality Assessment, 42*(2), 153-157.
- Deaton, W. L. (1992). Review of the Shipley Institute of Living Scale. In J. J. Kramer & J. C. Conoley (Eds.), *The eleventh mental measurements yearbook* (pp. 822-824). Lincoln, NE: Buros Institute of Mental Measurements.
- Drummond, R. J. (2001). Review of the State-Trait Anger Expression Inventory. In B. S. Plake & J. C. Impara (Eds.), *The fourteenth mental measurements yearbook* (pp. 1182-1183). Lincoln, NE: Buros Institute of Mental Measurements.
- Fischler, G. L. (2001). Psychological fitness-for-duty examinations: Practical considerations for public safety departments. *Illinois Law Enforcement Executive Forum, 1*, 77-92.

- Forgays, D. G., Forgays, D. K., & Spielberger, C. D. (1997). Factor structure of the state trait anger expression inventory. *Journal of Personality Assessment*, 69(3), 497-507.
- French, L. (2002). Assessing law enforcement personnel: Comparative use of the MMPI's. *Forensic Examiner*, 11, 21-27.
- Gough, H. G. (1987). *California Psychological Inventory: Administrator's guide*. Palo Alto, CA: Consulting Psychologists Press.
- Gough, H. G. (1995). Career assessment and the California Psychological Inventory. *Journal of Career Assessment*, 3(2), 101-122.
- Gough, H. (1996). *CPI manual*. Palo Alto, CA: Consulting Psychologists Press.
- Graf, F. A. (1986). The relationship between social support and occupational stress among police officers. *Journal of Police Science and Administration*, 14, 178-186.
- Grossman, L. S., Haywood, T. W., Ostrov, E., Wasyliw, O., & Cavanaugh, J. L. (1990). Sensitivity of MMPI validity scales to motivational factors in psychological evaluations of police officers. *Journal of Personality Assessment*, 55(3&4), 549-561.
- Hargrave, G. E., & Hiatt, D. (1987). Law enforcement selection with the interview, MMPI, and CPI: A study of reliability and validity. *Journal of Police Science and Administration*, 15, 110-117.
- Hargrave, G. E., & Hiatt, D. (1989). Use of the California psychological inventory in law enforcement officer selection. *Journal of Personality Assessment*, 53(2), 267-277.
- Hargrave, G. E., Hiatt, D., & Gaffney, T. W. (1986). A comparison of MMPI and CPI test profiles for traffic officers and deputy sheriffs. *Journal of Police Science & Administration*, 14(3), 250-258.
- Hart, P. M., Wearing, A. J., & Headey, B. (1995). Police stress and well being: Integrating personality, coping, and daily work experiences. *Journal of Occupational and Organizational Psychology*, 68, 133-156.
- Hiatt, D., & Hargrave, G. E. (1988). MMPI profiles of problem peace officers. *Journal of Personality Assessment*, 52(4), 722-731.
- Hiatt, D., & Hargrave, G. E. (1988). Predicting job performance problems with psychological screening. *Journal of Police Science & Administration*. 16(2), 122-135.
- Hogan, R. (1971). Personality characteristics of highly rated policemen. *Personnel Psychology*, 24, 679-686.
- Lawrence, R. A. (1984). Police stress and personality factors: A conceptual model. *Journal of Criminal Justice*, 12(3), 247-263.
- Lorr, M., & Strack, S. (1994). Personality profiles of police candidates. *Journal of Clinical Psychology*, 50(2), 200-207.

- Meier, R. D., Farmer, R. E., & Maxwell, D. (1987). Psychological screening of police candidates: Current perspectives. *Journal of Police Science & Administration*, 15(3), 210-215.
- Mills, C. J., & Bohannon, W. E. (1980). Personality characteristics of effective state police officers. *Journal of Applied Psychology*, 65(6), 680-684.
- Morey, L. C. (1991). *Personality Assessment Inventory professional manual*. Odessa, FL: Psychological Assessment Resources, Inc.
- Morris, A. (1996). Gender and ethnic differences in social constraints among a sample of New York City police officers. *Journal of Occupational Health Psychology*, 1(2), 224-235.
- Morton, T. (2004). Job-related stressors on African-American police officers. *Dissertation Abstracts International*, 64 (7-A), 2563. Walden University.
- Norvell, N. K., Hills, H. A., & Murrin, M. R. (1993). Understanding stress in female and male law enforcement officers. *Psychology of Women Quarterly*, 17, 289-301.
- Ostrov, E. (1986). Police/law enforcement and psychology. *Behavioral Psychology and the Law*, 4(4), 353-370.
- Ostrov, E., Nowicki, D., & Beazley, J. (1987). Mandatory police evaluation: The Chicago model. *Police Chief*, 54, 30-35.
- Pugh, G. (1985). The California Psychological Inventory and police selection. *Journal of Police Science & Administration*, 13(2), 172-177.
- Roberts, M. D. (2004). *Psychological screening: A cookbook*. Los Gatos, CA: Law Enforcement Psychological Services, Inc.
- Rostow, C. D., & Davis, R. D. (2004). *A handbook for psychological fitness-for-duty evaluations in law enforcement*. New York: The Hawthorn Clinical Practice Press.
- Sarchione, C. D., Cuttler, M. J., Muchinsky, P. M., & Nelson-Gray, R. O. (1998). Prediction of dysfunctional job behaviors among law enforcement officers. *Journal of Applied Psychology*, 83(6), 904-912.
- Saxe, S. J., & Reiser, M. (1976). A comparison of three police applicant groups using the MMPI. *Journal of Police Science and Administration*, 4, 419-425.
- Schmit, M. J., & Stanard, S. J. (1996). The utility of personality inventories in the employee assistance process: A study of EAP referred police officers. *Employee Assistance Quarterly*, 11(4), 21-42.
- Schneider, B. M. (2002, October). Using the big-five personality factors in the Minnesota Multiphasic Personality Inventory, California Psychological Inventory, and Inwald Personality Inventory to predict police performance. *Dissertation Abstracts International*, 63 (4-B), 2098. Florida International University.

Scogin, J. S., Schumacher, J., Gardner, J., & Chaplin, W. (1995). Predictive validity of psychological testing in law enforcement settings. *Professional Psychology: Research and Practice, 26*(1), 68-71.

Stone, A. V. (2000). *Fitness for duty: Principles, methods, and legal issues*. Boca Raton, FL: CRC Press.

Super, J. T. (1997). Select legal and ethical aspects of fitness for duty evaluations. *Journal of Criminal Justice, 25*(3), 223-229.

Violanti, J. M., & Aron, F. (1993). Sources of police stressors, job attitudes and psychological distress. *Psychological Reports, 72*, 899-904.

Wells, V. K. (1992, July). The MMPI and CPI as predictors of police performance. *Dissertation Abstracts International, 53* (1-B), 597. St. Louis University.

Marva Dawkins, PhD, a clinical psychologist, is president and CEO of the Center for Applied Psychology and Forensic Studies (CAPFS), an independent psychological services corporation based in Chicago.

Marvin P. Dawkins, PhD, is professor of sociology in the Department of Sociology at the University of Miami (Coral Gables, Florida).

Amanda Reyes, PsyD, is a former psychological intern at CAPFS.

Stephen Griffin, PsyD, is currently a clinical psychologist at CAPFS.

Career Paths: Maximizing Talent and Performance

Lynn A. Tovar, EdD, Assistant Professor, Department of Justice, Law, and Public Safety Studies, Lewis University

Law enforcement agencies today are facing many challenges; recruitment and talented leadership are two of the greatest. Attracting, developing, and retaining quality talented employees today is more costly and has a greater impact on the bottomline than ever before. Police leaders are dealing with retiring baby boomers and the infusion of the expectations from Generation X and Y employees, which can add up to a drastic shift in how to maximize the value locked up in your human capital. There are several core assumptions involving police officers' development: change the way you select, measure, develop, and channel the careers of your people. Much of the responsibility will lie with the top administrator(s) to select for talent, set clear expectations, focus on strengths, and develop each employee's career. Administrators should strive to capitalize on the strengths and talents of every employee.

One effective way to overcome these challenges is to implement a career planning initiative. This proactive approach to ensuring future leadership talent offers many benefits. Organizations with career planning programs have a higher retention rate of human capital and a reduction in recruitment and compensation costs (Frank, 2005). One of the greatest benefits the career plan offers is preparing the department's existing talent for future leadership roles. Consideration must be made for the future direction of the department as well as the direction of the employee's intended career path. This ensures that the employee is engaged in the process, committed to the department, and has a vested interest in the department's success.

Recruit Talent

The responsibility of recruiting and selecting the right fit for your department should be identified as one of the most critical functions within the organization. The first step in designing a career plan is to focus on recruiting strategies that link directly to the values and goals, of the department. Once your department has established these core values and goals the department can recruit for talented people to fulfill their mission. Qualified applicants must be educated, effective communicators who understand their role and can meet the standards of modern policing. Qualifications for hire have always included an individual's character, physical agility, cognition, and the aptitude to perform the job, but we have failed to look for the individual talents or strengths candidates possess.

Unlike skills, talents and personal strengths cannot be taught. Since skills can be taught, such as driving a squad car, firing a gun, or handcuffing an offender, emphasis on selection should be *talent*. Talents are different. Talents are those recurring patterns of thoughts, feelings, or behaviors. Talents such as empathy, desire, discipline, assertiveness, strategic thinking, avoiding confrontation, or positive attitude are talents that guide your choices and will remain constant your entire life. Skills and knowledge can change with time and reflection; however, talents remain constant. Skills can be transferred from one person to another, but

what is essential for the law enforcement profession are those talents that can be transferred from one situation to another situation. The ability to transfer a talent based on the circumstances is an undeniable asset for law enforcement officers. You cannot teach a talent; however, you can select a talent.

Across the country, police departments such as those in Arlington, Texas; Burnsville, Minnesota; Charleston, South Carolina; Dover Township, New Jersey; Lakewood, California; Redlands, California; and Tulsa, Oklahoma, require a bachelor's degree for new hires. These departments proclaim that a college degree is a benefit to the organization. Departments who require police officers to have college degrees have witnessed the difference in the officers' ability to develop critical thinking skills and communicate with people from all walks of life, including those from diverse ethnic and cultural backgrounds. Their college education provides them with a broader understanding of society, and they are more culturally aware. They are big-picture thinkers who utilize technology and sound constitutional law to make decisions with little supervision. Between 1997-2000, the Florida Criminal Justice State and Training Commission (CJSTC) examined whether education levels of police officers correlate to officer misconduct. The data results indicate the higher the educational level, the lower the level of discipline. This translates into fewer citizen complaints, sick days, disciplinary actions from crashes, and use-of-force allegations. In addition, college-educated officers have fewer on-the-job injuries; greater acceptance of minorities; and are less authoritarian, rigid, and conservative. Education also increases the number of career-minded officers seeking promotion to higher aspirations as well as enhancement in minority recruitment. The Arlington, Texas, Police Department has seen a very positive benefit as a result of requiring college degrees, which is an increase in the diversity of their department. Another benefit has been the creation of a network with college professors and instructors who refer their students to the Arlington Police Department and enhance the workforce diversification efforts. Requiring college degrees has not hampered recruitment and selection of the right officers for their department and community. College education does not guarantee that a candidate will become a great police officer, but it does promote critical thinking, which is a necessary talent in police work.

During a time of shrinking qualified candidate pools, it is tempting for departments to compete by lowering their hiring standards, which will only result in less-than-qualified people becoming police officers. Law enforcement agencies across the country that have lowered hiring standards have learned over and over again that it does not work. It opens the door for potential abuse of power, criminal activity, and performance problems (Hunt, 2006). Recruitment and selection of highly qualified police officers into the department is paramount to becoming a professional organization. The carefully selected personnel will advance the department's mission, goals, and objectives with their talent to communicate, think critically, and problem solve for today's ever-changing society.

Measure and Develop Performance

Many of today's police organizations are struggling to find good employees as well as hold onto them. Performance problems are career-related; officers often feel trapped, stagnated, or overlooked in their present position. Many officers find little pleasure in their jobs, which contributes to increased stress, lower productivity, and low morale. These officers do not work up to their full potential and often fail to meet departmental

expectations. They have lost their occupational mission in life and no longer can voice their vocational purpose (Gilley & Egglund, 2005). Further complications arise when supervisors are reluctant to approach officers about their performance and career development. They hold their breath, look the other way, and fail to measure performance in the hopes that the situation will work itself out sometime soon. Law enforcement organizations need to realize that each officer is different, and the organization must capitalize on these differences. "You have to do a lot of things really well in order to keep your best people on board and deeply engaged in their work" (Electronic Recruiting Exchange, 2005). By changing the way the department selects, measures performance, and channels the career paths of its people, it can build a strong, productive, healthy organization around the many strengths of each person. According to CareerMakers (2006), career planning with a focus on the individual's talents in partnership with the organizational needs can result in the following:

- Reduction of turnover
- Significant cost savings (Even if the program retains one to three police officers per year, it will pay off.)
- Positive and motivating work environment
- Reputation as a great place to work and grow skills while enhancing talents
- Open communication and support of growth within the organization
- Loyal employees
- A clear defined plan for supervisors to use while developing their officers
- Understanding and utilizing officers' skills, talents, and interests
- Individual accountability and responsibility for their growth
- Reduce recruiting cost
- Consistency within the organization for advancement

Measuring Talent

There is a saying about doing the same thing, the exact same way, all the time. . . . continue down this road, and you will never promote change. Career pathing provides a way to know which way you're going and which path you're taking, so you don't end up going the same way you always have. How does your department identify people who have the talents needed when the opportunity arises? What type of training and development opportunities are in place for your employees?

The supervisor's primary role is to reach inside each officer and release his or her unique talents into performance. This role works best with one officer at a time; one supervisor asking questions of, listening to, and working with the officer (Buckingham & Coffman, 1999). Without adequate supervision and frequent performance discussions, many officers can go long periods of their career not knowing what their individual strengths are. Feedback should be provided early and often on behalf of the department—as it relates to identifying what someone is good at and what he or she is weak at can be critical in identifying those officers who are capable of taking on advanced career opportunities and leadership responsibilities (Collins, 2003). One way to guarantee individual development and career growth is to let officers know what they are doing well and what they can improve upon. Reinforcing their strengths comes with good training. Training has been found to be the number one investment that organizations can currently make toward developing their people, especially by providing high-quality opportunities for the professional development of future leaders of the organization.

Career Planning Through Career Paths

How does a police agency go about establishing a system for identifying and developing talent within its organization? There are many routes a police officer can take to achieve professional and personal growth. Police administrators must realize that not everyone aspires to become a leader within their organization; however, managers need to acknowledge and support the idea that successful careers can follow a multitude of pathways. Not all employees have to climb the ladder to have a rich and rewarding career. The focus for police administrators should be to develop career opportunities in a variety of directions and then commit resources to assist in their development. Career paths can be structured with two objectives in mind: (1) employees' desires and (2) the organization's needs. The objectives of desire and need are not mutually exclusive. The department must focus on a combined effort to be effective.

Developing an employee through a career path that leads to higher performance and individual development is the ultimate goal of an effective and efficient organization. Those police officers who have a clear understanding of advancement opportunities and are actively involved in their professional career planning and development are more likely to be loyal and committed to the department. Formal career paths are the road maps to career opportunities. They can motivate your officers to excel in their current position with a focus toward the future. Career paths maximize the talents within your officers and inspire them to excel.

Career pathing is the department's and individual's process for identifying specific job opportunities within a department's structure and the sequential steps in education, skills, talents, and experience building needed to attend to specific career goals (Davis, 2005). The design and implementation of a formal career path begins with the support and commitment from the organization's leader. A specifically designed career path program can be developed by utilizing the existing talent within the organization to meet the needs as well as empower those officers working on the project. One avenue of designing and structuring a career path can be accomplished by forming a committee to proceed through the following necessary steps:

- Identify the core competencies, skills, and talents required for the various positions within the department through a need assessment.
- Develop job descriptions from a job task analysis for each position within the department.
- Establish accepted timelines for appointment opportunities.
- Establish career path and positional educational courses for each job description.
- Provide resources for career advancement opportunities.
- Provide career counseling; Supervisors will coach the employee through effective communication in identifying the employee's talents and how the organization can assist with job requirements and opportunities.
- Assess and place the right people in the right positions.
- Continue to provide development and growth opportunities for employees by helping them to perform better in their current position, make lateral moves, and prepare for the next level in their career path.

Even with the full support of the organization, however, it is the individual officer who assumes primary responsibility over his or her career growth. Individual career planning is a process of setting personalized career objectives

and creatively developing activity that will assist them in the achievement of those goals. Additionally, career planning is a personal process, which requires critical self-reflection in three primary areas: (1) broad life planning, (2) individual career development planning, and (3) performance planning. The department that offers a career pathing program with clear specific guidelines for professional opportunities can increase officers' self-confidence and morale and provide direction while strengthening the lines of communication.

Summary

Today's law enforcement profession is more demanding than ever, especially in these turbulent times. In creating a balance, therefore, the interests of all groups—those who are hired as police officers as well as those who are policed—must be served. Law enforcement is not just another job to be filled by placing a want ad in the local newspaper. Only the most qualified police officer candidate should be considered for a position of such importance; anything less is unacceptable. Today's professionals face a complex society that demands competence in problem solving, diplomacy, and consensus building, as well as the traditional qualities of courage and the ability to make sound decisions affecting citizens (Nelson, 1999). Policing is unique and demanding. Recruitment, selection techniques, and retention strategies should all rise to meet the challenge (Rafilson, 1999).

With professional performance being a fundamental cornerstone to success, police administrators will need to implement continuous learning developmental programs with a focus on career planning paths to enable officers to demonstrate talents and acquire new skills to thrive throughout their entire police career. Remember an expectation of the career experience begins with commitment and continues throughout the entire employment relationship. In the end, talent will prove to be your department's most significant competitive advantage in recruiting, performance, departmental *esprit de corps*, community relations, and future leadership development. Since the ultimate goal of law enforcement is to uphold the laws and serve and protect the citizenry, talented, professional, quality officers are essential. By maximizing the talent in the individual person to fit the organizational needs, all involved will benefit. Remember, the job belongs to the department; the career path belongs to the officer.

Bibliography

- Buckingham, M., & Coffman, C. (1999). *First, break all the rules*. New York: Simon & Schuster.
- CareerMakers, Division of HR Answers, Inc. (2006). *Career pathing within the organization*. Portland, OR. Retrieved August 30, 2006, from www.careermakers.com.
- Collins, H. (2003). *Leadership development*. Memphis, TN.
- Cunningham, S. (2003, October). *Discipline and educational levels of law enforcement officers: An exploratory report*. Paper presented at the 110th Annual IACP Conference, Philadelphia, PA.

- Davis, A. (2005, February). President's Pen: Planning for the future of HRACI. *HRA Connection* (Human Resource Association of Central Indiana Newsletter), 61, 1-8.
- Electronic Recruiting Exchange. (2005). The employment brand promise: Begin with the end in mind. Retrieved August 30, 2006, from www.ereexchange.com.
- Frank, J. (2005). *The promotion coach*. Seven unintentional actions that will slow your climb up the corporate ladder. Available online at www.corporateadvancementcoach.com.
- Gilley, J. W., & Egglund, S. A. (2005). *Principles of human resource development*. Reading, MA: Addison-Wesley Publishing Company.
- Hunt, T. (2006, July). Recruitment mission impossible: Experts break the crisis down for APB. *American Police Beat*, pp. 30, 54.
- Mayo, L. (2006, August). College education and policing. *The Police Chief*, 20-38.
- Nelson, K. R. (1999, October). A survey of selecting police officer applicants. *Law and Order Magazine*, 47(10), 42-45.
- Rafilson, K. (1999, June). An alternative to conventional law enforcement written examinations. *Law and Order Magazine*, 47(6), 83-88.

Lynn Atkinson Tovar, EdD, is an assistant professor at Lewis University, Romeoville, Illinois, in the Justice, Law, and Public Safety Studies department. She is a 25-year veteran of law enforcement, retiring as a Commander with the Elk Grove Village Police Department, a law enforcement agency in the Chicagoland area. A career law enforcement professional, Lynn has been involved in street patrol, criminal, and youth investigations with specializations in child sexual abuse and domestic violence. As a supervisor, she oversaw the Youth Investigation/Crime Prevention Division, Field Training Division, K-9, Bike Patrol, and Tactical Unit. Lynn has presented nationally and internationally on law enforcement topics in Illinois, Oklahoma, Hawaii, Texas, Washington, Ohio, Arizona, Michigan, China, and Finland. She has been published in both law enforcement and human resource development journals. In addition to her work at Lewis University, she teaches at the prestigious School of Police Staff and Command at Northwestern University and continues to consult on matters of criminal and social justice, human resource development, leadership education, and vicarious traumatization to first responders. Lynn received her undergraduate degree from Southern Illinois University, Carbondale, Illinois, and holds a Master's degree and a Doctoral degree in Adult Continuing Education with a focus in Human Resource Development from Northern Illinois University in DeKalb, Illinois.

Police Use of Force: Does Gender Make a Difference?

Lorene M. Sandifer, MA, The University of Texas–Arlington

O. Elmer Polk, PhD, Associate Professor, Graduate Advisor, Department of Criminology and Criminal Justice, The University of Texas–Arlington

Alejandro del Carmen, PhD, Associate Professor, Chair, Department of Criminology and Criminal Justice, The University of Texas–Arlington

Introduction

“When you’re in uniform and you’re a man, people see a cop. If you’re a woman and you’re in uniform, people don’t see a cop, they see a woman” (Gerber, 2001, p. xiii).

In contemporary society, police violence seems to populate the press, frequently attracting attention from all segments of the community. It can be argued from a review of the literature on police roles and responsibilities that women have brought different qualities than males to police work (Schulz, 1995). The role of the female officer, as well as acceptance by her peers, has been very slow to evolve (Harrington, 1999).

While the use of force is an inherent part of police work (Ross, 2002), it appears that excessive force has a controversial and costly result (Spillar & Harrington, 2000). According to a study conducted by the Feminist Majority Foundation and the National Center for Women and Policing (NCWP), there is a significant gender difference in the level of police brutality (Lonsway, Moore, Harrington, Smeal, & Spillar, 2003). The director of the NCWP stated in 2000 that “the new study shows that increasing women on the force holds the key for substantially decreasing police violence and its cost to taxpayers” (Smeal, Spillar, & Harrington, 2000). This was in response to the LAPD Christopher Commission study, which found male officers to be liable for payouts in cases of brutality and misconduct at a male to female ratio of 23:1 (Lonsway et al., 2002).

The need for written policies on the use of force was recognized in 1967 by the President’s Commission on Law Enforcement and Administration of Justice, and since then, agencies have tried to specify the definitions of the terms, actions, and discretions surrounding the use of force, providing officers a range of acceptable force options (Alpert & Smith, 1994). Law enforcement officers are allowed to use some degree of force in all citizen contacts, and when making arrests, all reasonable means are permitted (Alpert & Smith, 1994). No greater force shall be used, however, than is necessary to secure the detention or arrest (Adams, Alpert, & Dunham, 1999). Excessive force is that which a reasonable and prudent law enforcement officer would not use under the circumstances (Holman, 2005).

It is quite often this excessive force that sparks intense and expensive lawsuits for police agencies and officers (Alpert & Smith, 1994). The term *excessive* may constitute anything from verbal use; handcuffing improperly or too tightly; physical handling of subjects or prisoners; and brutal and extreme active punching,

kicking, and restraining of subjects to the inappropriate use of deadly force. Gender encompasses physical stature, strength, behavioral, and psychological differences. According to Anne Mangold (2003), gender appears to influence the initiative, handling, and outcome of force situations. Other key terms used interchangeably in this study include *officers*, *personnel*, *police*, *law enforcement*, and *police officer*. All of these terms are used to refer to persons who have obtained law enforcement training and certification or licensing by the state to perform the duties of law enforcement. For the purpose of this study, the term *physical force* refers to any contact force and is not intended to include verbal command.

The purpose of this study is to examine police officers' perceptions toward the use of force and, more specifically, to determine whether there appears to be perception differences between male and female officers. If perception differences toward use of force are found to exist between genders, implications could be inferred for law enforcement agencies' use-of-force policies, as well as training for behaviors within agencies. Three primary questions are addressed in this study:

1. Are the attitudes of male and female officers different toward the capabilities of females performing their jobs?
2. Are female officers equally capable of making arrests as male officers?
3. Do female officers spend more time talking out a situation with a subject rather than resorting to physical force?

Literature Review

Normal force can be defined as coercive behavior that officers view as "necessary, appropriate, reasonable, or understandable" (Cancino, 2001). It is seen as necessary to a particular situation. The use of force to affect an arrest is a lawful action. Excessive force, which is often the basis of lawsuits, is any force exceeding that necessary to make a lawful arrest (Alpert & Smith, 1994). Allegations of excessive force in policing have been cited as one of the most frequent claims filed against the police in arrest situations (Ross, 2002). Plaintiffs won in 63% of researched cases filed involving police shootings, and the average award was \$1,327,927 (Ross, 2002).

In 1998, The Human Rights Watch published *Shielded from Justice*, a report on its 2.5-year study of police brutality and accountability in the United States. It examined several major cities but did not receive the information necessary to isolate physical use-of-force situations from other brutality issues. Although this distinction was not made, the results still may raise concern if use-of-force abuse is only statistically reported a small percentage of the time.

The Office of the City Attorney of Los Angeles reported that between 1991 and 1995, the city paid approximately \$79.2 million in judgments, awards, and pre-trial settlements against police officers (Harrington et al., 1998). The Christopher Commission examined 83 successful lawsuits, alleging excessive or improper force and involving a payment of at least \$15,000, and found that most of the cases involved clear and often egregious misconduct (Human Rights Watch, 1998). Chicago bundled their settlements to include excessive force, false arrest, and improper search allegations, equaling 1,657 cases between 1992 and 1997 (Human Rights Watch, 1998).

Reports prepared by Detroit's City Councilman, Mel Ravitz, indicated that Detroit paid out \$117 million between 1987 and 1997 and Indianapolis paid \$745,424 for 21 settlements between 1994 and 1996 (Human Rights Watch, 1998). Atlanta's City Attorney's Office claims to not maintain readily accessible data on city payouts and therefore had to ask staff members to recall settlements and rewards from 1994 to 1997: \$677,368 for those cases in 1994 and 1995, and those from 1996 through 1997 totaled just over \$1 million (Human Rights Watch, 1998).

Women's Emergence in Policing

Women were initially allowed to serve as officers for nonaggressive and nonthreatening roles, such as counselors, and the more involved and protective roles of patrol officers were reserved for the dominant, aggressive male (Schulz, 1995). Since the passage of the Equal Employment Opportunity Act in 1972, however, women have continued to enter male-dominated professions such as police work (Lanier, 1996). A female police officer's attitude and evolution of the perception of the tough cop can perhaps be summarized by a quote from Moore (2004): "There's a militaristic culture in most law enforcement agencies. Power, image, use of force. It's a very authoritarian attitude. But good policing isn't in the shoulders; it's in the head."

It may be concluded from the literature that history reveals a stereotypical image of a policeman, and that image contributes to the attitudes and perceptions of officers today. Approximately 50 years ago, William Westley pioneered a study on the special characteristics of police work. Cancino (2001) conducted a study to comparatively examine what changes in policing, if any, had occurred since Wesley's study took place. Cancino found that not only has there been a lack of change in attitude and practice of excessive and violent force but that the research signals a much needed reassessment of the patrol culture.

Prior to 1989, most federal circuit courts followed the 14th Amendment's substantive due process "shocking to the conscience" standard enunciated by the Second Circuit in *Johnson v. Glick*. In this case, the subjective mental state of the offending officer was relevant in determining whether an actionable injury occurred. This resulted in ambiguity in police misconduct cases regarding the standard of evaluation for claims of excessive force. In 1989, that ambiguity shifted in a clarification attempt in the ruling of *Graham v. Conner*. In this case, the United States Supreme Court determined that "objective reasonableness" is the 4th Amendment standard to be used in evaluating claims of excessive force. *Graham* only applies to persons at liberty. Although there is no precise application for the reasonableness test, the Court examines the facts and circumstances of each case independently.

A major fallacy of this standard is that while officers may apply one level of reasonableness to a use-of-force situation, those officers are rarely seated on the jury that determines that reasonableness. A "reasonable person" civilian is sure to view force differently than the "reasonable person" officer. Each Circuit Court appears to adhere to its own set of criteria when determining excessive force, while relying on previous case law. Although police shootings are statistically rare, lawsuit reaction is almost guaranteed. Police prevailed in 80% (n=221) of cases analyzed between 1989 and 1999 (Ross, 2002).

Skolnick and Fyfe (1994) depicted and described unnecessary violence as having two components: (1) brutality and (2) unnecessary force. They describe *brutality* as “a conscious and venal act committed by officers who usually take great pains to conceal their misconduct,” while *unnecessary force* is described as “ineptitude or insensitivity, such as when well-meaning officers unwisely charge into situations from which they can extricate themselves only by using force . . . unnecessary force may be a good faith police mistake” (Alpert & Smith, 1994). Carl Klockers defined excessive force as “the use of any more force than a highly skilled police officer would find necessary to use in that particular situation” (as cited in Alpert & Smith, 1994).

It is clear that force, justified or unnecessary and excessive, can take several definitions and is subject to numerous interpretations. Although research is beneficial and imperative, it is a result of objective tabulations and subjective speculations and is based on hindsight and retrospective analysis. Without nationally recognized standards and definitions, as well as equal interpretation among the courts, the application of, and retribution for, the use of force will continue to be a vague puzzle with various outcomes. The studies presented here have examined various aspects of law enforcement. It seems apparent that past research lacks specific studies addressing police officer perceptions toward the use of force.

Past Research

Prior studies have limited strengths and substantial weaknesses for identifying the characteristics of officers and suspects who use force and environments and police organizations in which force is used (Garner, Maxwell, & Heraux, 2002). Suspect characteristics have been studied as a cause of the use of force, as well as the degree of force. A central concern of research in regard to this aspect has been race. Research has focused on whether the police have used force on Hispanics and African Americans more than White Americans. One study showed that Hispanics account for the largest number of use-of-force cases at 64.9% with Whites at 19.4% and Blacks at 15.1% (Terrill, 2003). Race also tends to play a role in citizens’ observations of police performance. One study showed that 18% of non-White respondents were not satisfied with police performance in contrast to only 6% of White respondents (Son, Tsang, Rome, & Davis, 1997). A major area of dissatisfaction appeared to be a lack of respectful treatment in a face-to-face encounter with a police officer. Respondents’ dissatisfaction generally appeared to be significantly higher when there was an observation of the use of force by the police.

Suspect’s sex has also been studied as a precipitator to the use of force as well as to the degree of force used. Female suspects have been shown to receive less force than male suspects. One study revealed that the effect of a suspect’s sex on the use of force is one of the most consistently measured factors (Garner et al., 2002). Explanations offered for this centered around physical size, disparities, as well as the resistance offered. The female suspect aspect also relates to the type of crime committed. The more violent the crime and the greater likelihood of officer injury, the more significant the level of force.

A surprising finding in one study was that the police use less, not more, physical force if the suspect is a member of or associated with a gang (Garner et al., 2002). Without surprise, it has been found that suspects’ resistance increases

proportionally to the amount of force used. Suspects who display an antagonistic manner but no physical force received a higher degree of force by police than suspects displaying a civil demeanor. Suspects who used physical force compared to suspects who displayed a civil demeanor increased the odds of police using physical force by 1,800% (Garner et al., 2002).

Research on gender has revealed that female officers use less force and receive fewer officer complaints than male officers. In one study, female officers accounted for only 1.6% of the use-of-force reports filed while the male officers accounted for 98.4% (Terrill, 2003). While White officers tend to use force more often, minority officers tend to receive more officer complaints.

Officer's experience appears to be a factor, revealing that officers with less than 5 years of experience account for 50% to 75% of all use-of-force reports generated. Two factors that tend to skew officer characteristic findings are that females usually account for 10% or less of the personnel, and that less than one-fourth of the officers account for over one-half of all use-of-force reports (Terrill, 2003). Officers with some college, but no degree, represent the largest percentage of force reports followed by those with a bachelor's degree (a 50% reduction).

"Males have existed in a role of machismo, or hyper masculinity. This is the value system that celebrates male physical strength, aggression, violence, competition, and dominance. It denigrates the lack of these qualities as weak, female behavior" (Benson, 2000, p. 682). Machismo is slow to die in the police organizational culture, but its digression is being heard louder each day by police departments, city officials, and community members. Research in the United States and internationally has clearly demonstrated that female officers rely on a style of policing that uses less physical force, are better at defusing and de-escalating potentially violent confrontations, and are less likely to become involved in problems involving the excessive use of force (Lonsway, 2000).

Studies in the 1980s and early 1990s (Belknap & Shelley, 1993; Grennan, 1987; Harrington, 1999) have shown women to be more effective than men in many areas of policing. Women police officers rely more on verbal skills than violence. They have been repeatedly determined to be more effective in handling female victims of violence, as in a 1983 study of the performance of women in the Los Angeles Police Department (Hickman, 1983). Hickman found that women had superior communication skills, field tactics, initiative, and self confidence and were more adept at public relations.

In 1989, Sean Grennan studied 3,515 complaints filed against the New York Police Department. Women officers received fewer complaints, were less inclined to use deadly force, and were involved in fewer shooting incidents, even though they were involved in just as many violent confrontations as their male counterparts. Grennan concluded, . . .

The reality of the information related to the (lower) proportion of shooting incidents involving female officers and the (lower) number of civilian complaints against female officers is that these figures have remained, consistently, at the same levels for the past 7 years. This seemed to indicate

that female officers have not accepted the overly aggressive style of policing that has become the trademark of most male officers. (Spillar, 1991)

Research over the last three decades indicates that women officers have a less authoritarian and aggressive policing style and use force less often than male officers. In the 1970s, Louis J. Sherman, in his research on women in policing, stated that no research has shown that strength is related to an individual's ability to successfully manage a dangerous situation. Balkin (1988) reported that policemen see police work as involving control through authority, while policewomen see it as public service. Balkin even went as far as to say that women's orientation is more likely to result in better relations with the public and a better image of the police department. In 1974, an expansive study by Peter Block and Deborah Anderson found that the female officer is more likely than a male officer to calm a potentially violent situation and avoid injury to the participants.

The 1991 Christopher Commission studied use of force in the Los Angeles Police Department. The commission stated "virtually every indicator examined establishes that female LAPD officers are involved in excessive use-of-force at rates substantially below those of male officers. There were no female officers among the 120 officers with the most use-of-force reports." The commission also looked at the top 10% of the LAPD officers ranked by the combined use-of-force reports, personnel complaints, and officers involved shootings and determined there were no female officers among the top 132 officers. This lack of females within this group may have to do with female officers' perception toward the use of force and how it differs from that of male officers, as this study suggests.

Penny Harrington, a former police chief in Portland, Oregon, and founding director and chair of the board for the National Center for Women and Policing, feels strongly about the capabilities of women in law enforcement. She was quoted in the *Christian Science Monitor* as saying "policing is not upper body strength; it is the ability to think and act. If women knew that real policing is typically problem-solving, handling family situations and neighborhood disputes—all things that many women are very good at doing—then you'd get more women into police work" (as cited in Holmstrom, 2000).

Texas, the second largest state in the United States, ranks third in the nation for sworn and nonsworn employees in local and state agencies, yet the percentage of sworn female officers in larger agencies ranges from 2% to 18%, while in some smaller agencies, they are nonexistent (Greene & del Carmen, 2002). In January 2002, officials at the National Center for Women and Policing in Los Angeles claimed that in departments with more than 100 officers, women represented only 13% of the workforce (Hockensmith, 2002).

It appears from the literature that one could conclude that women have a place in law enforcement and offer a variety of characteristics beneficial to the departments that employ them, as well as the communities they serve. The trend suggests that women are less forceful, less aggressive, more capable of maintaining composure, and more appreciated by female victims of violence. The literature suggests that a confirmation of the suggested beliefs is warranted, with a probe into the specific characteristics that divide male and female officers and the root causes and influences of these differential characteristics.

Methodology

This research utilized a cross-sectional, analytic survey with a mailed questionnaire containing 26 topic questions and 10 demographic questions. The survey form was developed based on gaps in the literature, approved by the IRB, and pilot-tested on the local university police department consisting of 30 sworn police personnel (27 males and 3 females). Each department's participation in the study was obtained by contact with either the chief or a designated assistant. The survey was distributed to agencies across the United States for the purpose of determining the respondents' perceptions toward gender differences in the use of force. The instrument was designed with responses on a 6-point scale, indicating the degree of the respondent's agreement with each item.

In 2002, the National Center for Women and Policing (NCWP) published findings from its 2001 study that estimated the percentage of total sworn women officers in large agencies employing over 100 officers to be approximately 12.7% (Lonsway et al., 2003). The departments chosen for this survey were systematically selected from this list consisting of agencies that met or exceeded the above percentage and were in geographically representative states. Departments were asked that only sworn law enforcement personnel participate in the survey.

Initially, a request for participation was sent to seven departments: (1) Saginaw, Michigan, (2) Boulder, Colorado, (3) Appleton, Wisconsin, (4) Concord, California, (5) Denton, Texas, (6) Framingham, Massachusetts, and (7) Spartanburg, South Carolina. Saginaw declined participation, and Boulder returned the questionnaires undistributed. The sample then consisted of five agencies with a sample of 629 officers.

Sample Departments

Appleton, Wisconsin, has a population of 72,000, and its police department consists of 105 officers. They have 90 male officers and 15 female (14%) officers. Appleton was chosen to represent the Northern United States and due to the fact that it has 14% female officers. Concord, California, has a population of 127,600, and its police department has 155 officers. They have 128 male officers and 27 female (17.4%) officers. Concord was chosen to represent the West Coast and participated with the highest female officer percentage in the survey. The city of Denton, Texas, has a population of 96,200 with a police force of 140. Denton has the smallest female officer percentage among those surveyed with 7%. There are 130 males and 10 females. Denton represents the central and southern United States. Framingham, Massachusetts, has a population of 65,598 with a police force of 112 officers. They have 100 males and 12 females (10.7%) and represent the northeastern coast. Spartanburg, South Carolina, has a population of 39,407, and a police department with 117 sworn officers. With 14.5% female officers, 17 females and 100 males, it has the second highest female officer percentage in the survey and represents the southeastern coast.

Findings

The 629 officers in the sample departments were comprised of 548 males and 81 females, constituting a sample with 13% female officer representation. Of the surveys distributed, 317 were returned for a 50% response rate. The returned surveys included 49 female respondents for a 15.4% female response.

The Concord, California, Police Department had 71 males and 19 females respond, which was a 46% departmental and 70% female response, respectively. Spartanburg, South Carolina, had a departmental response of 17% (18 males) and 12% female (2) response. The third department, Framingham, Massachusetts, had a 77% departmental (75 males) and 92% (11) female officer response. Denton, Texas, responded with 42% (54 males) for the department and 50% female officers (5). The fifth department, Appleton, Washington, had 81 respondents for 77%, of which 69 were male and 12 females (80%). Obviously short of a 100% response rate, the national average for current female officers within departments was obtained.

Once the survey was returned, the survey questions were divided into three categories of questions addressing the three hypotheses. Table 1 includes seven questions relating to the following hypothesis: "The attitudes of male and female officers are different toward the capabilities of females performing their job."

Table 1. Means & T-Test Results for Attitudes Toward Females Performing Police Duties

Table variable	Male	Female	P-Value
Female officers are too lenient.	4.68	4.71	0.836
Female officers are just as capable of making arrests as male officers.	2.04	1.59	.015*
Female officers handle domestic disputes better than male officers.	4.64	4.33	0.065
Female officers perform tasks as effectively as male officers.	2.13	1.80	.035*
Female officers perform tasks more effectively than male officers.	4.79	4.06	.000**
Most female officers are not tough enough to properly do the job.	4.64	5.06	.026*
Female officers are more calm and polite than male officers in dealing with uncooperative subjects.	4.45	3.71	.000**

*significant at .05

**significant at .01

At the significance levels indicated, five of the seven statements included in this table have statistical significance. This can be interpreted that female officers perceive more strongly that they are as capable as males to make arrests and perform tasks as effectively as male officers. They more significantly disagree that they are not tough enough to properly do the job.

One of the variables, "Female officers are just as capable of making arrests as male officers," had a mean of 2.04 for males and 1.59 for females, showing that females more strongly agree with the statement. The t-test resulted in a p-value of .015. The next statement, "Female officers perform tasks more effectively than male officers" showed a p-value of .035 from the male and female mean of 2.13 and 1.80, respectively. The last variable in this group stated, "Most female officers are not tough enough to properly do the job." Males had a mean of 4.62, and females had 5.06, indicating stronger disagreement by females; the p-value was .026.

Two other variables in Table 1 show significant gender differences. "Female officers perform tasks more effectively than male officers" resulted in a male mean of 4.79 and a female mean of 4.06. Female officers agreed more aggressively to this question. The p-value was .000. Females agreed more definitively than males to "Female officers are more calm and polite than male officers in dealing with

uncooperative subjects.” The female mean was 3.71, while the male mean was 4.45. This question also had a p-value of .000.

Two variables in Table 1 showed no statistical significance. “Female officers are too lenient” had a male mean of 4.68 and a female mean of 4.71. The t-test revealed the p-value to be .836. Similarly, the variable, “Female officers handle domestic disputes better than male officers,” was not significant with a p-value of .065. The male and female mean used for this t-test was 4.64 and 4.33, respectively.

Table 2 includes 17 variables that relate to the second hypothesis: “Male and female officers attitudes’ differ toward the use of force.” The t-test for this set of variables revealed two that showed significance at the .05 level and six that showed significance at the .01 level. The first of these, “Most situations can be resolved without physical force,” showed a male mean of 1.75 and a female mean of 2.04. The t-test resulted in a p-value of .026. The other variable in Table 2 showing statistical significance at .05 was in response to “Training should be developed to help officers find verbal solutions to situations, rather than resorting to physical force.” This resulted in a male mean of 2.71 and a female mean of 3.18. This test offered a p-value of .018.

Table 2. Means & T-Test Results for Attitude Toward Force by Gender

Table Variables	Male	Female	P-value
Most situations can be resolved without physical force.	1.75	2.64	.026*
Officers who cuss at subjects cause situations in which they must use physical force.	3.19	3.31	0.517
I have observed physical force by fellow officers that I felt was premature or unnecessary.	3.55	3.27	0.185
If a subject is being difficult, I prefer to get to a solution quickly by using physical force.	4.40	4.45	0.781
Male officers prematurely engage in physical force with subjects.	4.76	3.98	.000**
Female officers respond to calls wanting to mediate a resolution, not use physical force.	3.66	2.92	.001**
Male officers are too quick to use physical force.	4.73	4.20	.005**
Male officers respond to “hot” calls wanting to “kick ass.”	4.39	3.82	.002**
Female officers are equally capable of controlling a physical fight between two subjects as male officers.	3.25	2.65	.002**
Female officers try to avoid physical force contact on calls at all costs.	4.62	4.63	0.944
Female officers are better at resolving conflicts without force than male officers.	4.33	3.45	.000**
A female officer is too slow to use physical force.	4.57	4.65	0.062
Situations can be resolved without using physical force all of the time.	5.30	5.00	0.127
Male officers need to practice more patience to handle situations without resorting to physical force.	4.45	4.18	0.061
I have initiated physical force on a lot of my calls.	4.97	4.84	0.395
In the past year, an excessive force complaint was made against me.	5.69	5.55	0.381
Training should be developed to help officers find verbal solutions to situations, rather than resorting to physical force.	2.71	3.18	.018*
I spend time talking out a situation with a subject rather than resorting to physical force.	2.14	2.04	0,55

*significant at .05

** significant at .01

It is shown in Table 2 that six other variables had statistical significance at the .01 level. First, "Male officers prematurely engage in physical force with subjects" resulted in a male mean of 4.76 and a female mean of 3.98. These means entered into a t-test gave a p-value of .000. Next, "Female officers respond to calls wanting to mediate a resolution, not use physical force" had male and female means of 3.66 and 2.92, respectively. The p-value was .001. The next one showing significance at the .001 level, "Male officers are too quick to use physical force," had a male mean of 4.73, a female mean of 4.20, and a p-value of .005.

Another variable in Table 2 consistent with statistical significance at the .001 level was "Male officers respond to 'hot' calls wanting to 'kick ass.'" It had a male mean of 4.39, a female mean of 3.82, and a p-value of .002. The variable, "Female officers are equally capable of controlling a physical fight between two subjects as male officers," had women agree more strongly than males, with a female mean of 2.65, a male mean of 2.65, and a p-value of .002. The last of this category, "Female officers are better at resolving conflicts without force than male officers," had a male and female mean of 4.33 and 3.45, respectively.

Nine remaining variables in Table 2 did not show any statistical significance. For the first of these, "Officers that cuss at subjects cause situations in which they must use physical force," the male mean of 3.19 and female mean of 3.31 resulted in a p-value of .517. The next variable, "I have observed physical force by fellow officers that I felt was premature or unnecessary," had a male and female mean of 3.55 and 3.27, respectively, with a p-value of .185. "If a subject is being difficult, I prefer to get to a solution quickly by using physical force" resulted in a male mean of 4.40 and female mean of 4.45. The p-value was .781.

Another variable, "Female officers try to avoid physical force contact on calls at all costs," shows a male mean of 4.62 and a female mean of 4.63. The t-test resulted in a nonsignificant p-value of .944. The next variable without significance in Table 2: "A female officer is too slow to use physical force" had a male mean of 4.57 and a mean of 4.65 for females. The p-value was .062. The next variable that showed no statistical significance at the .05 or .01 level, "Situations can be resolved without physical force all of the time," had a male mean of 5.30, a female mean of 5.00, and a p-value of .127. "Male officers need to practice more patience to handle situations without resorting to physical force" yielded a p-value of .061 from a male mean of 4.45 and a female mean of 4.18. The variable, "I have initiated physical force on a lot of my calls," presented a male mean of 4.97 and a female mean of 4.84 with a t-test result of .395. The last of this category, "In the past year, an excessive force complaint was made against me," showed a male and female mean of 5.69 and 5.55, respectively, with a p-value of .381. The variable, "I spend time talking out a situation with a subject rather than resorting to physical force," resulted in a male mean of 2.14 and a female mean of 2.04. It did not show significance as a result of the t-test. Although these variables did not reveal statistical significance at the tested levels, they are not without merit and are discussed later in the study.

Discussion and Implications

This study has addressed the differences perceived by officers in the use of force as it relates to gender. Numerous variables in this study showed statistical significance, while others did not. They are not, however, without merit. The

nonsignificant variables reflect areas of homogeneity between genders on some issues. For instance, both genders answered similarly that while they believe most situations can be resolved without physical force, force cannot always be avoided. Males and females alike agreed to having initiated force in some situations and showed no statistically significant difference in the perception that they spend time talking out situations rather than resorting to force. It should be noted that males showed a stronger affirmation toward developing training for verbal solutions than did females.

It can be seen in Tables 1 and 2 that numerous variables revealed statistically significant differences between the genders. For example, females perceive that they arrive on scene in the mediator role, while males arrive wanting to “kick ass.” The males did not perceive it the same way. It is possible this is a result of the long standing, historical culture attached to police work, defining it as a place for the tough and strong. As shown in the literature review, that stigma has been evolving, but as seen here, the evolutionary wheels seem to be spinning slowly.

Females answered more strongly toward being tough enough for the job and disagreed more adamantly about not being tough enough than did their male counterparts. Females view themselves as better at resolving conflicts than the males see them. Females tended to agree more strongly that they were not only as effective as male officers in performing tasks but more effective. While male officers did not disagree that females are capable of controlling a physical fight between two subjects, the difference in responses between the genders was enough to cause statistical significance.

A significant difference was also found between genders responding to the idea of males prematurely and too quickly using force on subjects. The females perceived more of a problem in this area than did the males. Lastly, female officers perceive that they are more capable of making arrests than male officers perceive them to be. This perception could strongly impact how male officers handle an arrest involving a female colleague.

While the survey asked for a response based on an officer’s belief or perception, one must understand that it is within this realm of perceptive reality that an officer operates. Differences found in a male and female officer’s perception of the same scene could have major impacts on the decisions, actions, and outcomes of that event.

The findings have shown that male officers do not have the same perceptions of female officers encompassing a female’s toughness for the job and her ability to perform the necessary tasks. Females, on the other hand, appear to perceive their toughness as appropriate, their ability as effective, and their communication as superior.

Studies have found women to be less costly to a department in terms of lawsuits (Terrill, 2003), and that their less physical style of policing is indicative of a needed change (Lonsway, 2000). Perhaps with some policy additions and revisions, women can continue to infiltrate the law enforcement arena, and males can begin to view them as a capable and effective part of law enforcement.

As illustrated by the survey, male officers perceived more strongly than females that training should be developed to help officers find verbal solutions

to situations. This indication alone should speak volumes to administrators, educators, and politicians—more verbal solutions, less physical force, less injury, more understanding, and quite possibly less harm.

City government needs to be aware of social needs within the police agencies so that they may properly budget for these needs. Support for the recruitment of more females should be sought, while funds must be made available to increase awareness. Funds are necessary to initiate training plans and programs to educate male officers on the benefits of female colleagues and increase skills for better communication. Administrators could view this initial step of research and its implications as a starting point for more in-depth research to be performed.

Educators could also view this possibility of perception differences as a direction for future education. If the gender differences should provide marketable traits, then harness this information and expand the knowledge base of students. Educators could provide tangible roots for mediation and subject content that could lead to less perceived differences and more nonviolent resolutions.

While this study attempted to reveal and explain some perception differences between genders about the use of force, it is limited in that it dealt only with a small number of qualified sworn officers. One could argue that there is merit to this type of research based on the number of statistically significant responses found. Perception is each person's reality, and, therefore, each officer lives within and acts upon his or her own perception. The success of a department depends on the success of its officers, and each officer's perception is a vital reality worth understanding.

References

- Adams, K., Alpert, G. P., & Dunham, R. G. (1999). *Use of force by police: Overview of national and local data*. Washington, DC: U.S. National Institute of Justice, Bureau of Justice Statistics.
- Alpert, G. P., & Smith, W. C. (1994). How reasonable is the reasonable man?: Police and excessive force. *Journal of Criminal Law and Criminology*, 85, 481-501.
- Balkin, J. (1988). Why policemen don't like policewomen. *Journal of Police Science and Administration*, 16, 24-38.
- Belknap, J., & Shelley, J. K. (1993). The new lone ranger: Policewomen on patrol. *American Journal of Police*, 12(2), 47-75.
- Benson, R. W. (2000). Changing police culture: The sine qua non of reform. *Loyola of Los Angeles Law Review*, 34, 681.
- Cancino, J. M. (2001). Walking among giants 50 years later. *Policing*, 24(2), 144-161.
- Christopher Commission. (1991). *Christopher Commission Report*. Los Angeles: Author.
- Garner, J. H., & Maxwell, C. D. (2002). *Understanding the use of force by and against the police in six jurisdictions*. Rockville, MD: National Institute of Justice.

- Garner, J. H., Maxwell, C. D., & Heraux, C. G. (2002). Characteristics associated with the prevalence and severity of force used by the police. *Justice Quarterly*, 19(4), 705-746.
- Gerber, G. L. (1996). Status in same-gender and mixed gender police dyads: Effects on personality attributions. *Social Psychology Quarterly*, 59, 350-363.
- Gerber, G. (2001). *Women and men police officers status, gender and personality*. Westport, CT: Praeger.
- Greene, H. T., & del Carmen, A. (2002). Female police officers in Texas. *Policing*, 25, 385-398.
- Grennan, S. A. (1987). Findings on the role of officer gender in violent encounters with citizens. *Journal of Police Science and Administration*, 15(1), 78-85.
- Harrington, P. E. (1999). *Challenges facing police administrators*. Portland, OR: Feminist Majority Foundation.
- Harrington, P., Besser, A., McAnney, D., Terman, S., Smeal, E., & Spillar, K. (1998). *Equality denied: The status of women in policing, 1997*. Portland, OR: Feminist Majority Foundation.
- Hockensmith, D. (2002). Police agencies look to boost female ranks. *St. Clair [Michigan] Times Herald*.
- Holman, L. (2005). Use of force. *Campus Law Enforcement Journal*, 33-36.
- Holmstrom, D. (2000). Women officers arrest the gender gap. *The Christian Science Monitor*.
- Lanier, M. M. (1996). An evolutionary typology of women police officers. *Woman and Criminal Justice*, 8(2), 35-57.
- Lersch, K. M. (1998). Exploring gender differences in citizen allegations of misconduct: An analysis of a municipal police department. *Woman and Criminal Justice*, 9, 69-80.
- Lonsway, K. A. (2000). *Hiring & retaining more women: The advantages to law enforcement agencies*. Portland, OR: Feminist Majority Foundation.
- Lonsway, K., Moore, M., Harrington, P., Smeal, E., & Spillar, K. (2003). *Hiring & retaining more women: The advantages to law enforcement agencies*. San Francisco: National Center for Women & Policing.
- Lonsway, K., Wood, M., Fickling, M., De Leon, A., Moore, M., & Harrington, P. et al. (2002). *Men, women and police excessive force: A tale of two genders*. Los Angeles: Feminist Majority Foundation.

- Mangold, A. (2003, August 20-24). *The peaceable police woman? The practice of de-escalation in the eyes of female and male police officers*. Paper presented at Gender and Power in the New Europe, the 5th European Feminist Research Conference, Lund University, Sweden.
- Moore, M. (2004). *Women reach top of police ranks, growth still slow*. Available online at www.womensnews.org
- Ross, D. L. (2002). An assessment of *Graham vs. Connor*, ten years later. *Policing*, 25(2), 294-318.
- Schulz, D. M. (1995). *From social worker to crimefighter*. Westport, CT: Praeger.
- Smeal, E., Spillar, K., & Harrington, P. (2000). *Gender differences in police brutality lawsuits: Men cost more!* Portland, OR: Feminist Majority Foundation.
- Son, I., Tsang, C., Rome, D. M., & Davis, M. S. (1997). Bradford citizens' observations of police use of excessive force and their evaluation of police performance. *Policing*.
- Spillar, K. (1991). *Testimony of Katherine Spillar, national coordinator, The Fund for the Feminist Majority*. Portland, OR: Feminist Majority Foundation.
- Spillar, K., & Harrington, P. (2000). *This is what you get when men rule roost*. Los Angeles: National Center for Women & Policing.
- Terrill, W. (2003). *Use of force analysis*. San Antonio, TX: U.S. Department of Justice.
- Terrill, W., Alpert, G. P., Dunham, R. G., & Smith, M. R. (2003). A management tool for evaluating police use of force: An application of the force factor. *Policing Quarterly*, 6, 150-171.

Lorene M. Sandifer, MA, attended the University of North Texas and earned a BA in biology. She is a licensed paramedic and served for almost 8 years as a police officer in Grand Prairie, Texas. She obtained her MA in Criminal Justice and Criminology from the University of Texas–Arlington.

O. Elmer Polk, PhD, earned his doctoral degree from Sam Houston State University and is currently an associate professor and graduate advisor at the University of Texas–Arlington. Previous research interests have primarily been in the areas of criminal justice career paths, juvenile justice, corrections, and violent crime.

Alejandro del Carmen, PhD, earned his doctoral degree from Florida State University and is currently an associate professor and the department chair of the Department of Criminology and Criminal Justice at the University of Texas–Arlington. He has published numerous articles and books with a research focus on terrorism, profiling, and police administration.

Appendix: Survey Items in Summary Form

For this survey, physical force is defined as any force beyond verbal command that results in physical contact with a civilian. (All items were answered by circling a number between 1 and 6 indicating the degree of agreement with the item, with 1 being strongly agree and 6 being strongly disagree).

1. Most situations can be resolved without physical force.
2. I have the opportunity to work with female officers on a regular basis.
3. Officers who cuss at subjects cause situations in which they must use physical force.
4. I have observed physical force by fellow officers that I felt was premature or unnecessary.
5. If a subject is being difficult, I prefer to get to a solution quickly by using physical force.
6. Male officers prematurely engage in physical force with subjects.
7. Female officers are too lenient.
8. I spend time talking out a situation with a subject rather than resorting to physical force.
9. Female officers respond to calls wanting to mediate a resolution, not use physical force.
10. Male officers are too quick to use physical force.
11. Female officers are just as capable of making arrests as male officers.
12. Male officers respond to "hot" calls wanting to "kick ass."
13. Female officers are equally capable of controlling a physical fight between two subjects as males.
14. Female officers try to avoid physical force contact on calls at all costs.
15. Female officers are better at resolving conflicts without force than male officers.
16. A female officer is too slow to use physical force.
17. Female officers handle domestic disputes better than male officers.
18. Female officers perform tasks as effectively as male officers.
19. Female officers perform tasks more effectively than male officers.
20. Most female officers are not tough enough to properly do the job.
21. Female officers are more calm and polite than male officers in dealing with uncooperative subjects.
22. Situations can be resolved without physical force all of the time.
23. Male officers need to practice more patience to handle situations without resorting physical force.
24. I have initiated physical force on a lot of my calls.
25. In the past year, an excessive force complaint was made against me.
26. Training should be developed to help officers find verbal solutions to situations, rather than resorting to physical force.

Please complete the following information about yourself.

Age: ____ years

Gender: (Please mark one.) ____ Male ____ Female

Race/Ethnicity: (Please mark one.)

____ American Indian/Alaska Native ____ Asian
____ Native Hawaiian/Pacific Islander ____ White
____ Black/African American ____ Hispanic/Latino
____ Other (please specify) _____

Current marital status: (Please mark one.)

____ Single ____ Divorced ____ Married
____ Widowed ____ Separated ____ Live-in-Partner

Highest grade of school completed: (Please mark one.)

____ High School Diploma/G.E.D.
____ Four-Year Degree (BS, BA, etc.)
____ Some College
____ Advanced Degree (MS, MA, JD, PhD, etc.)
____ Two-Year Degree (AS, AA, etc.)

Total number of years you have been employed by Police Department(s):

____ years

What division do you currently work in? (Please mark one.)

____ Uniformed Patrol ____ Detective Bureau
____ Administration ____ Special Investigative Bureau
____ Other (please specify) _____

Current Rank: (Please mark one.)

____ Police Officer ____ Captain or above
____ Lieutenant ____ Sergeant
____ Other (please specify) _____

What shift do you work most often? (Please mark one.)

____ Day Shift (early morning to late afternoon)
____ Evening Shift (early afternoon to late evening)
____ Night Shift (midnight to early morning)
____ My shift assignment rotates on a regular basis.
____ Other (Please specify.)

Do you have military experience? ____ No ____ Yes

The Relationship Between Ethical Ideology and Ethical Decisionmaking Among Experienced Police Officers

Dennis W. Catlin, PhD, Associate Professor, Department of Criminal Justice, Northern Arizona University–Tucson

James R. Maupin, PhD, Associate Professor and Department Head, Department of Criminal Justice, New Mexico State University

The literature is replete with studies that examine police ethics, integrity, and corruption (Conti & Nolan, 2005; Crank & Caldero, 2000; Houn, Hesketh, Frank, McConkey, & McGrath, 1995; Kappeler, Sluder, & Alpert, 1998; Rokeach, Miller, and Snyder, 1971; Sherman, 1982; Zhao Ni, & Lovrich, 1998). The most recent series of studies was catalyzed by the landmark study of police integrity by Klockars, Ivkovich, Harver, and Haberfeld (2000). In this study, 3,235 officers from 30 U.S. police agencies responded to 11 case scenarios describing police behavior. They were asked to rate the seriousness of the case, the severity of discipline the behavior should and would receive, and whether or not they would report the behavior. The study found “substantial differences in the environment of integrity among the 30 agencies in the sample” and that “most police officers indicated that they *would* report a colleague who stole from a found wallet or a burglary scene, accepted a bribe or kickback, or used excessive force on a car thief after a foot pursuit” (p. 2). Respondents were less likely, however, to report officers who cover up a DUI accident or accept holiday gifts from merchants.

Several subsequent studies expanded on the Klockars et al. study. Ivkovic (2005) used the data from the 3,235 U.S. officers and compared it with surveys using the same 11 case scenarios administered to 1,694 Croatian and 378 Finnish police officers. This study found “evaluations of case seriousness seem to be more heterogeneous across the three countries in the least serious cases such as the off-duty employment, the acceptance of gratuities, or the use of excessive force, and more homogeneous for the most serious cases such as the kickback, a bribe, or a theft of found property” (p. 560). This may be due to cultural variances associated with the perceptions of the seriousness of issues, such as accepting free merchandise. Similar cross-cultural studies were conducted by Huberts, Lamboo, and Punch (2003), comparing police integrity in the United States and the Netherlands, and Ekenvall (2003), comparing police behavior in Sweden, the United States, and Croatia.

These studies focus primarily on the organizational ethical environment. They provide valuable clues to the impact of the organizational environment on police ethics. While these studies are informative about the organizational environment, they do not address the personal ethics of police officers and the impact of personal ethics on ethical decisionmaking.

Statement of the Problem

While the literature on measuring integrity in some instances has examined independent variables, such as organizational environment, as they are related to responses to integrity scenarios, there is a dearth of research that looks at how a law enforcement officer's ethical and moral position is related to ethical decisionmaking as measured by responses to hypothetical ethical scenarios. This study examines this problem by measuring personal ethical orientations of experienced police officers using the Ethical Position Questionnaire (EPQ) and responses to six hypothetical ethical dilemmas

Measuring Ethical Orientation: The Ethical Position Questionnaire (EPQ)

EPQ Development

Historically there have been two major problems confronting researchers in conducting empirical research to identify personal ethical orientations: (1) identifying a theoretical framework based on accepted ethical philosophies and (2) is operationalizing that theoretical framework. In an attempt to address these problems, Forsyth and Schlenker (Forsyth, 1980; Schlenker & Forsyth, 1977) proposed that the current major schools of ethical thought could be most parsimoniously defined in terms of two major scales. The first scale draws on the two ethical philosophies of ethical absolutism and ethical relativism. The second scale focuses on ethical idealism.

The first scale is based on the proposition that in making ethical judgments, some people draw on universal ethical rules, while others reject ethical absolutes. Ethical absolutism suggests that "objective standards of moral truth exist independently of us" (Harris, 1997, p. 103) and that there "exists an eternal and unchanging moral code that transcends the physical world and is the same for all people at all times and places" (Holmes, 1998, p. 165). Ethical relativism, on the other hand, holds that there is no such thing as universal ethical truths and that ethical dimensions of right and wrong vary from person to person and culture to culture (Holmes, 1998; Polloch, 2007; Rachels, 1999).

The second scale focuses on idealism in ethical judgment. At one extreme, ethical idealists assume that "right" action will result in desirable consequences. Those who are less idealistic believe that "right" action does not always result in desirable consequences (Forsyth, 1980).

To operationalize this theoretical framework, Forsyth (1980) conducted research to develop a valid, reliable, and easily administered instrument to determine personal ethical orientations of individuals. His goal was to develop and validate an Ethical Position Questionnaire (EPQ) that would facilitate the classification of individuals according to ethical orientation (Forsyth, 1980, p. 177). Forsyth's (1980) work resulted in the development of the EPQ consisting of 20 statements. Ten of the statements concern idealism, and 10 concern relativism. A Likert-type response scale consisting of nine points from "completely disagree" to "completely agree" is used for each item. Individuals are classified as to ethical orientation by calculating their mean scores on the relativism items and the mean scores on the

idealism items. Tests of concurrent and discriminate validity as well as predictive validity were conducted. He proposed that ethical judgments can be found to lie on two major dimensions: (1) ethical idealism and (2) ethical relativism. The resulting taxonomy of ethical orientations is presented in Table 1.

Table 1. Taxonomy of Ethical Orientations

	High Relativism	Low Relativism
High Idealism	<i>Situationist</i> Rejects ethical absolutes; advocates individualistic analysis of each act in each situation; relativistic	<i>Absolutist</i> Assumes that the best possible outcome can always be achieved by following universal ethical rules; Absolutist
Low Idealism	<i>Subjectivist</i> Appraisals are based on personal values and perspective rather than universal ethical principles; relativistic; Ethical Egoist	<i>Exceptionist</i> Ethical absolutes guide judgments but pragmatically open to exceptions to these standards; Utilitarian

Adapted from Forsyth (1980)

EPQ Research in Non-Law Enforcement Professions

Subsequent to its development, the EPQ has been used and validated in ethics research among numerous professional disciplines. Studies have been conducted in accounting (Chan & Leung, 2006; Ziegenfuss & Martinson, 2002), education (Deering, 1998), medicine (Eastman, Eastman, & Tolson, 2001; Furham & Olfstein, 1997; Ganzini, Fenn, Lee, Heintz, & Bloom, 1996), business and management (Bass, Barnett, & Brown, 1999; Davis, Andersen, & Curtis, 2001), criminal justice education (Byers & Powers, 1997a, 1997b), advertising (Treise, Weigold, Conna, & Garrison, 1994) marketing and market research (Vitell, Lumpkin, & Rawwas, 1991), animal research (Wuensch & Poteat, 1998), and information technology (Winter, Stylianou, & Giacalone, 2004).

EPQ Research in Law Enforcement

Some studies have been conducted using the EPQ in the law enforcement setting. Catlin and Maupin (2002) studied the ethical orientations of a state police recruit class using the Ethical Position Questionnaire (EPQ) and compared that class to a group of state police officers with one year of experience. They found that there was a statistically significant difference in ethical orientations between the two groups. New recruits were more oriented to ethical idealism, and one-year experienced officers were more oriented to ethical relativism.

Also using the EPQ, Catlin and Maupin (2004) examined the ethical orientations of two cohorts of state police officers. The first cohort was administered the EPQ during the recruit academy and again after one year of experience. The second cohort took the EPQ when they had one year of experience and again at the two-year point in their careers. For cohort one, there was a significant shift of orientation from the idealism scale to the relativism scale. The biggest shift in ethical orientation was from an *absolutist* orientation to the *subjectivist* orientation. There was a similar but nonsignificant result for cohort two. From year one to year

two, there was a shift from idealistic orientations to the *subjectivist* ethical position. At year two, 41% of all officers occupied the *subjectivist* orientation.

Maupin, Bond-Maupin, and Catlin (2006) used the EPQ to measure the ethical orientations of local police recruits at the beginning of recruit training and again at the end of the training academy. They found a similar trend in a shift down in the idealism scale and an increase in the relativism scale.

While these studies suggest that there is a relationship between the longevity of experience in the law enforcement profession and ethical orientation, the studies did not attempt to look at the relationship between ethical orientation and ethical decisionmaking. This study is an attempt to shed some light on that research question.

Examining the Relationship Between Ethical Position as Measured by the EPQ and Ethical Decisionmaking Using Responses to Ethical Scenarios

While there are no reported studies examining this relationship between ethical position as identified by the EPQ and decisionmaking in law enforcement, there are studies in other professions and academic disciplines. These studies have had mixed results. In the following studies, the first three found a relationship between ethical orientation and responses to ethical scenarios; whereas, the third found no significant relationship.

Caswell (2003) explored the relationship between EPQ and scores on the Dilemmas in Athletic Training Questionnaire (DAT-Q) among undergraduate athletic training education students and instructors. This study found that there is a positive relationship between athletic trainers' idealism scores and their ethical decisionmaking scores on the DAT-Q and that "individuals scoring high in idealism and low in relativism (*absolutists*) reported significantly higher ethical decisionmaking scores than all other respondents" (p. 175).

Bass, Barnett, and Brown (1998) conducted a study of the relationship between ethical orientations based on the EPQ and ethical decisionmaking-based responses to three ethical scenarios administered to a random sample of American Marketing Association members who identified themselves as marketing management/sales management professionals. The first scenario concerned "allowing liking for one customer and disliking another to affect price, delivery, and other decisions regarding terms of sale." The second involved "giving physical gifts, such as free sales promotion prizes or 'purchase volume incentive bonuses' to a customer." The third scenario concerned "gaining information about competitors by asking buyers for specific information about these competitors" (p. 7).

This study (Bass et al., 1998) found that sales managers' ethical judgments of the scenarios were related to the *absolutist*, *subjectivist*, *exceptionist*, or *situationist* ethical orientation. The only significant relationship was with the first scenario. Judgment of the first ethical scenario was significantly different from the other three orientations. They judged it to be more unethical. The researcher then combined the results for the ethical positions of *absolutists* and *situationists*, both of which are high on the idealism scale. The resulting analysis indicated that the high

idealism positions were harsher on the first and third scenarios, suggesting that idealism explained differences more than relativism.

Byers and Powers (1997b) examined the relationship between ethical ideology and responses to two versions of a vignette designed to focus on the question of loyalty among actors within organizations. The subjects of this research were criminal justice and non-criminal-justice majors in a Midwestern university. They found that *absolutists* and *situationists* perceived the act of being disloyal and truthful more important than the reverse of being loyal even if it involved lying. *Subjectivists* perceived lying and loyalty more positively than honesty combined with disloyalty. There was not a significant relationship for *exceptionists*.

Eastman et al. (2001) measured the relationship between ethical ideology using the EPQ and four managed care ethical dilemmas among physicians. They found no significant relationship between ethical ideology and the ethical dilemmas.

Method

Research Question

For purposes of this study, we posed the following research question: Is there a relationship between the four ethical orientation categories of *situationists*, *exceptionists*, *subjectivists*, and *absolutists* as measured by the EPQ and the six hypothetical ethical scenarios designed specifically for this study?

Participants and Instruments

One hundred seventy-seven experienced law enforcement officers attending advanced training academy workshops completed the EPQ developed by Forsyth (1980) and used successfully in subsequent studies (Byers & Powers, 1997b; Forsyth, Nye, & Kelly, 2001; Henle, Giacalone, & Jurkiewicz, 2005; Treise et al., 1994). We also used six separate hypothetical ethical dilemmas. The officers were asked to indicate agreement or disagreement with the outcome of each. The six hypothetical dilemmas were developed with the assistance of experienced police officers, police supervisors, commanders, and trainers. One hypothetical dilemma, Hypothetical 6, was adapted from Jetmore (1997) and reviewed by a SWAT commander. They were pilot tested in conjunction with the EPQ with training commanders and training officers at a regional law enforcement academy. The six hypothetical dilemmas covered specific areas in the professional and personal lives of law enforcement officers. These areas included testifying in court (Hypothetical 1), responding to public questions (Hypothetical 2), personal family relationships (Hypothetical 3), tactical/operational decisions (Hypothetical 4), interactions between commanders and supervisors (Hypothetical 5), and interactions between line officers and commanders (Hypothetical 6). The hypothetical dilemmas are available in the Appendix.

Table 2 displays characteristics of the participating officers. The average age was 39.15 years, and the average years of service was 12.58 years. Twenty (11.3%) were female, and 157 (89.7%) were male. Anglos comprised 61.58 % (n=109) of the population, and non-Anglos represented 38.42%. The highest level of education of 52 officers was a bachelor's degree (30.2%); 6 (3.39%) possessed a graduate degree

ranging from a master to a juris doctor to a PhD; 93 (52.54%) officers had earned some college credit; and 26 (14.69%) possessed a high school/GED degree only.

Table 2. Characteristics of Participants

Characteristic	N
Number	177
Average Age	39.15
Average Years of Service	12.58
Males	157
Females	20
Anglos	109
Hispanics	49
African-Americans	7
Other Ethnicity	12
High School Graduate/GED	26
Some College	93
Bachelor's Degree	52
Graduate Degree	6

Analysis and Results

The ethical position questionnaire was split into the two halves measuring the primary ethical dimensions of idealism and relativism. Table 3 displays the descriptive statistics of our analysis of these two ethical dimensions. The mean Idealist score was 51.46 (median = 49), and the mean Relativist score was 47.37 (median = 48). As with prior research (Byers & Powers, 1997a; Forsyth, 1980), we analyzed these two dimensions and found no statistically significant correlation between the scores on these two dimensions.

Table 3. Idealism and Relativism Scores

Mean	Median	Mean	Median
Idealism	Idealism	Relativism	Relativism
51.46	49.00	47.37	48.00

Next, we adapted the technique of others (Byers & Powers, 1997a; Forsyth, 1980; Hadjistavropoulos, Malloy, Sharpe, & Fuchs-Lacelle, 2003; Treise et al., 1994) to distribute the respondents across the four ethical orientation categories. We used the actual as opposed to the theoretical midpoint of the Likert response options to place the respondents into the four ethical orientation categories.

We also compared the four ethical positions with the agree/disagree responses of the officers to the six hypothetical dilemmas. The results of that analysis are displayed in Table 4.

Table 4. Comparison of Ethical Position with Response to Hypothetical Ethical Dilemmas

Variable	Hypothetical #1		Hypothetical #2		Hypothetical #3		Hypothetical #4		Hypothetical #5		Hypothetical #6	
	Agree	Disagree	Agree	Disagree	Agree	Disagree	Agree	Disagree	Agree	Disagree	Agree	Disagree
Situationist (%)	9 (19.6)	37 (80.4)	39 (84.8)	7 (15.2)	32 (71.7)	13 (28.3)	31 (67.4)	15 (32.6)	27 (58.7)	19 (41.3)	20 (43.5)	26 (56.5)
Absolutist (%)	10 (27.8)	26 (72.2)	21 (58.3)	15 (41.7)	22 (61.1)	14 (38.9)	19 (52.8)	17 (47.2)	17 (52.8)	19 (47.2)	9 (25.0)	27 (75.0)
Subjectivist (%)	16 (29.1)	39 (70.9)	49 (89.1)	6 (10.9)	41 (74.5)	14 (25.5)	33 (60.0)	22 (40.0)	36 (65.5)	19 (34.5)	16 (29.1)	39 (70.9)
Exceptionalist (%)	7 (17.5)	33 (82.5)	31 (77.5)	9 (22.5)	31 (77.5)	9 (22.5)	15 (37.5)	25 (62.5)	21 (52.5)	19 (47.5)	13 (32.5)	27 (67.5)

The analysis revealed two statistically significant relationships. Hypothetical #2 and #4 are related to the ethical orientation categories (Chi-Square for Hypothetical #2=13.670, $p \leq 0.05$; Chi-Square for Hypothetical #4=9.473, $p \leq 0.05$). For Hypothetical #2, 84.8% of *situationists* (n=39), 58.3% of *absolutists* (n=21), 89.1% of *subjectivists* (n=49), and 77.5% of *exceptionists* (n=31) agreed with the resolution of Hypothetical #2. For Hypothetical #4, 67.4% of *situationists* (n=31), 52.8% of *absolutists* (n=19), and 60% of *subjectivists* (n=33) agreed. (62.5%). *Exceptionists* tended to disagree with the resolution of Hypothetical #4.

We isolated the responses to Hypotheticals #2 and #4. The distribution of responses for these two hypothetical dilemmas appear in Table 5. A further analysis of the relationship of ethical position to the responses to Hypotheticals #2 and #4 was conducted using Pearson Correlation analysis.

Table 5. Comparisons Between Ethical Orientation and Hypotheticals #2 and #4

Ethical Position	Hypothetical #2 Response to Public		Hypothetical #4 Tactical Operational	
	Agree	Disagree	Agree	Disagree
Situationist	39 (84.8)	7 (15.2)	31 (67.4)	15 (32.6)
Absolutist	21 (58.3)	15 (41.7)	19 (52.8)	17 (47.2)
Subjectivist	49 (89.1)	6 (10.9)	33 (60.0)	22 (40.0)
Exceptionist	31 (63.2)	9 (22.5)	15 (37.5)	25 (62.5)

For Hypothetical #2, there is a moderately weak negative relationship between *absolutists* and Hypothetical #2 ($r = -.258, p < .05$) and a weak positive relationship between the hypothetical dilemma and *subjectivists* ($r=.165, p < .05$). For Hypothetical #4, there is a weak negative relationship between *situationists* and the hypothetical dilemma ($r=-.163, p < .05$) and a weak positive relationship between the hypothetical dilemma and *subjectivists* ($r=.184, p < .05$).

Discussion

There were no significant relationships between ethical positions and four of the six hypotheticals. The only relationships identified were with respect to Hypotheticals #2 and #4.

Hypothetical #2

Hypothetical #2 dealt with responding to public questions in which the officer did not tell the truth to the parents about how their daughter died in an automobile accident. The analysis suggests a relationship between this hypothetical and the *absolutist* and *subjectivist* ethical positions. It also suggests that *absolutists* are less likely to agree with the outcome, not telling the truth, than non-absolutists. In addition, *subjectivists* are more likely to agree with the outcome than non-subjectivists.

Truth-telling, no matter what the consequences, is closely associated with moral absolutism. Ethical absolutists believe that there are universal unchanging ethical rules and that persons should obey these rules, regardless of the consequences (Harris, 1997). Ethical absolutism is associated with a deontological system of ethics.

Deontological systems of ethics are concerned only with whether or not the act is “right.” If the act is right, it is ethical regardless of the ultimate consequences of the act; therefore, whether the outcome is good or bad is non-consequential (Holmes, 1998; Polloch, 1998). In the case of truth telling, moral absolutists would view truth telling as important no matter what the outcome. A fundamental principle of non-consequential (deontological) ethics is that one cannot tell what the outcome of an act will be, so there is an imperative to act morally, in this case to tell the truth, because it is the moral thing to do without regard to whether the outcome is good or bad. Emmanuel Kant (as cited in Souryal, 1992) would view telling the parents the truth as an act of respect for the parents. Kantian ethics, a form of moral absolutism, suggests that the parents, and all human beings, should be treated “with dignity, and impartiality, regardless of what we may gain or lose from the relationship” (p. 167). This principle is frequently referred to as Kant’s “respect for persons” categorical imperative. In the case of this hypothetical dilemma, telling the truth to the parents shows respect for them since they have the right to know what really happened.

The analysis suggests that *subjectivists* are more likely to agree with the outcome than non-subjectivists. In this case, the *subjectivist* would agree that not telling the truth to the parents was the correct moral action. The *subjectivist* is high on the relativism scale and low on the idealism scale. The *subjectivist* is very closely associated with the school of ethical thought known as ethical egoism. Ethical egoism is a version of consequential (teleological) ethics (i.e., the ethics of means and ends) (Souryal, 1992). In this case, the moral judgment is based on what end would best serve the officer. Rachels (1999) suggests that “according to ethical egoism, there is only one ultimate principle of conduct, the principle of self-interest, and this principle sums up all of one’s natural duties and obligations” (p. 84). It is not surprising that ethical egoism might come into play by officers in interactions with the public. A good share of police training focuses on protecting oneself physically and emotionally.

Hypothetical #4

This hypothetical dilemma dealt with a tactical/operational decision in which a SWAT officer follows orders to fire a CS grenade into a building where young children are being held hostage. It is possible that the CS gas could kill one or more of the young children. In this case, the analysis suggests that *situationists* are less likely to agree with the outcome of Hypothetical #4 than non-situationists. Also, *subjectivists* are more likely to agree with the outcome of than non-subjectivists.

This dilemma presents one of the most difficult choices for police officers who are trained, like the military, to follow orders. Polloch (2004) captures the question as follows: “Is an individual excused from personal moral decisionmaking when following orders, or should one disobey orders that one believes to be illegal or immoral?” (p. 28).

In this hypothetical dilemma, *situationists* are less likely to agree that the officer acted morally in firing the CS grenade. *Situationists*, while high on the relativism scale, also are high on the idealism scale. The *situationist* “distrusts absolute moral principles and argues instead that each situation must be examined individually” (Forsyth, 1980, p.176). Ethical ideals are, however, applied in judging each situation. The *situationist* holds that love or *agape* is intrinsically good. Agape love is a higher love that acknowledges all people are part of God’s creation and should be treated as such (Fletcher, 1966). The *situationist* would ask, “What in this concrete situation would be

the most loving act?" (Holmes, 1998, p. 198). The participants in this study who were oriented toward the *situationist* position appear to have rejected the easy solution, which was to follow the orders of the superior. To some extent, they appear to have taken into account the possibility of killing innocent children and rejected the possible consequences associated with disobeying an order based on their moral position.

In this hypothetical dilemma, the *subjectivists* (egoists) agree with the officer's decision to follow orders and launch the grenade. The motivation of the *subjectivist* is based on an ethical analysis that focuses on the consequences and the best personal outcome for the officer. Disobeying an order rarely has a positive personal outcome in a military or paramilitary organization.

Limitations

While this sample of 175 experienced police officers was sufficient to carry out a robust analysis, it was a convenience sample, and it represented police officers from a specific regional area of the country. Larger samples from additional studies are required to determine whether the outcomes of this study can be replicated. Hypothetical ethical dilemmas are just that. They are hypothetical. They can only minimally replicate real-life situations. Only general assumptions can be made about the ethical motivation of participants in this type of study. In-depth interviews would be required to assess the nature of the ethical motivations.

This study suggests that there may be some relationship between personal ethical orientations as measured by the EPQ instrument. Additional studies using other instruments measuring personal ethical position would further inform the results of this study.

References

- Bass, K., Barnett, T., & Brown, G. (1998). The moral philosophy of sales managers and its influence on ethical decision making. *Journal of Personal Selling and Sales Management, 18*(2), 1-17.
- Bass, K., Barnett, T., & Brown, G. (1999). Individual difference variables, ethical judgments, and ethical behavior intentions. *Business Ethics Quarterly, 9*, 183-205.
- Byers, B., & Powers, W. B. (1997a). Ethical orientations and criminal justice: The effects of major and gender. *Journal of Criminal Justice Education, 8*, 162-179.
- Byers, B., & Powers, W. B. (1997b). Criminal justice and ethical ideology: An exploration of a loyalty-truthfulness dilemma. *Journal of Criminal Justice, 25*, 527-540.
- Caswell, S. V. (2003). *Individual moral philosophies and ethical decision-making of undergraduate athletic training education students and instructors*. Unpublished doctoral dissertation, Ohio University, Athens.
- Catlin, D. W., & Maupin, J. R. (2002). Ethical orientations of state police recruits and one-year experienced officers. *Journal of Criminal Justice, 30*, 491-498.

- Catlin, D. W., & Maupin, J. R. (2004). A two cohort study of the ethical orientations of state police officers. *Policing: An International Journal of Police Strategies & Management*, 27, 289-301.
- Conti, N., & Nolan III, J. J. (2005) Policing the platonic cave: Ethics and efficacy in police training. *Policing & Society*, 15(2), 166-186.
- Crank, J. P., & Caldero, M. A. (2000). *Police ethics*. Cincinnati, OH: Anderson.
- Chan, S. Y. S., & Leung, P. (2006). The effects of accounting students' ethical reasoning and personal factors on their ethical sensitivity. *Managerial Accounting Journal*, 21, 436-457.
- Davis, M. A., Andersen, M. G., & Curtis, M. B. (2001). Measuring ethical ideology in business ethics: A critical analysis of the Ethics Position Questionnaire. *Journal of Business Ethics*, 32, 35-53.
- Deering, T. E. (1998). The ethical perspective of British and American pre-service teachers. *Educational Research*, 40, 353-358.
- Eastman, J. K., Eastman, K. L., & Tolson, M. A. (2001). The relationship between ethical ideology and ethical behavior intentions: An exploratory look at physicians' responses to managed care dilemmas. *Journal of Business Ethics*, 31, 209-224.
- Ekenvall, B. (2003). Police attitudes toward fellow officers' misconduct: The Swedish case and a comparison with the USA and Croatia. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 3(2), 210-232.
- Fletcher, J. F. (1966). *Situation ethics*. Philadelphia: Westminster.
- Forsyth, D. R. (1980). A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology*, 39, 175-184.
- Forsyth, D. R., Nye, J. L., & Kelly, K. (2001). Idealism, relativism, and the ethics of care. *The Journal of Psychology*, 122(3), 243-248.
- Furham, A., & Olfstein, S. J. (1997). Ethical orientation and the allocation of scarce medical resources. *British Journal of Medical Psychology*, 70, 51-63.
- Ganzini, L., Fenn, D. S., Lee, M. A., Heintz, R. A., & Bloom, J. D. (1996). Attitudes of Oregon psychiatrists toward physician assisted suicide. *American Journal of Psychiatry*, 153, 1469-1475.
- Harris, C. E. (1997). *Applying moral theories*. Boston: Wadsworth.
- Hadjistavropoulos, T., Malloy, D. C., Sharpe, D., & Fuchs-Lacelle, S. (2003) The ethical ideologies of psychologists and physicians: A preliminary comparison. *Ethics & Behavior*, 13(1), 97-104.
- Henle, C. A., Giacalone, R. A., & Jurkiewicz, C. L. (2005). The role of ethical ideology in workplace deviance. *Journal of Business Ethics*, 56, 219-230.

- Holmes, R. L. (1998). *Basic moral philosophy*. Boston: Wadsworth.
- Houn, G. F., Hesketh, B. L., Frank, M. G., McConkey, K. M., & McGrath, G. M. (1995). *Perceptions of ethical dilemmas: Ethics and Policing study 1*. Payneham, Australia: National Police Research Unit.
- Huberts, L. W. J. C., Lamboo, T., & Punch, M. (2003). Police integrity in the Netherlands and the United States: Awareness and alertness. *Police Practice and Research, 4*, 217-232.
- Ivkovic, S. K. (2005) Police (mis)behavior: A cross-cultural study of corruption seriousness. *Policing: An International Journal of Police Strategies and Management, 28*, 546-566.
- Jetmore, L. F. (1997). *The path of the warrior: An ethical guide to personal and professional development in the field of criminal justice*. Flushing, NY: Looseleaf Law Publications, Inc.
- Kappeler, V. K., Sluder, R. D., & Alpert, G. P. (1998). *Forces of deviance: Understanding the dark side of policing*. Prospect Heights, IL: Waveland Press.
- Klockars C. B., Ivkovich, S. K., Harver, W. E., & Haberfeld, M. R. (2000). The measurement of police integrity. (NIJ Publication NCJ 181465). Washington, DC: National Institute of Justice.
- Maupin, J. R., Bond-Maupin, L. J., & Catlin, D. W. (2006). The impact of the police academy experience on the ethical orientations of American police recruits. *Law Enforcement Executive Forum, 6*(4), 1-16.
- Polloch, J. M. (1998). *Ethics in crime and justice* (3rd ed.). Belmont, CA: West/Wadsworth.
- Polloch, J. M. (2004). *Ethics, crime and justice* (4th ed.). Belmont, CA: Wadsworth/Thomson Learning.
- Polloch, J. M. (2007). *Ethical dilemmas and decisions in criminal justice* (5th ed.). Boston: West/Wadsworth.
- Rachels, J. (1999). *The elements of moral philosophy*. Boston: McGraw-Hill.
- Rokeach, M., Miller, M. G., & Snyder, J. A. (1971). The value gap between police and the policed. *Journal of Social Issues, 27*, 155-171.
- Schlenker, B., & Forsyth, D. R. (1977). On the ethics of psychological research. *Journal of Experimental Social Psychology, 13*, 369-396.
- Sherman, L. (1982). Learning police ethics. *Criminal Justice Ethics, 1*(1), 10-19.
- Solomon, R. C. (1992). *Morality and the good life: An introduction to ethics through classical sources*. New York: McGraw-Hill.
- Souryal, S. S. (1992). *Ethics in criminal justice*. Cincinnati, OH: Anderson.

- Treise, D., Weigold, M. F., Conna, J., & Garrison, H. (1994). Ethics in advertising: Ideological correlates of consumer perceptions. *Journal of Advertising*, 3, 59-62.
- Vitell, S. J., Lumpkin, J. R., & Rawwas, M. Y. A. (1991). Consumer ethics: An investigation of the ethical beliefs of elderly consumers. *Journal of Business Ethics*, 10, 365-375.
- Winter, S. J., Stylianou, A. C., & Giacalone, R. A. (2004). Individual differences in the acceptability of unethical information technology practices: The case of Machiavellianism and ethical ideology. *Journal of Business Ethics*, 54, 279-301.
- Wuensch, K. L., & Poteat, G. M. (1998). Evaluating the morality of animal research: The effects of ethical orientation, gender and purpose. *Journal of Social Behavior and Personality*, 13, 139-151.
- Zhao, J., Ni, H., & Lovrich, N. P. (1998). Individual value preferences among American police officers. *Policing: An International Journal of Police Strategies & Management*. 21, 22-37.
- Ziegenfuss, D. E., & Martinson, O. B. (2002) The IMA code of ethics and IMA members' ethical perception and judgment. *Managerial Accounting Journal*, 17, 165-173.

Dennis W. Catlin, PhD, is an associate professor in the Department of Criminal Justice at Northern Arizona University's Tucson Campus. In addition to teaching, he coordinates the Criminal Justice Department's distance learning bachelor's degree program, designed specifically for working criminal justice professionals. He also serves as codirector of the Law Enforcement Command Institute of the Southwest, a cooperative project of the Tucson Police Department, Northern Arizona University, the University of Arizona, and Arizona State University. Dr. Catlin served as a police officer, special agent for the Federal Bureau of Investigation, and training supervisor for the Michigan Law Enforcement Officers Training Council. He was executive director of the Michigan Judicial Institute, an agency of the Michigan Supreme Court. He taught law enforcement, police supervision, and court administration courses at several community colleges in Michigan and at the School of Criminal Justice at Michigan State University. Prior to coming to Northern Arizona University, he was assistant professor in the Department of Criminal Justice at New Mexico State University. Dr. Catlin has consulted on "rule of law" and judicial reform projects in Egypt, Botswana, Croatia, Bulgaria, the Philippines, Barbados, Slovakia, and Armenia. He received his master's degree in criminal justice and his PhD in administration and higher education from Michigan State University. His areas of teaching and research are justice system organization and administration, education and training of justice system personnel, comparative justice systems, and ethics and law enforcement.

James R. Maupin, PhD, earned his MPA from Southwest Missouri State University and his doctorate in political science from Arizona State University. James is an associate professor, director of the Master of Criminal Justice Program, and academic head of the Department of Criminal Justice at New Mexico State University. He has published numerous articles on decisionmaking within the juvenile justice systems of the southwestern United States.

Appendix: Hypothetical Ethical Dilemmas

Instructions

Below you will find six hypothetical ethical scenarios. Following each scenario, you will be asked to agree or disagree with the person's decision in the scenario. Please focus on the ethics of the decision.

Hypothetical 1: Testifying

Detective Raymond is a witness in a rape and murder trial. The defendant has been investigated in the past for several rapes, but a good case has never been made against him until this one. The previous cases and this one have received widespread attention. While on the witness stand, Detective Raymond answers all the prosecutor's and defense attorney's questions. She completes her testimony and answers all the questions truthfully. She exits the courtroom knowing that she has specific information that may clear the defendant. This information was never elicited from her by the prosecuting attorney prior to the trial, and none of the questions on the stand from either the prosecutor or defense attorney specifically addressed the information she had.

Detective Raymond made the right ethical decision not to reveal the information.

Place an X in the box that indicates your response: Agree Disagree

Hypothetical 2: Responding to Public

Officer Schmidt is dispatched to a personal injury automobile accident. He arrives on the scene to find a young teenage girl pinned under a vehicle that has rolled over. She is screaming out in pain during the final minutes of her life as the EMTs and fire rescue workers try to free her. She dies a few minutes after Officer Schmidt's arrival. During the follow-up investigation, Officer Schmidt encounters the young girl's parents in the emergency room of the hospital. The girl's mother engages Officer Schmidt and asks Officer Schmidt whether or not her daughter was in pain at the time of her death. Officer Schmidt tells the parents that their daughter was unconscious and died immediately and did not suffer.

Officer Schmidt made the right ethical decision about what he told the parents.

Place an X in the box that indicates your response: Agree Disagree

Hypothetical 3: Personal Life

Sergeant Rodgers was reviewing the incident reports for his patrol squad. During that review, he discovered that there was a shoplifting complaint filed by the Target® store in his division that indicated a Ms. Jane Lever had been identified by the store as a possible shoplifter. The circumstances of this particular incident did not result in an arrest of Ms. Lever, however, the information in the report indicated that this was not the first time that Ms. Lever had been suspected of shoplifting. Sgt. Rogers knows that Ms. Lever is the wife of his son's Boy Scout

Leader. After discussing the information he has obtained with this wife, they decide to change his son, Robert, to another Scout Troop. When Sergeant Rogers tells Robert that they have decided to move him to another troop, Robert asks why. Sergeant Rogers does not divulge the information he has but rather makes the excuse that the new troop meets at a more convenient time and location.

Sergeant Rogers made the right ethical decision not to tell his son.

Place an X in the box that indicates your response: Agree Disagree

Hypothetical 4: Tactical/Operational Decision

Officer Mallick is a member of the police department’s SWAT team. His mission is to fire 37 MM tear gas grenades into a room where a dangerous gunman is concealed. The suspect shot an innocent bystander in a botched robbery attempt. His team leader will authorize him when to fire. As the incident unfolds, Officer Mallick is informed by a scout that the suspect has a young woman with two children in the room. One of the children is an infant. Officer Mallick does not know precisely where the mother and children are inside the room. He is familiar with the chemical munitions. The grenade he is ready to fire is CS gas. It is lethal in sufficient concentrations to infants and young children or to those with respiratory problems.

Negotiations with the suspect have failed. Suddenly, the team leader orders an assault. He orders Officer Mallick to fire two grenades into the room through an accessible window in his direct line of fire. After the grenades have been launched, the assault will proceed. Officer Mallick responds that he doesn’t know where the hostages are, that they may be in the line of fire, and two grenades in succession may prove hazardous to everyone inside the room, especially the children. The team leader orders him to fire, and Officer Mallick fires the grenades.

Officer Mallick made the right ethical decision to fire the grenades.

Place an X in the box that indicates your response: Agree Disagree

Hypothetical 5: Commander and Supervisor Relations

Captain Alexander is the commander of the police department’s internal affairs bureau. They have had information from an informant that Officer Blass in the Alpha Patrol Division has been engaging in illicit sexual activities with prostitutes that he has picked up but not arrested. Furthermore, there is information that other officers in Alpha Patrol Division may also be involved. Captain Alexander has set up a sting operation in an effort to determine whether or not the accusations have merit. Sergeant Crais is Officer Blass’s patrol supervisor. She has heard some rumors that there is an internal affairs investigation involving one of her officers. Sergeant Crais requests and is granted a meeting with Captain Alexander. In that meeting, she asks Captain Alexander whether or not one or more of her officers is under investigation. Captain Alexander tells her he is not aware of a current investigation.

Captain Alexander made the right ethical decision not to divulge the investigation to Sergeant Crais.

Place an X in the box that indicates your response: Agree Disagree

Hypothetical 6: Commander and Line Officer Relations

Officer Alvarez is assigned as the crime incident analyst/intelligence officer in a patrol division. Captain Sparks is the commander of the patrol division. Captain Sparks has been asked to speak to a local neighborhood association about the incidents of crime in the neighborhood. Officer Alvarez is asked by the captain to prepare incident reports and crime trends for his presentation to the association. Officer Alvarez is in attendance at the association meeting. Officer Alvarez's analysis of the crime incident reports suggests to him that there is a distinct and troubling rise in the incidents of home invasions and that this trend has been consistent over time. In the presentation by the captain, the captain does not discuss the trend but rather emphasizes that incident of home invasions in this neighborhood is low compared to other areas of the city and that the residents should not be concerned. During the course of his discussion with residents, he turns to Officer Alvarez and asks him to confirm what the captain has just said. Officer Alvarez confirms the captain's statements without elaborating.

Officer Alvarez made the right ethical decision not to dispute what the captain said.

Place an X in the box that indicates your response: Agree Disagree

Bioterrorism Preparedness: The Interdependent Relationship of the Local, State, and Federal Governments

Fee F. Habtes, Dr. PA, MHSA, MPH, Senior Program Policy Advisor, Freedom of Information Officer, Illinois Department of Public Health

“The one that frightens me to death, perhaps even more so than tactical nuclear weapons, and the one we have the least capability against, is biological weapons.”

– Colin Powell

Introduction

The obscured working relationship and the interdependency of the local, state, and federal government in preparation against disasters from 9/11 to Katrina have been puzzling. The dependency of the local government on the state and the state dependency on the federal government have been ineffective and unreliable. In case of emergency, the local government officials are designated as first responders, with fewer resources to react and respond effectively. The state’s dependency on the federal government is another problem, which burdens the first responders to obtain the necessary means to ensure response in a timely fashion. The federal government’s tortoise-like reaction in times of disaster has been unsatisfactory.

This study examines the interdependency of local, state, and federal government in the case of a disaster and focuses on bioterrorism. The study favors strengthening the first responders as a means of prevention and preparedness in case of biological attack. Finally, the study supports the reinforcement of the local government and calls on the state and federal government to provide needed resources.

Bioterrorism

The interest in biological warfare has grown tremendously in recent years. Bioterrorism (biowarfare) has become effective in killing many people at once in a short period of time. Most biological agents are easily produced in laboratories. They are small, less expensive, and difficult to detect. This kind of warfare may cause economic damage by easing the killing or incapacitation of large numbers of people. The knowledge to produce these agents is readily available in books and on the Internet, and it can be bought with minimal restriction from laboratories in the United States. It is also easily accessible in Russia due to economical and political collapses and lack of strict controls.

In May 2001, the Center for Strategic and International Studies (CSIS) reported that the United States’ local, state, and federal governments currently lacked a comprehensive strategy for countering the threat of bioterrorism (Cilluffo, Cardish, & Lederman, 2001). Terrorist actions and threats, brought on by political unrest, have escalated

internationally with plane hijackings, bombings, burnings, and assassinations, killing military personnel and civilians mostly in Europe, the Middle East, Asia, and Africa (Simon, 1989). For the United States, however, the real threat is bioterrorism. In the United States, the occurrence of bioterrorism is imminent due to the growing terrorist actions internationally and the availability of biological organisms.

September 11, 2001, demonstrates that national security has been compromised, and peace is a thing of the past. President George W. Bush promised the country that he would bring back stability and minimize foreign threats. To that end, he created the Office of Homeland Security, which addresses the safety and protection of the country. The primary function of this office is to prevent and secure the country from another attack. Its second mission is to locate terrorists and bring them to justice for their crimes against humanity. In order to achieve security, the federal government funded local and state governments to assure that first responders are prepared to confront head-on any terrorist attack of mass destruction.

First Responders

This study focuses on local government preparedness. The designated first responders are the police, fire, EMS, and public health officials, and it is their responsibility to prepare against this threat of terrorism. Often, local governments have fewer resources than the state and federal governments, which is a constant problem that creates a dependency relationship. Ideally, if all things are possible and equal, then the three partners must act simultaneously as one unit to perform the duties required in preparedness for an attack.

For the purposes of this study, there are three levels of preparedness that correspond to the three branches of government: (1) local preparedness, (2) state preparedness, and (3) federal preparedness. Local government as first responders must have the capability and resources needed to meet the demands of the threat and protect the public. This involves significant cooperation among various entities including private healthcare and nonprofit organizations because they must prepare and act in case of a massive emergency attack.

Cilluffo et al. (2001) contend that preparedness requires investing in communication facilities, administrative support, and personnel capacities. FEMA (2001) encourages close working relationships with departments at both the state and federal levels. Davis & Gilman (2002) define *preparedness* through crisis communications as the way any local, state, or federal government provides information to others—internally and externally. Furthermore, Davis & Gilman (2002) explain that in order to be prepared, responders must realize that crisis is possible; it is crucial that events are anticipated, diagnoses are conducted, a plan is developed, and staff are trained adequately. The critical element in any preparedness program is a surveillance system that can provide warnings prior to a bioterrorism attack against the public (Institute of Medicine National Research Council, 1998). Various kinds of drill activities can be used to correct mistakes and learn from the exercise before an actual emergency occurs. In addition, having effective communications during a crisis brings normalcy. After a crisis, it is time to learn from it by assessing damage, evaluating what went right and wrong, and learning to act effectively in the future.

Neglecting Local Government

The researchers mentioned above addressed only general preparedness and failed to mention the relationship of the three levels of government and the critical cooperation in resource allocation. This study addresses how local jurisdictional preparedness is dependent on the state and federal government and the “domino effect” model for terrorist attacks. The domino effect is a synchronized, effective, and efficient way of preparing organizations at the local, state, and federal levels to respond to natural or manmade disasters.

Local public health officials, fire fighters, EMS, and police play a major role in preparedness at the local level as first responders. Key to effective response capabilities is the development of effective communication between partners on the first level through the Incident Command System (ICS). This system is designed for each department in order to provide an effective response to the needs of the victims and the public. The use of new communication technologies in each organization as a network will facilitate timely communication and disburse information quickly. Building public awareness and informing the public about how to react in case of an emergency will make first responders’ responsibilities much easier. Public cooperation and involvement through training on what to do and expect in case of a massive emergency prevents chaos during a disaster and is part of the local government’s responsibility. A well-informed public in time of crisis reduces confusion and contributes to smooth operation.

A successful team effort is dependent on how well all stakeholders work together. Effective training of the first responders and solid education of the public can greatly enhance the chances of success in disaster situations. In a time of emergency, lack of education about what to do leads to guessing and havoc. People without adequate information and education tend to act differently from those who are well-informed. For example, in preparation for a bioterrorism event, the public overreacts when purchasing gas masks for protection against biological agents. This type of behavior demonstrates lack of education. Additionally, bioterrorist experts do not recommend stockpiling antibiotics. The inappropriate use of antibiotics not prescribed by a physician may cause the development of antibiotic-resistant strains of common bacterial diseases. Improper use of antibiotics could cause serious side effects. Stockpiling antibiotics can also lead to expired medications and can result in a shortage of national supplies for routine use (NYC, 2006). The best way for the public to be safe is to be prepared when disaster strikes. Consistent with longstanding disaster preparedness guidelines, one should be prepared for 3 to 4 days of confinement inside a residence with sufficient water and food for the duration (NYC, 2006).

This study demonstrates the need to educate the public and the need to inform and involve the public in the action plan. Educating the community assists the first responders in operating smoothly, effectively, and efficiently. An involved public minimizes emotional confusion and chaos in times of disaster. According to Donald A. Henderson, the Director for Center for Civilian Biodefense Studies (2001) at Johns Hopkins University, educating the civilian population is one of the best strategies of preparedness. The Centers for Disease Control and Prevention also acknowledges that the public is a critical component of preparedness. Indeed, the CDC has developed a national public health strategy for terrorism preparedness and response that encompasses these three categories: (1) Local and state education and training, which are mandated by CDC’s Cooperative Agreement to conduct

needs assessment, develop training, and maintain data on who has been trained, (2) partnerships, comprised of 23 schools of public health and 13 specialty centers, which work with local and state partners to meet identified community needs, and (3) a direct provider of education and training, both internally and externally.

An immediate, prepared response by first responders is crucial in any terrorist attack. The first responders at the local level play a critical role in the communication link. Different tasks are the responsibility of various partners on the team. Firefighters deal with arson; EMS personnel provides medical help; EPA assesses and addresses hazardous materials (chemicals); and law enforcement secures the area. Organizers need to be familiar with the ICS, which internally and externally connects to similar networks.

Since the local jurisdiction is the focus of this study, first responder strategies for preparedness against any mass emergency, such as terrorist attack or natural disaster, will be analyzed.

Local police preparedness to secure and control effected areas is paramount; therefore, the number of police and the training they have received are crucial components in an emergency or bioterrorism attack. If the police have all the equipment and materials needed to protect the community, they will satisfy the requirement of most primary mechanisms of preparedness.

The fire department and EMS team is a vital group that needs to be prepared through extensive training and possession of the proper equipment. There should be an adequate number of ambulances to be disbursed and trained medical personnel to act quickly. Public health officials should be on alert and prepared through the accumulation of prophylaxis and vaccinations to protect the public in its jurisdiction.

State-level preparedness is actually secondary for the support of the local level and makes more resources available to the first responders. If the incident overwhelms the first responders, the local government has to request the assistance and cooperation of Illinois Emergency Management Agency (IEMA), which triggers the various state agency resources and support. If the local government is not prepared, then there is a strong need for cooperation with the state government. The local government would call for cooperation, coordination, communication, and teamwork from the state government, including the support of the private sector. For example, the state reinforces the preparedness of the local level through cooperation in the form of funds and resources, such as prophylaxis and vaccinations, to protect and prepare in advance. The resources of the state, such as security, the state police and the National Guard, public health officials, the IEMA, and others, are all available to be used by the local level to manage response to a terrorist attack.

Finally, when state preparedness is not adequate to assist the local government and the disaster is beyond the state's capacity, then the federal government will be called, and the disaster will be coordinated by the Federal Emergency Management Agency (FEMA).

Cooperation invites the involvement of all three parties, local, state, and federal government, including private organizations. The degree to which the three components are involved is based on the seriousness of the emergency. An effort to protect the public against bioterrorism demands tremendous resources from all

levels. The local, state, and federal governments are responsible for coordinating as a team to protect the community from a possible bioterrorism attack.

This study begs local governments to use every capability to prepare with or without others' cooperation for potential bioterrorism attacks. Hurricane Katrina is an example of the devastation that occurs when the government is not prepared to deal with disaster. Government officials must learn from such examples in order to ensure that the mistakes of Katrina are not made again.

Conclusion

The local government is a building block of preparedness in case of emergency. More resources are needed for training, equipment, and intelligence gathering, which can be beneficial at the state and federal levels. A strong and prepared local government minimizes the effect of any disaster by reacting quickly and effectively. Lack of resources in local government may be an indication of lack of preparation and a threat to the safety of the public. Coordinated efforts in the three levels of government can be a confidence booster for the public and the providers to fight terrorism in the present situation.

Bibliography

- Alexander, Y. (Ed). (1976). *International terrorism. National, regional and global perspectives*. New York: Praeger.
- Agency for Healthcare Research and Quality. Available online at www.ahrq.gov
- Arnold, T. E. (1988). *The violence formula. Why people lend sympathy and support to terrorism*. Lexington, MA: Lexington Books.
- Becker, M. H. (1974). *The health belief model and personal health behavior*. Thorofare, NJ: Temple University Press.
- Bevelacqua, A., & Stilp, R. (1998). *Terrorism handbook for operational responders*. Stanford, CT: Thomas Learning.
- Bhatnagar, N. Raghav. (2003). *Understanding bioterrorism*. Baltimore: American Literary Press, Inc.
- Brodsky, A. C., Hillel, W., & Gould, R. M. (2000, August). Civilian protection measures against terrorist attack are the best preventive medicine. *American Journal of Public Health, 90*(8), 1325-1328.
- Buck, G. (2002). *Preparing for terrorism.*, Stanford, CT: Thomas Learning.
- Center for Civilian Biodefense Studies. (2001). Agent fact sheets. Johns Hopkins University. Available online at www.hopkinsbiodefense.org/pages/response/agent.html
- Centers for Disease Control and prevention (CDC). (2000). Biological and chemical terrorism: Strategic plan for preparedness and response. Retrieved February 5, 2002, from www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm

- CDC. (2002a). CDC, local public health preparedness and response inventory, a voluntary rapid self-assessment. www.phppo.cdc.gov/od/inventory
- CDC. (2002b). Public health assessment of potential biological terrorism agents. Retrieved February 5, 2002, from www.cdc.gov/ncidod/EID/vol18no2/01-0164.htm
- Central Intelligence Agency (CIA). Available online at www.cia.gov
- Charters, D. A. (1994). *The deadly sin of terrorism*. Westport, CT: Greenwood Press.
- Cilluffo, F. J., Cardish, S. L., & Lederman, G. N. (2001). *Combating chemical, biological, radiological, and nuclear (CBRN) terrorism*. Washington, DC: Center for Strategic and International Studies (CSIS).
- Cohen, S., Eimicke, W., & Horan, J. (2002, September). Catastrophe and the public service: A case study of government response to destruction of the World Trade Center. *Public Administration Review*, 62(1), 24-32.
- Davis, S. C., & Gilman, A. D. (2002). *Communication coordination*. Crisis management. (Business methods for communication during a crisis). *Risk Management*, 49(8), 38-43.
- Department of Health and Human Services, Public Health Service. (2004, January). *Bioterrorism and health care system preparedness*. Issue Brief, No 2, AHRQ Pub. 04-p007.
- Federal Emergency Management Agency (FEMA). (2001). www.fema.gov/library/terror.htm
- Institute of Medicine National Research Council. (1998). *Improving civilian and medical response to chemical and biological terrorist incidents*. Washington, DC: National Academy Press.
- The New York City (NYC) Department of Health and Mental Hygiene. (2006). Advises providers against prescribing antiviral medications for personal stockpiling due to concerns about pandemic influenza.
- Simon, D. J. (1989). *Terrorist and the potential use of biological weapons: A discussion of possibilities*. Santa Monica, CA: The RAND Publication Series.
- State of New Jersey. (2006). *Emergency preparedness: Public health component*. Available online at www.state.nj.us/health/er/bioterror.htm

Fee F. Habtes, Dr. PA, MHSA, MPH, serves as a senior program policy advisor and freedom of information officer for the Illinois Department of Public Health (IDPH) in the Office of the Director. Prior to taking his current position, he served in different capacities as Illinois Department of Public Health division chief for the Division of Health Assessment and Screening and chief for the Division of Injury and Violence Prevention. Among many other responsibilities, he also serves as a mentor for the Mid-America Regional Public Health Leadership Institute (MARPHLI) for Executives fellowship program at the University of Illinois in Chicago.

Dr. Habtes has been teaching, training, and consulting for the last quarter of a century. He has presented many professional papers at various events, including the annual American Public Health Association (APHA) Conference in Washington, DC. He visited Cuba to study public health and public administration with 30 other professionals from the United States. He is an expert in bioterrorism preparedness and the war against terror.

Guidelines for Preparing Manuscripts

There are virtually no restrictions on subject matter as long as the material pertains, in the opinion of the editor, to law-enforcement-related areas. Manuscripts should be typed and double-spaced. A résumé or vitae from the author(s) must accompany submissions. Book reviews and research notes will be considered for publication. No submission will be published until recommended by referees, who will review blind copies.

Final manuscripts must be submitted on 3.5" microcomputer diskettes readable on Macintosh or IBM (and true compatible) computers. Please specify word processing program used when submitting diskettes (e.g., *MacWrite* 5.0, *WordPerfect* 5.1, and so on). Also, an ASCII version would be most helpful. Disks will not be returned. Figures and line drawings must be submitted in camera-ready form.

Send three hard-copy manuscripts, vitae(s), and a diskette to . . .

Vladimir A. Sergevnin, PhD, Editor
ILETSEI *Law Enforcement Executive Forum* Editorial Office
1 University Circle
Macomb, IL 61455
(309) 298-1939; fax (309) 298-2642

Manuscripts should be prepared according to the *Publication Manual of the American Psychological Association* (5th ed.) (2001). *Webster's Third New International Dictionary* (3rd ed.) (1983) is the standard reference for spelling. Contributors are responsible for obtaining permission from copyright owners if they use an illustration, table, or lengthy quote that has been published elsewhere. Contributors should write to both the publisher and author of such material, requesting nonexclusive world rights in all languages for use in the article and in all future editions of it.

New Publications Available!



Chicago Police: An Inside View – The Story of Superintendent Terry Hillard

Authors: Thomas J. Jurkanin, PhD, with Terry G. Hillard

In macro-style, this book examines crime, criminal activity, and police response in the city of Chicago, which has a long history of and association with crime. This book will give the reader an inside view of the Chicago Police Department so that a better understanding might be gained of police operations not only in Chicago but in other major city police agencies.

Critical Issues in Police Discipline

*Authors: Lewis G. Bender, Thomas J. Jurkanin,
Vladimir A. Sergeonin, Jerry L. Dowling*

This book examines the problem of police discipline from the collective perspective of professional law enforcement leaders. It offers the reader practical, not theoretical, solutions in dealing with problem employees and misconduct incidents. It reflects the experience and dedication of a highly experienced group of Illinois police chiefs and sheriffs.

To order, contact the Illinois Law Enforcement Training and Standards Board Executive Institute at (309) 298-2646.

Illinois Law Enforcement Training and Standards Board Executive Institute

Law Enforcement Executive Forum

Back Issues Available (\$10.00 each includes shipping)

No. Ordered

<i>Racial Profiling: Special Edition</i> – July 2001	_____
<i>Recruitment</i> – August 2001	_____
<i>Retention</i> – December 2001	_____
<i>Terrorism</i> – March 2002	_____
<i>Police Ethics</i> – July 2002	_____
<i>The Impact of Emerging Science and Technology on Law Enforcement Agencies</i> – August 2002	_____
<i>Police Training</i> – November 2002	_____
<i>Police Management and Leadership</i> – February 2003	_____
<i>Use of Force</i> – May 2003	_____
<i>Police-Medical Collaborations: Dealing with Mental Health</i> – July 2003	_____
<i>Law Enforcement Response to Methamphetamine</i> – September 2003	_____
<i>Legal Self-Defense for Law Enforcement Administrators</i> – November 2003	_____
<i>Police Pursuits</i> – January 2004	_____
<i>Personnel Administration: Psychological Landmines</i> – March 2004	_____
<i>Training the Police Trainer</i> – May 2004	_____
<i>Community Policing</i> – July 2004	_____
<i>Patrol Resource Allocation</i> – September 2004	_____
<i>Special Edition</i> – October 2004	_____
<i>Internal Affairs Investigations</i> – November 2004	_____
<i>Law Enforcement Agency Accreditation</i> – January 2005	_____
<i>Law Enforcement Unions</i> – March 2005	_____
<i>Generational Conflict and Diversity</i> – May 2005	_____
<i>Undercover Policing</i> – July 2005	_____
<i>Public Relations, Media and Political Affairs</i> – September 2005	_____
<i>Homeland Security</i> – November 2005	_____
<i>Racial Profiling: Special Edition</i> – January 2006	_____
<i>Best Practices in Recruitment and Retention</i> – February 2006	_____
<i>Gangs, Drugs, and Violence Prevention</i> – March 2006	_____
<i>Mental Health</i> – May 2006	_____
<i>Integrity-Based Policing</i> – July 2006	_____
<i>Police Resource Management: Patrol, Investigation, Scheduling</i> – September 2006	_____
<i>Interagency Cooperation</i> – November 2006	_____
<i>Critical Issues in Police Civil Liability</i> – January 2007	_____
<i>Special Edition</i> – February 2007	_____
<i>Police Officer Safety</i> – March 2007	_____
<i>Police Administration</i> – May 2007	_____
<i>Financial Management and Police Administration</i> – July 2007	_____
<i>Police Training: Investigations</i> – September 2007	_____
Total Ordered	_____

Topics for Next Year's Subscribers (Topics Subject to Change)

<i>Community Policing: Immigration</i>	<i>November 2007</i>
<i>FBI: 100 Years of Cooperation: Special Edition</i>	<i>January 2008</i>
<i>The Impact of New Technology</i>	<i>March 2008</i>
<i>New Wave of Crime and Police Response</i>	<i>May 2008</i>
<i>Less Lethal Use of Force</i>	<i>July 2008</i>

See reverse side of this page for Ordering Information.

Illinois Law Enforcement Training and Standards Board Executive Institute
Law Enforcement Executive Forum

Ordering Information

Payment can be made by check, money order, or credit card (MasterCard, VISA, or Discover).
No CODs are accepted. Orders may be faxed to (309) 298-2642 or mailed to . . .
ILETSBEI • 1 University Circle • Macomb, IL 61455

For further information, contact the Illinois Law Enforcement Training and
Standards Board Executive Institute at (309) 298-2646.

Shipping Information

First Middle Initial Last

Address

City State Zip

Telephone Fax

E-Mail

\$40.00 Subscription price July 2007-June 2008

Credit Card Information

Name on Credit Card _____ MC VISA Discover

Card Number _____ Expiration Date _____

Signature _____