Program Abstracts

Plenary Session, Monday, 10:30 am - 12:00 pm

Science, Technology, and Law Updates

Daubert *and* Frye *Update*

Paul C. Giannelli

This presentation will discuss (1) the transformation of the Supreme Court's *Daubert* decision into an exacting standard for governing the admissibility of expert testimony in federal trials, (2) the disparate treatment of *Daubert* in federal, civil, and criminal cases, (3) the effect of *Daubert* on state evidentiary rules, and (4) specific challenges to scientific evidence in criminal cases (e.g., fingerprint examinations, questioned document comparisons, firearms identifications ("ballistics"), bite mark comparisons, and the like).

Confluence of Technology on the Enforcement, Application, and Interpretation of Law: Is the Tail Wagging the Dog?

Erin Kenneally

Technology is a means by which we can manifest our imaginations and has been directed to make our lives more efficient. This presentation explores case studies and legal controversies related to the ever-increasing application of automated technologies in performing actions traditionally relegated to humans or resigned to the realm of the imagination.

The ubiquity of computer technology has challenged us to re-examine the meaning of "reasonableness," and has forced society to increasingly rely on digital evidence to resolve disputes in the civil and criminal arenas. The difficulty of tying an individual to a particular computer that was used in exacting harm, the interconnectedness of computers via the Internet, and the mutable nature of electronic information have facilitated novel defenses and evidentiary challenges to the reliability of digital evidence. Whether it involves verification of vehicle speed, breath alcohol levels, or computer transactions, digital evidence is increasingly utilized to resolve legal disputes and act as the lynchpin of proof. Consequently, there are signs of a shift from presumptive acceptance of digital traces to disputing the inner workings of the technologies used to buttress claims. Should courts continue to rely exclusively on humans as the "real witness" in making admissibility and reliability determinations, or do courts need to delve under the hood of the technologies embedded in the activities where humans run afoul of the laws?

Role of Science and Technology in Law Enforcement: From Fundamental Research to Practical Applications

Vahid Majidi

Research and development activities sponsored by the federal government are an integral part of homeland security strategy. Over the past five decades, national laboratories have been the leading institutions in the U.S. at the forefront of pure and fundamental research leading to both strategic and practical applications. The research conducted at these labs covers nearly all known scientific areas in many disciplines. In this talk, examples of current research programs and their significance to national security will be discussed. Additionally, many of these programs have a potential impact as novel forensic tools for the law enforcement community.

Plenary Session, Monday, 1:30 pm - 5:00 pm

Investigation, Prosecution, and Defense of Cybercrime Cases

Investigation, Prosecution, and Defense of Cybercrime Cases

Syndi L. Guido, Leonard Deutchman, Jennifer D. Eakin, Michael L. Levy, Michael J. McTavish, Mark Rasch

Panel members will discuss the types of computer crime cases currently being committed, including online seduction, the exchange of child pornography, pfishing, theft of information, malicious intrusions, and illegal online businesses. Panelists will discuss the people who are committing these crimes and the methods they employ. In addition, investigative techniques, legal issues, and future trends will be explored.

Online Sexual Victimization of Children: A Behavioral Perspective

Jennifer D. Eakin

Investigations involving the online sexual victimization of children necessarily encompass at least three areas: legal, technical, and behavioral. The investigator has to have at least an appreciation for all three. This discussion focuses on the behavioral issues associated with these investigations. There has been significant media attention on this crime problem; the number of federal, state, and local agencies involved in this type of investigation has increased dramatically, and yet investigators are not running out of work. Is there a new breed of sex offender? Online investigations tend to focus on individuals who use the Internet to traffic in child pornography, often referred to as "traders," and individuals who use the Internet to meet and have sex with children, often referred to as "travelers." But is this an oversimplification of the problem? Is there added risk when individuals not only fuel their deviant sexual arousal patterns but also receive validation through interaction with other like-minded individuals? What can be gleaned about the relationship between collecting child pornography and contact offending?

Plenary Session, Tuesday, 8:30 am - 10:00 am

Investigation of Abuse: Use of Science, Technology, and Law in Detection and Resolution

Child Abuse Issues

Robert Block

As part of a panel discussion on child and elder abuse, Dr. Block will discuss the science of abusive head trauma as an example of dealing with challenges to scientifically accepted conditions, defining evidence-based medicine, and confronting controversy. New technologies are being developed to bring better biofidelity to modeling, as human experimentation is obviously precluded when studying abusive injuries. The law must deal with the credibility of expert witnesses, so a guide to assessing the value of a witness will be presented.

Forensic Markers of Elder Abuse: "She's Just Old!"

Laura Mosqueda

There is much confusion regarding forensic markers of physical abuse and neglect in older adults. This, in part, stems from the fact that many normal and common age-related illnesses increase one's

likelihood of sustaining injuries such as bruises, pressure sores, and fractures. In this presentation we will review this dilemma and discuss some of the science and models of interdisciplinary team work that have been used to overcome it.

Using Long-Term Care Information to Improve Diagnostic Post-Mortem Accuracy for the Elderly Decedent

Richard E. Powers

Long-term care includes services provided through home-based care of disabled elders, nursing homes, assisted living, and unlicensed unregulated residential facilities. This panel will briefly review caregiver dynamics in both the family and long-term care setting. The discussant will outline regulatory and enforcement mechanisms that apply to each long-term care system and available data for residents within those facilities. The discussant will review the scope of unrecognized and unprosecuted abuse, based on recent survey data from long-term care professionals, forensic pathologists, and district attorneys. The discussion will include potential policy changes at the state and federal level that may improve detection of abuse or neglect in long-term care settings.

Plenary Session, Tuesday, 10:30 am - 12:00 pm

Ensuring Accuracy and Reliability in Science and Technology

Accuracy: A Trial Judge's Perspective

Elizabeth A. Jenkins

The trial judge's gatekeeper role in determining what evidence is reliable and relevant is nothing new. *Daubert* added a stringent set of guidelines for federal courts to follow prior to admitting opinion evidence that has a scientific basis. The trial judge must find that the evidence is both reliable and relevant. The reliability inquiry involves such questions as (1) can the theory or technique be tested? (2) has it been subjected to peer review? (3) does the technique have a high known or potential rate of error? and (4) has the theory attained general acceptance within the scientific community? The relevancy inquiry asks whether the evidence has a valid connection ("fit") to the disputed facts in the case. The third factor in the reliability analysis – potential error rate – can be decisive.

Regulating Crime Laboratories

Paul C. Giannelli

This presentation will discuss (1) the American Bar Association's resolutions on forensic science, which were adopted in August 2004, (2) the provisions in the "Justice for All" Act that relate to the regulation of forensic science, (3) the state statutes that require the accreditation of crime laboratories, and (4) legal procedures that may impact on the work of forensic laboratories.

Scrutinizing Peer Review

Susan Haack

This presentation will discuss meanings of "peer-review" and the origins and history of the practice of peer-reviewed publication: roles of peer-reviewed publication in the sciences, in universities' tenure and promotion systems, in the publishing business, and in the law (specifically, in *Daubert*). The discussion will cover peer-reviewed publication as an indication of reliability, its epistemological rationale, difficulties in

testing its effectiveness, what factors influence peer review functions, and reasons for reservations. There are limitations and failures of peer review; some examples of badly flawed papers accepted after peer review will be given. Peer-reviewed publication is a *Daubert* factor: it was misapplied in *Berry* and misunderstood in *Havvard*. Some tentative conclusions about its appropriateness or otherwise will look at (a) Peer-reviewed publication as an indication that proffered scientific testimony is reliable enough to be admitted in court, (b) Peer-reviewed publication as an indication that proffered scientific testimony is reliable enough to be credible, and (c) Lack of peer-reviewed publication as an indication that proffered scientific testimony is too unreliable to be admissible.

Ensuring Accuracy and Reliability in Science and Technology

Carl M. Selavka

"CSI" provides a close look into the world of forensic science, and it depicts the most important components of reality. Forensic science is absolutely interesting! However, one of the challenges of this discipline, which is often left out of the 48 minutes of non-stop drama, is the essential role of quality assurance. The overall forensic process includes many components, including (but not limited to) (a) period of crime commission to discovery; (b) on-site first-responder practices and initial investigative steps; (c) evidence recognition, presentation, collection, transport, and documentation of integrity; (d) triaging of cases and items within cases to effectuate the highest productivity and minimize potentially exhaustive testing; (e) forensic examinations; (f) interpretive management of elicited and missing data; (g) determination of proper contextual elements to insure forensic reports that represent "probative information;" (h) determination of subsequent iterative evidentiary management steps to insure appropriate presentation of forensic information to all law enforcement, legal advocates, and stakeholders; and (i) presentation of information in court in a manner that is forensically defensible. For each of these forensic process components, quality assurance plays a substantive role. The words "accuracy" and "reliability" are commonly used to refer to the desired outcome of each component. But given the adversarial nature of the realm into which the forensic scientist imparts her or his outcomes, experience, and wisdom, accuracy and reliability are never "ensured." They remain in the eye of the beholder.

Plenary Session, Tuesday, 1:30 pm - 5:00 pm

Balancing Information Sharing and Privacy Concerns

CCTV Technology and Privacy

Susan F. Brinkley

Since the terrorist attacks of 9/11, the United States has been interested in applying technology that will assist in the identification, detection, and apprehension of people who aim to do harm to America. CCTV technology is one application that has shown promise in accomplishing these goals. The use of CCTV in the United Kingdom greatly surpasses that of the United States and has for decades. With the swift actions of the British police after the July 7 London bombings and the July 21 attempted London bombings, the world could see the usefulness of CCTV as a tool to assist law enforcement in the identification of criminal suspects. Within days of the July 21, 2005, London bombings, there were people urging America to expand the use of CCTV cameras, especially in train stations, subways, and other public areas. While it is tempting to put cameras in many public areas, authorities do have to be cautious of privacy concerns. There are constitutional, ethical, and practical issues that any police department, university, hospital, or other public official must take into account before the deployment of CCTV technology in order to be confident that privacy concerns are addressed on the front end. This presentation covers the current case law dealing with

privacy in the U.S. with respect to CCTV technology and will briefly look at European case law dealing with human rights concerns and CCTV.

Balancing Information Sharing and Privacy Concerns

Donna A. Bucella

It is clear that information sharing is an essential tool in government's efforts to combat terrorism. The creation of the Terrorist Screening Center (TSC) by presidential directive in 2003 was one of the earliest U.S. Government initiatives to consolidate and share information in the struggle against terrorists and extremists. The TSC's mission is to coordinate the government's approach to terrorism by screening and maintaining the U.S. government's consolidated terrorist watchlist, which is made available to agencies that perform terrorism screening. Recently, legislative initiatives like the Intelligence Reform Act have gone even further by requiring all federal agencies to share terrorism information with one another. The Act also mandates the creation of a new Federal government IT system, called the "information sharing environment," to facilitate the sharing of terrorism information, including the consolidated terrorist watchlist.

With respect to terrorism at least, it is clear that what was once one agency's information is now potentially every agencies' information. Given that, how do we provide for appropriate privacy protection and deal with terrorism? Here are some examples of TSC initiatives to safeguard privacy while allowing appropriate information sharing:

Develop and follow clear written procedures. While the law and internal privacy policies already limit information sharing, clear and detailed standard operating procedures, or "SOPs," must be in place to ensure these limits are observed in practice. At the TSC, our SOPs are in writing and reviewed by our privacy officer to ensure that any sharing of information meets legal and policy-based requirements. TSC personnel are instructed that information sharing that is not expressly permitted by the SOP must be approved in advance by privacy or legal counsel.

Make use of appropriate technology to enhance the privacy and security of personal data. Technology can greatly enhance the privacy and security of personal information. TSC is exploring the development and use of privacy-friendly technologies like anonymization, which will keep personal information in an "anonymous" or scrambled form unless and until it is matched to the watchlist.

Ensure fairness by providing redress to those who are adversely affected. TSC routinely reviews complaints from individuals who were inconvenienced or delayed during screening and will correct any erroneous data in its records. TSC works with agencies that perform screening and collect terrorism information to ensure that data errors are corrected in those agencies' record systems as well.

Technologically-Rational Doctrine of Search

Stephen E. Henderson

The Fourth Amendment to the United States Constitution prohibits "unreasonable searches and seizures." Yet as interpreted by the United States Supreme Court, the Amendment places no restriction on police combing through financial records; telephone, e-mail, and website transactional records; or garbage left for collection. In fact, there is no protection for any information "voluntarily" provided to a third party, because the provider is said to retain no "reasonable expectation of privacy" in that information. As technology dictates that more and more of people's personal lives are available to anyone equipped to receive them, and as social norms dictate that more and more information is provided to third parties, this restriction threatens to render the Fourth Amendment a practical nullity. By reviewing some modern technologies (e-mail, millimeter wave detectors, off-the-window eavesdropping, TEMPEST receivers, cell phone location tracking, and data mining) participants will be able to appreciate the magnitude of the issue and discuss how Fourth Amendment jurisprudence can be altered to better balance privacy and security in the post-9/11

United States. Each state has a constitutional analog to the Fourth Amendment; so one source of useful information is the constitutional jurisprudence of the 50 states. Perhaps among these state "laboratories" research may find a workable alternative to the Supreme Court's strict third party doctrine.

Operation of a Criminal Intelligence Center – The Pennsylvania Experience

Frank E. Pawlowski

In response to the tragedy of September 11th, a number of major law enforcement agencies across the county have created intelligence centers to strengthen information-sharing capabilities. In July 2003, the Pennsylvania State Police (PSP) opened the Pennsylvania Criminal Intelligence Center (PaCIC). Staffed with professional intelligence analysts, PaCIC is designed to assist local, state, and federal law enforcement agencies in their principal mission: the prevention of crime and terrorism.

Like many counterparts across the country, the PSP created this intelligence center to provide law enforcement with a central point of contact for their information needs. Authorized law enforcement officers can gain access to public source information, investigative data, and intelligence information by contacting PaCIC intelligence analysts, who have entrée to many statewide and national databases. These trained and professional analysts provide the law enforcement community with controlled yet comprehensive access to critical and timely information that assists law enforcement in protecting citizens.

With better accessibility to information and the proliferation of technology, law enforcement still must adhere to a business model that allows for the legal and efficient collection, analysis, and dissemination of information, while guarding against violations of personal privacy and public trust. While professional and legal standards continue to evolve with regard to the creation and operation of intelligence and fusion centers, the PSP is committed to pursuing the latest technological advances in information sharing. At the same time, the PSP remains steadfast in its belief that American values and constitutional safeguards must not be compromised as law enforcement strives to prevent crime and protect the citizens of this country from the threat of terrorism.

Protecting Society by Protecting Information: Looking at the Costs of Information Sharing

Adam Shostack

Potential benefits of information sharing are widely touted. But the fiscal and societal costs of surveillance databases and systems are often ignored. Information sharing has come to entail high availability of information. High availability of information enables a set of crimes, including stalking and identity theft. The traditional response of better certification led to corruption at DMVs across the country. That corruption and the fraudulent issuance problem lead to data quality problems in warrant databases (and elsewhere). Presenters will examine the economic feedback loop of improved identification and data sharing, and ask if there are local or global optima available. Participants will also examine framing problems created by easily accessible, high quality data; how such data discourages alternate forms of investigation; and how terrorists could exploit such habits.

Virtual Searches

Christopher Slobogin

This talk will briefly canvass a significant new development in the government's relationship with its citizens: the "virtual" search. The classic law enforcement search–a detective entering a house armed with a warrant, or police officers rummaging through the contents of a car–has long been the government's primary investigative tool. But that may no longer be the case. Technology increasingly enables law enforcement to garner evidence of crime without physically intruding onto or into a person's property.

These virtual searches usually involve some sort of surveillance, often conducted covertly. This surveillance can be divided into three types: communications surveillance (interception of communications); physical surveillance (observation of physical activities); and transaction surveillance (the accessing of recorded information). Technology has vastly expanded the government's ability to conduct all three types of surveillance. Wiretapping, bugging, and computer hacking devices make "eavesdropping" on oral and written communications infinitely easier. Physical activities can now be observed through telescopic lenses, nightscopes, and devices that detect heat and images through walls. Transactional information is readily accessible using "snoopware," commercial data brokers, and ordinary Internet searches.

This talk focuses on physical and transaction surveillance. Communications surveillance is well-studied, and the law in the area, epitomized by the federal statute known as Title III, is well-developed. Physical and transaction surveillance have received much less attention. To date, these two methods of government investigation have been subject to relatively little legal monitoring. Yet they can be just as intrusive as communications surveillance. The talk will describe various forms of physical and transaction surveillance and then analyze the "hot issues" triggered by each type of surveillance.

Plenary Session, Wednesday, 8:30 am - 10:30 am

Emerging Legal Issues with Science and Police Investigation Tools

Advantages and Disadvantages of Videotaped Police Interrogations

George Cadavid

Until the 1980s, most confessions were recorded and presented in either a written or audiotape format. However, as a result of advances in videotape technology during the past two decades, one-third of the nation's law enforcement agencies now videotape some interrogations. Proponents claim that videotaping an interrogation in its entirety can only enhance justice by limiting or ending the number of wrongful convictions obtained through forced confessions. They contend it would save tax money by reducing multimillion-dollar awards in wrongful arrest lawsuits and police misconduct cases, as well as eliminating the cost in court confession suppression hearings.

Recent studies indicate that the increasing reliance on videotape confessions may be inadvertently introducing a new bias into criminal justice proceedings that has the potential to adversely affect the judgment of the suspect's voluntariness. The camera perspective may influence judgment of voluntariness. Numerous studies in this area demonstrate that people's attributes of casualty are strongly influenced by their point of view. This so-called "salience effect" specifically indicates that there is a pervasive tendency for people observing a social interaction to overestimate the casual role of the individual who is most visually prominent; that is, the one who can be seen most clearly. Although none of the studies alone will adequately address this generality question, together they should provide a solid indication of whether or not the criminal justice system needs to be seriously concerned about how it acquires and uses videotaped confessions.

Science of Identification and Misidentification

Steven E. Clark

Eyewitness errors that lead to wrongful convictions have two primary causes: poor line-up composition and suggestive police procedures. Once a misidentification has occurred, it can be extremely difficult to rectify. It is much more efficient to stop misidentifications before, rather than after, they occur. Toward that goal, eyewitness identification research has pointed toward a number of procedural reforms that can minimize the factors that lead to misidentifications. These reforms include scientific line-up construction

and pre-line-up evaluation, blind line-up administration, the use of sequential line-ups, and the mandatory audio or videotape documentation of line-up procedures.

Police Experience with Recording Custodial Interrogations

Andrew W. Vail

This presentation offers a discussion of law enforcement's experiences with recording complete custodial interrogations, including reports and quotes from law enforcement officers who regularly record custodial interrogations in their entirety; a survey of state recording laws; model recording legislation; and recording technology and interrogation room recording set-up, with a focus on the Chicago Police Department's recording system and procedures.

Conducting Line-ups and Presenting Line-up Evidence in Court

William E. Wynn

Pre-trial line-up has proven to be an excellent method of testing a witness' ability to identify a perpetrator. The courts have discretion in granting or denying a request for a line-up. There is no constitutional right to a pre-trial line-up. If the defendant's appearance has altered substantially, the line-up will be cancelled pursuant to Municipal Court Criminal Procedure. All suspects/defendants have the right to counsel unless a waiver has been signed, and defendant's attorney must appear at the line-up or be subject to sanctions. Police can place a person in custody into a line-up against their will; no person has a right to refuse to appear in a line-up. Notice of a line-up must be given to the suspect or defendant and to the defense counsel. Fill-ins for the line-up might be chosen by counsel, via court order from outside the prison, or by the suspect/defendant. No Philadelphia County Court has granted a Motion to Suppress a line-up identification since 1981. In Philadelphia, Pennsylvania, line-ups are scheduled in several ways: by counsel (court-ordered), through voluntary consent when the suspect requests it, or by law enforcement (police ordered).

Plenary Session, Wednesday, 11:00 am - 12:30 pm

Impact of New Technologies on the Criminal Justice System

Biotracks Pilot Leverages DNA Technology to Solve Burglaries and Other Lesser Offenses

W. Mark Dale

This program is a unique partnership between private and public DNA laboratories, the District Attorney, and the crime scene unit. Most public laboratories do not have the capacity to analyze lesser offenses. Ironically, it is the lesser offenses that need to be included in the Combined DNA Index System (CODIS) to increase the effectiveness and efficiency of the system. Data now show that over one-half of the violent crime hits in CODIS are from lesser offenses. Burglary is a crime that affects millions of Americans, yet most of these cases go unsolved. Under this pilot program in Queens, crime scene evidence will be analyzed for the presence of DNA profiles from burglars, which can now be obtained using tiny quantities of DNA from perspiration or saliva on items left by suspects at crime scenes. The DNA profiles from these samples are matched against local, state, and federal DNA databases to identify suspects. DNA technology focused on these repetitive crimes could be an effective crime-fighting tool, because a large proportion of burglaries are committed by repeat offenders, many of whom graduate to violent crime. Linkages will be explored between lesser offenses, violent crime, and recidivism in a specific geopolitical area.

Recent Evolution of the Forensic Sciences

Joseph L. Peterson

The field of forensic science has made remarkable improvements in the past 30 years. First, the number of forensic laboratories tripled in the 1970s. This expansion was largely due to the rising drug abuse problem, increase in violent crime, and availability of federal monies to underwrite new laboratories at the state and local level. This period also saw the introduction of proficiency testing, accreditation, and the development of various certifying bodies. There was a dramatic improvement in the use of latent fingerprints as automated databases were introduced in jurisdictions throughout the United States. The 1980s saw the introduction of DNA typing, which was to revolutionize the forensic sciences by increasing the sensitivity and specificity with which biological samples could be characterized. The 1990s then saw the application of DNA methods in post-conviction testing of evidence that demonstrated that many defendants had been unjustly convicted and sentenced based upon erroneous evidence (scientific and otherwise). Extending into the new millennium, there has been the growth of DNA databases and another generation of improvements in its sensitivity. The 1990s also ushered in a new judicial awareness of scientific evidence through the U.S. Supreme Court decisions of *Daubert* and *Kumho Tire*, causing courts to be much more interested in the scientific foundation and reliability of the various forensic sciences.

In the current decade, a dramatic change occurred in the awareness of forensic science among the general public, legislators, criminal justice professionals, and investigative journalists. The public has been sensitized to the forensic sciences through such television programs as “CSI” (leading to a phenomenon known as the CSI Effect); criminal justice professionals are aware that forensic evidence can be the critical difference between winning and losing a case; federal and state representatives have enacted legislation to direct greater funding assistance to crime laboratories; and journalists have responded to the reports of whistleblowers and others who have uncovered questionable conditions within certain laboratories. The field of forensic science, itself, has been brought under a microscope, and observers have learned that all is not well. Professional standards are largely voluntary and not all laboratories (and scientists) are in compliance. Parent police agencies have not always given laboratories the financial support they need to insure the forensic profession can maintain high standards of science and respond to rising caseloads. Just this year, a report from the Bureau of Justice Statistics reported that more than 500,000 requests are backlogged in the nation’s publicly supported crime laboratories.

There is unparalleled attention trained on the forensic sciences profession in this period of time. The forensic sciences possess tremendous potential for the justice system and society, but there are serious obstacles and dangerous pitfalls. The field desperately needs added resources, but the profession itself must respond to a growing demand for superior science and the need for complete objectivity. These and other issues will be addressed in this presentation.

Impact of New Technologies on the Criminal Justice System

Carl M. Selavka

A mantra related to the education process following high school in America has long been that, with each advanced degree you pursue, you learn more and more about less and less. Scientific technologies that lend themselves to the examination of physical evidence to elicit probative information in forensic cases commonly have the same apparent goal. The scientific process itself entails today's generation of specialists (who often know more than you would ever care to hear, about an infinitesimally small sliver of one type of physical material in the forensic world), applying today's best technologies to provide "better" results than yesterday's specialists using yesterday's technologies. One huge difference between "regular" science and forensic science is the forensic requirement to interpret one's analytical findings such that the examiner provides "probative information," not just information. People often describe examination methods in terms

of their analytical "Figures of Merit" (FOMs). These FOMs include sensitivity, selectivity, reliable response range, susceptibility to interference(s), and the *Daubert*-related FOMs that might help define "error rate." But forensic technologies must also contend with residua that may implicate or exculpate the connection between victims, suspects, and crime scenes, ensuring that they are not purposefully left behind. Rarely does such transfer occur onto a pristine surface. In the end, one of the most influential factors that new technologies play in the criminal justice system is how these new results can be interpreted to elicit optimized FOMs. Researchers are often not able to optimize such FOMs and their utility in the CJS, because of the nature and complexity of matrices from which justice research recovers trace residua of probative interest.