SYMPOSIUM COMMENTARY

EVIDENCE TODAY: DISCUSSING THE IMPACT OF TECHNOLOGY ON TRADITIONAL EVIDENCE AND ITS INFLUENCE ON THE EVOLUTION OF MODERN EVIDENTIARY TECHNIQUES*

I. OPENING REMARKS[1]

Rebecca Harp:

Good afternoon. I would like to welcome you to the Albany Law Journal of Science and Technology's Symposium. Additionally, I would like to thank our esteemed panelists and moderators for being here today. I would also like to recognize and thank everyone who helped me organize this event including my fellow journal members, the journal executive board, and various Albany Law staff members. I would like to introduce our first moderator, Professor Christian Sundquist, who is the Director of Faculty Research and Scholarship here at Albany Law School, as well as a professor of immigration law, privacy technology courses, and evidence. Professor Sundquist practiced in law firms for 14 years and received his degree from Georgetown University. We will begin our first panel after the introductory video from Jan Stiglitz,

* Transcript from Albany Law Journal of Science & Technology's symposium held on November 16, 2016.

[1] This article has been reviewed and edited by the Journal of Science and Technology members to ensure that the article is grammatically correct. No other information has been changed.

who founded the California Innocence Project, and has been endorsing the importance of DNA evidence and helping the wrongly convicted.

[Video Segment from Jan Stiglitz, from the California Innocence Project]

II. PANEL ONE: ANALYZING NEW TECHNOLOGICAL ADVANCEMENTS IN BIOLOGICAL AND PHYSICAL EVIDENCE

Professor Christian Sundquist:

Hello everyone and thanks for coming out. We have some very interesting things that we are going to explore today during this panel, and we are joined by some esteemed panelists here with us today. I want to thank you for coming out today to help with this symposium. I am going to do a brief introduction. I'm going to somewhat selectively skim over your bios, if that's okay, just in the interest of time so that we have more time to talk about issues and solicit feedback and questions from the audience.

To my far right, we have Melissa Mourges, who has been a career prosecutor for more than 30 years and is currently Chief of the Forensic Science Cold Case Unit in the New York County District Attorney's Office. She monitors and advises on all cases involving forensic evidence within the office and apparently, you are undergoing a systematic review of every unsolved homicide in Manhattan since 1980, which is a significant endeavor, to see if new forensic testing could be useful in solving these crimes. She was also the Co-Chief of the DNA Cold Case Project, which led our state in investigating and prosecuting cold case sexual assaults in homicide cases via the main DNA database. Perhaps and most importantly, she is a 1980 graduate of Albany Law School.

To my near right, we're joined by Stephen Hogan. Again, thank you for joining us. Mr. Hogan is Assistant Counsel for the New York State Police. He has a variety of duties, including providing legal assistance and training to officers and to prosecutors concerning scientific evidence and the DNA hints. He has presented at national, as well as international, conferences on a variety of topics related to forensic testing and DNA testing. Before he joined the New York State Police he served as an ADA in Rensselaer County, where he prosecuted sex crime cases. Unfortunately, he is not an Albany Law School Alumni but you did

get your B.A. at the University of Albany, so that is close. To my near left, we are joined by Dr. Ann Willey, who not only has a Ph.D. in Genetics and Cell Biology from the University of Minnesota, but she is also alumni of Albany Law School. In 2000, she spent most of her time at the Wadsworth Center for the New York State Department of Health. She served as the Director of Cytogenetics testing laboratory and quality assurance program. She served within the Laboratory of Human Genetics division of Laboratory Quality Certification and she also teaches as an adjunct, a number of courses, here at Albany Law School, which I encourage you to explore, especially if you are excited about the issues that we're talking about today including public health and genetics in the law.

To my far left we are joined by John Carey, who recently retired from the New York State Police after a 32-year career, and when he retired, he was a Senior Investigator who supervised the Troop G Forensic Identification Unit, which covered an expansive area in the state. This unit is charged with processing major crime scenes, documenting scenes, collecting evidence, processing evidence, as well as providing courtroom testimony. It shouldn't be surprising that he is a certified evidence technician, as well as fingerprint examiner and police instructor. I found this interesting on your bio, to skip some of the other things, but apparently, he has collaborated with HBO, as well the Discovery Channel Canada, PBS, the Forensic Files, and Oxygen network regarding a variety of cases in which he had been involved with. He is also a member the Federal Disaster Mortuary Operational Response Team since 1993, and he lectures on a variety of topics throughout the state.

Thank you again for joining us. You are experts in your field and we certainly have a lot to learn from your experiences. Right now, we are going to transition and each of our panelists will talk. I'll try to keep tight control on the time but will allow approximately 5 to 7 minutes for each panelist to discuss some of the things they do in their experience. We will then lead into some more directed questions from me before I open it up to the audience.

Melissa Mourges:

I have just a few minutes, so I'm going to talk fast. Being from New York that shouldn't be too much of a problem. When I first started as a prosecutor in 1980, when dinosaurs roamed the earth, a sex crime case would typically involve a vaginal swab taken from

the victim and then rubbed on the slide. A detective who might have a little bit of training would look through a microscope to see if sperm were present, and if yes, I could walk confidently into a courtroom and state that somebody had ejaculated somewhere near the vicinity of my victim. Additionally, I might be able to tell his blood type if he were a secretor. With the advent of forensic DNA testing in the late 1990s, if we had a blood or semen stain the size of a quarter we could identify somebody. Today we can get a complete profile out of the stain one-billionth the size of a packet of Sweet and Low. In the year 2000, New York State joined CODES, the Combined DNA Index System administered by the FBI, which allowed a comparison of crime scene profiles and offender profiles across state and federal lines. Recognizing the potential to solve crimes, New York City was the first jurisdiction to test its rape kit backlog. We had 17,000 untested kits. Not because we did not care about rape, but because there was no point in testing because there was no database for rape kit profiles. I was one of two senior lawyers in the Manhattan DA's office to work on the cold case project, where we got hits on hundreds of cases, including cases that would otherwise never be solved. These involved vulnerable victims like drug users, as well as victims of both stranger and acquaintance rapes. The DNA is without question a game changer because DNA can prove identity not beyond a reasonable doubt but beyond any doubt. DNA is like other evidence and it needs context. DNA might prove who left evidence, but it does not prove the circumstances under which it got there. Crime scene investigators might pick up every cigarette butt left on the playground where a shooting took place or every condom on the scene of a rooftop rape. That does not mean that everyone whose DNA is on those cigarettes or condoms is guilty. We must always rule out an innocent explanation for the presence of that evidence. I am in charge of the cold case program and we have had phenomenal success with the application of new forensic techniques to old cases. This particular case is a 1994 strangulation rape-murder. You can see the woman's body, up there, she was left on the rooftop. At the time, investigators recovered a Kleenex on the rooftop and vouchered it. The medical examiner also clipped and saved the victims fingernails because strangulation victims often claw at and scratch the people who were choking them. In 2013, the Office of Chief Medical Examiner's DNA lab used the new process called sonication. Sonication is where they dropped the whole fingernail into a tube

and hit the soundwaves to shake the DNA off the fingernail and into the solution. DNA testing yielded a complete male profile, which matched a convicted rapist in the CODES database. We also found the suspect's semen and blood on that Kleenex. It told the story that the victim obviously scratched him as he raped and killed her, and then he wiped himself off on the Kleenex, dropping it on the roof. In his case, the fine for littering was life in prison. This is another case in a playground of Manhattan, where the victim was strangled and sexually assaulted in 1991. Again, in 2013 our DNA lab was able to get male DNA from under the victim's fingernails. Again, it matched a convicted rapist in the DNA database. Further testing of semen, collected from the leg of the victim, revealed a matching DNA profile. Oddly, the jury did not believe the defendant had consensual sex with her and someone else came by and killed her later. This defendant was convicted in under an hour. I understand why defense attorneys do what they do. I understand their ethical obligations to zealously defend their clients but you will forgive me if I have grown a little cynical over the years. The defense bar in general and the post-conviction bar in particular have a love-hate relationship with DNA. In the early days in a post-conviction proceeding, if there was untested DNA and those results were different from the person convicted in an eyewitness case, the defense bar would argue, correctly, that the eyewitness evidence was wrong and that the DNA was great because it proved the defendant was innocent. The same thing with confessions. The defense will argue that the confessions were false and coerced and the DNA was great because it proved the defendant was innocent. But now that DNA testing is done in virtually every case, the tides have changed. Now the defense bar spends lots of time and money arguing that DNA is unreliable because it proves the defendant is guilty. There's a whole cottage industry of DNA experts to testify for the defense and are happy to make $200, $400 an hour arguing that fully accredited government forensic labs have gotten it wrong. DNA is not the only common type of forensics. I am a liaison between the lawyers in my office and all the forensic lab. The medical examiner uses forensic pathology for cause and manner of death, and forensic toxicology for the presence of drugs, alcohol, and poisons. We use forensic odontology re bitemarks, especially in child abuse cases, where a child has been left in the custody of a small population of individuals. We examine hair and fibers. We examine documents and test narcotics. Ballistics tool mark

matching is particularly useful. It can match two bullets coming from the same gun, or prove that a bullet came from a gun. The automated fingerprint system is loaded with the database of millions of inked prints from fingerprint cards taken during arrest or licensing procedures. Each finger is coded by an algorithm that assigns a numerical value to each of the minutia or features of a fingerprint, such as a loop, an arch, and a whirl. Then latent prints recovered from the crime scene are scanned into the same computer and there, also coded. The latent print is launched against the database and candidates for potential matches are suggested. The final comparison is done by a human latent print examiner to determine whether there is a match. Finally, other technologies mean that even without the blood and guts forensics, a one-eyewitness case will be rare indeed. For example, we can put someone at a crime scene or show that they were not at a crime scene through surveillance video, GPS on a cell phone through cell tower records, mass transit Metro cards, automated license plate readers, and E-ZPass records. We provide more information to the government just by walking around with our phones than George Orwell ever could've imagined. If anyone is interested, get in touch with me later that for how you do it.

Stephen Hogan:

Good afternoon everyone, I am very excited to be here. I work for the State Police, but I am not here in my official capacity. I do not purport to speak for the State Police. I am here in the capacity I wake up in every single day—the capacity of Jennifer's husband and Hannah's Dad. I am also very likely to be the most enthusiastic DNA geek that you will likely meet in the course of your lifetime. I fell in love the application of molecular biology to context of forensic science and criminal justice late 1980s that passion remains undiminished. I am fortunate because my job responsibilities for the New York State Police Forensic Investigation Center require me to understand the scientist details and to work on issues that involve important, and at times competing social values that will hopefully emerging during this symposium.

Professor Sundquist and I spoke briefly how there may be room some consensus among the various criminal justice stakeholders in the context of new forensic technologies. For several issues on the horizon it may be possible to integrate advances in of forensics technology into the criminal justice system without compromising

vital civil liberties. I envision working toward a sweet spot, rather than defaulting to a "zero sum" approach.

Most criminal justice officials want juries to be able to exercise their fact-finding prerogatives. We want advocates for accused defendant's to be able to present evidence without unnecessary restrictions. However, it has been—and it always will be—critical have some effective means to protect civilian jurors form junk science and pseudo-science. To illustrate, in 1972 the Congress enacted the Federal Rules of Evidence, as part of general initiatives indicating that Congress wanted a more liberal approach that would allow jurors to hear and evaluate scientific and technical evidence. However, the arcane and technical nature of certain expert testimony can make it difficult for jurors who are not highly trained in science to effectively evaluate.

In 1972, the FBI laboratory was performing a forensic testing technique known as composite bullet lead analysis. In cases in which this technique was used, an FBI scientist would that a bullet that was found in this person's house and was analytically indistinguishable (or words to that effect) from the bullet in the victim's brain. This was understood to mean that the bullet in the victim's head came from the ammunition found in the defendant's possession. What would juror's without scientific backgrounds be expected to do with this information? Often they deferred to the FBI expert and were persuaded by the prosecutor's closing arguments about the clarity of the FBI expert testimony and the excellent international reputation of the FBI Crime Laboratory. Think of the jurors in cases like these. They hear the testimony of an FBI analyst who has travelled several hundred miles to testify at a County Court murder trial. The FBI expert could have a Ph.D. in metallurgy from Carnegie Mellon. The defense is unable to obtain an expert to counter the composite bullet lead analysis testimony. In the deliberation room, could jurors reasonably be expected to ask questions about the possibility of pre-existing heavy metal contaminants? Is it reasonable to expect that they would challenge the experts? No. They are much more likely to accept the expert's conclusions and be persuaded by the prosecutor's closing argument and return a verdict of guilty. This tragic result is an unjust convictio0n.l this fun stuff.

I want to start with the DNA databank and what you need to know about the databank because it is a natural launching point for discussion of arrestee DNA and familiar searching. Eventually as we developed PCR, Polymerase Chain Reaction, a gift from Dr.

Kerry Mullis, a very colorful character, we gave scientists in all disciplines the ability to take a very small amount of DNA, make millions of copies of the areas of interest. This PCR technique allowed forensic scientists to develop digital profiles from crime scene evidence. The New York State Police DNA Databank now has approximately 60,000 unidentified crime scene DNA profile in the Forensic Index. The DNA of persons who are required by New York State law to provide a DNA sample are submitted to the New York State Police DNA Databank. The Databank also develops DNA profiles individuals (identified only by number) and these profiles are used to populate the Offender Index. Each week the DNA profiles developed from crime scene evidence are searched against all against the approximately all other crime scene profiles in New York and against all Offender DNA profiles in New York. If the crime scene sample meet federal eligibility criteria promulgated by the FBI, these "forensic unknowns" can be search throughout the country as part of the FBI CODIS system. On occasion they can be searched through Interpol. For example, about 10 month ago, we had a hit between a rape in California and Offender in Israel. He was arrested in Tel Aviv. This ability to digitize DNA profiles and then use supercomputers allows investigator to find needles in a haystack.

These are cases that would be otherwise impossible to solve—even if you used thousands investigators working full time for extensive periods of time.

Another benefit of the DNA Databank is that it has been proven to exonerate the innocent, there have been approximately DNA Databank 40 exonerations and more at this point. Many people know about the Troy Barry Batista case. This is where two people were about to tried for a murder they did not commit. On the eve of trial, there was a hit to the DNA databank.

Another benefit of the DNA Databank is that it uses criminal justice resources very efficiently. With the robots now we now use at the New York State DNA Databank, we can develop a DNA profile and now upload it to the Offender Index in the New York State Police DNA Databank at a cost of approximately $30 dollars per sample. Since operations began at the national level, over about 350,000 investigative leads have been generated for Investigators to further evaluate.

Over time in the class of individuals who are required by New York State Law to provide a sample has risen. A 2012 initiative by Governor Cuomo resulted in the change in the definition of a

"designated offender" in Executive Law § 995(7). It now includes all crimes as defined in the Penal Law (with the exception of Criminal Possession of Marijuana in the 5th Degree) and all felonies described in other New York statutes. For example, the new law covers felony-level violations of the Agriculture and Market's Law. Inclusion of "Buster's Law" felony animal cruelty, has been a helpful strategy for us. In fact, every time the definition of "designated offender" in Executive Law § 995 has been expanded, many significant unsolved cases are solved.

The demonstrated benefits of DNA Databank efforts suggests a moral imperative. Specifically, if law enforcement has at its disposal, a legal method to identify persons who have committed past crimes (some of whom are serial offenders who will continue to commit crimes), how can the failure to use this tool to its fullest potential be justified?

At least 27 states have chosen to compel persons arrested for certain crimes be compelled to profile a sample for inclusion for the state's DNA databank. A large number of serious felony cases in states that compel production of a DNA sample from certain individuals at the time of arrest.

The constitutionality of arrestee DNA testing has been established in *Maryland v. King*.

The criminal justice benefits of arrestee DNA testing are inarguable. However, opponents of these laws raise several valid concerns. This tension reflects the competing values for our society I mentioned earlier.

If time permits today, we can also talk about the New York State DNA Partial Match Policy and the policy used in at least 10 states to use computer algorithms to trawl state offender DNA Databases in an attempt to identify a close biological relative of the person who committed the crime.

Ann Willey:

I'm a geneticist first, I am a scientist, and I spent 31 years at the Health Department doing genetic testing for diagnostic diseases. Now we have talked about dinosaurs, I describe my genetics career as starting in the dark ages, where we had to start with pounds of flesh to extract grams of DNA, and the only genetic characteristics we could look at in an analytical way were what we now call junk DNA, even though it is probably not junk and it probably has vital functions we haven't figured out yet, but it is large repetitive blocks of DNA. My particular field of genetic practice involves the

examination of whole chromosomes. These are the colored structures that we see in dividing cells. Each human zone contains, on average, more than 100 million nucleotides of DNA. We have 3 billion, each chromosome has about 100 million. We talk today about single nucleotide polymorphisms. This is a change in the DNA molecule of individuals that involve a single nucleotide. So, we have gone from the dark ages to current status in one career.

I only worked for three decades. I spent much of my career at the Health Department, because as a geneticist and as genetics was an expanding function of clinical laboratory medicine. I was involved in the quality assurance program in New York and I am sure that as most of us know in New York State, if it exists, we regulate it. In the Health Department if it has to do with laboratory analysis, clinical labs, environmental labs, blood banks, tissue banks, forensic labs that are not government owned, the Health Department regulates them. I became director of all of our regulatory programs at the Health Department, and as a result, encountered a lot of attorneys.

When the regulatory program challenges the livelihood of a laboratory operator, the first person they're likely to call is their attorney. The attorney would come to my office and start to tell me that I did not understand the law, even though the governor's pen was on the wall, and I drafted most of the implementing regulations. I had to admit they were right. As a scientist, who had been charged with writing scientifically valid standards for operations of laboratories, I did not study how the law would look at things like property interest in a license and even evidence issues. I came to law school. After graduating from law school and being admitted to the bar, I continued my function with the Health Department, during and after law school. The attorney would come to my office and they would start with the "you do not understand the law", and I would say, "No, you do not understand the science."

I feel like I have spent most of my career as a translator, trying to teach legal issues, mandates, statutes, rules, process, to scientists, whether they were trying to file a patent and did not understand the rules that you could not publish before you file and things like that. The regulatory requirements of the operation of the laboratory. Personal standards of professional conduct or more recently, teaching science, scientific method, scientific principles, sometimes the actual science, to lawyers and as my students will

tell you, they often criticize my courses as being too much science. At least, we have to talk about the vocabulary before we can talk about the legal issues involving genetics or other aspects. I have also served as a member the New York State Forensic Science Commission since its inception in 1996, created under Executive Law § 995 and the implementing regulations being found at 9 NYCRR 6190 to 93. In that capacity, the Forensic Science Commission in New York is responsible for accrediting all the government operated (state and local) forensics laboratories operating in New York State and conducting analysis of evidentiary materials. Now, as a scientist, one of the issues about validating the methods that you use means that you have to have a theory. You have to be able to test that theory. Hopefully you have published your findings. Hopefully others have reproduced your findings and the methodology is added to the general base of knowledge and has become generally accepted in whatever the relevant scientific field.

When we are accrediting labor in the field of forensics, the standard is that whatever the discipline that they are going to be accredited in, it has to have standards of operation and the methods that each lab uses must be valid and accepted in the community and in general use. Now DNA is exciting, fingerprints are interesting, ballistics are used.

As a scientist, when I validate a method I must be able to establish an error rate of that method. Every scientific method has a limit: it has an error rate. This is not because the technician dropped it on the floor. It is not because they failed the proficiency test. It is intrinsic to the method I am using. I am going to tell you that even DNA, by the methods we use today, has an error rate. The error rate is small. In the field of promise and analysis, 99.9% of the time I was right. If a woman has a pap smear for the detection of cervical cancer and she gets told she does not have cervical cancer, that result is wrong 25% of the time because that's the error rate. Every scientific method has an error rate. Science has errors, the legal system has errors and, unfortunately, some of those errors are often attributable to the overstatement of the value of the science that is describing the evidence. If every statement of forensic science included a description of the error rate and the limitations of the method applied, perhaps we could assist the triers of fact, the jury, in better understanding the limitations of what that analyst is testifying to.

I hope by the end of this morning that if you learn anything, it is that the scientific method is the key element is determining the limitations and the error rates of any analysis that we perform on evidence. If we were better at educating our audiences, whoever they are, and how that affects the information that we are sharing, we might make fewer mistakes in the application of forensic science. Thank you.

John Carey:

I will be brief because I do not have letters after my name, in case you noticed. I have an M.P.A., I just got my Masters' degree in May. I took a brief 32 years off between undergrad and graduate school. This is all about truth; that you've heard a dose of truth today. Steve is, in fact, the biggest DNA geek I have ever met in my life. Every few months myself, Steve, and one of my former crime scene investigators go out for what we call a "girls night," and we go out for drinks with DNA scientists. They all talk at a level so far above my head, I just stare at the bubbles in my beer, so it is all good.

I did not join the New York State Police to become a crime scene investigator; I could not really have told you what at a crime scene investigator was. I joined the State Police because I wanted to be a trooper and wear the cool hat. A couple years into my career, I was the first trooper to arrive at a homicide scene. I would recommend it—it is quite a charge. When the crime scene people got there, it was very antiquated, what was done at a crime scene back in the mid-80s. When I got there I really enjoyed watching what they were doing. The individuals were systematic in the way they collected the evidence and documented the evidence. I had the opportunity to become a crime scene technician in 1986, and in 1987

I had the opportunity to move full-time into the forensic identification unit. I spent the final 27 years of my career in that unit, and the final 19 years of my career running that unit. The changes that I saw were remarkable. In 1987, DNA was something I was trying to forget from 10th grade biology. In fact, 10th grade biology was the highest level of a science course that I took. My bachelor's degree is in music, which I found instrumental in law enforcement. We didn't have to worry about scene protection. We didn't have to worry about who came into the crime scene or documenting who was at the crime scene. As a result, we had police officers leaving fingerprints at crime scenes.

In 1991, I believe it was, when SAFIS (Statewide Automated Fingerprint Identification System) went online, my very first hit was that of a trooper who picked up a piece of evidence for me. It was a check and he held the check in his hands. I had a wonderful double loop whirl thumb impression on the check, which was the first printed during the training phase that I entered into SAFIS and I got hit. The first people put in the SAFIS database statewide were police officers. This was because police officers were most likely to leave fingerprints at a crime scene, more likely than perpetrators. It was mentioned earlier that crime scene, or rather fingerprint databases are great. They can give you candidates, as they are called, but they do not make the final determination as to whether fingerprints are, call it what you will, an individualization, a match.

There are a lot of words everyone stays away from given the fact that the science of fingerprint is under the act. It is always done by an examiner. The way it ran in my unit, at the time of my retirement, was that if one of my investigators made a fingerprint match, it would have to be verified by a co-worker, by a peer review. That was a peer review taking place at the base level. That case then came to my desk, where I had to arrive at the same result. If I did, if I had the same conclusions on the case, it would then go to the forensic investigation center, where somebody not connected to the case, who had no intimate knowledge of the case necessarily, would do what we call the quality assurance review. What would happen there is the fingerprint match would be scrutinized, enlarged, scanned, the latent print itself would be examined microscopically, and then they would make a determination and issue a QAR report. Then and only then could a fingerprint match proceed prosecutorial. I felt that we did what we did, in light of some of the things that happened in the history of the state police and the evidence tampering scandal in the early ’90s involving fingerprints. A lot of times we have something terrible happen that good can come out of it, and that’s exactly what happened. The protocols we established in fingerprints brought the science to a level where it was almost impossible to put forth an erroneous identification. With that said, any science, whether you are talking about DNA or what you are talking about is fingerprints, when there is a human element, you are always going to have the potential for error. It is unavoidable. I was asked by Etell Draw, a scientist I studied under, whether I believed that fingerprints were an objective science or subjective science. I have

to say it is both. This is because whenever you have some degree of subjectivity, you have a human element in anything. I really enjoyed the career I chose; it was wonderful. I am very honored to come here and participate in this. Please don't beat me up because I'm not a lawyer. Thank you.

Professor Christian Sundquist:

Thank you all. There are a lot of very interesting issues to explore. I do have a list of questions that I'm supposed to ask and I believe that I will ask most of those questions, but I am going to use my moderator's privilege to tweak a few of those questions here and there. The first question that I think that we have seen through our presentations and otherwise is just how important is it, how significant is the admission of DNA evidence in a criminal trial? Melissa, I believe you stated during your presentation that DNA is beyond any doubt. Would you like to explore or respond to what extent does the admission of DNA evidence aid the jury's fact finding mission? To what extent can it be seen as usurping the juries' fact-finding obligations?

Melissa Mourges:

I think it is a tremendous help to the jury because it proves the issue of identity much better than eyewitness evidence would or you know, somebody signs in someplace and that's proof that they were there. What I see most often is what it does is it changes the defense. In a sex crimes case, a sexual assault case, even if they were strangers, the defense is no longer, "it is not me," the defense is now, "it was consensual." Instead of "whodunit," it becomes a "what happened." This is almost universal. It is rare that you see any more of the O.J. defense, which would be without the molecules flying through the air. The attack on the science of DNA I see much more rarely than we're just going to change the defense, we are going to embrace the DNA because everybody knows that in general DNA works. That is how I see it.

Ann Willey:

I think we both established that DNA evidence as performed, particularly in New York State by an accredited forensic DNA lab, is admissible. We do not ask that question anymore. We still have to ask the question, what is the weight of that evidence in the context of the case? What is the weight in the context of the analyst

to perform the analysis, instead of the one to have to come and testify? What was their experience? What was their training? What was their prior performance? This is all open to questions. In some cases, the issue has been whether it is admissible, because it's DNA and we all know what 3 billion nucleotides look like, but if a lab has chosen to modify its methods? What about the use of the new method? What about buying a new instrument? What if they decided to get re-agents from a new source? What if maybe they decided to use a new algorithm? For example, when you know those two peaks of short tandem repeats were so close and so we data algorithm split them when the analyst said it was one. Then the second analyst said it was another, and the supervisor said well no, it is both. Those elements of that testimony, again they may be admissible, but the weight of that testimony, and I am going to go back to my claim that one of the questions to the person testifying is, have you established the error rate of that algorithm? If so, how? On how many cases have you tested that error rate or have you used to determine that error rate? That should not be left to the defense because that could be raised as part of the defense.

It is not that you made a mistake, it is that the inherent science has a limit to it, and it does. Every scientific method has a limit. It is better, in the case of a criminal case, that the prosecution is raising those issues as an explanation to the trier of fact. They should be explaining as to why this information is so important, but in and of itself it is not determinative. You can raise doubt about a DNA identity. It does not mean that he is not the perpetrator, it just means the science has a limit. In my opinion, better the presenter of that data acknowledges the limitation then leave it to the defense who is going to do their best to make it sound like you overrepresented and overstated. The admissibility of DNA is not an issue any more; it is about the weight. There have been new methods. Remember in New York, in order for a lab to use a new method, they must go to the DNA subcommittee of the Forensic Science Commission and submit their validation of the process that they went through to prove that result is acceptable within the stated limits. They must document what the error rate is, the predicated value is, positive and negative before the DNA subcommittee then recommends to the Forensic Science Commission that this lab should be allowed to use this method.

Professor Christian Sundquist:

Now, this picks up on something that John mentioned earlier, in his talk. John, you stated that there is always going to be a potential for human error, it will always be present, and I think most of us here would agree with that. Given that observation and the technological advances in evidence that have helped exonerate innocent people, when their convictions were, in part, based on faulty scientific evidence, I was wondering if you or any of the other panelists could speak to whether there still exists a real danger for wrongful convictions based on scientific evidence, perhaps based on the admission of DNA evidence?

John Carey:

Wrongful convictions, I think, are a lot less likely now, because people are awake and paying attention. We have enhancements in all of the sciences, regardless of who is labeling what a junk science, even something as simple as a photo array. A lot of the innocent people, cleared by the Innocence Project using DNA, were probably convicted based on eyewitness identifications, photo arrays, or lineups. When someone is wrongfully convicted, that is a travesty, anything that can be done to avoid that happening is a good thing.

In New York, prior to me retiring, we re-vamped the way that photo arrays were done. You take a victim of any crime, I wouldn't pick on the elderly because I am "the elderly" now, and you show someone a six-pack, a photo array containing six photos. They have been traumatized by some crime, maybe robbed, knocked down, or beat up. What is there first thought, when they look at the photo array, the bad guy is in here, they are in here. They think that they just need to pick the person out. Then they realize that none of them look familiar, what am I going to do. They think that they must help them out, so number four looks fairly close in my mind. So, they choose number four, but they must do better than that. They are asked if they are sure that it is number four. It is so simple and quick, but it can lead to a wrongful conviction.

Everything has to be transparent in every investigation. All the documenting that we do, we spend hours and days inside crime scenes, there is a reason for that. We are documenting things so that there can never be a question about where something was,

where you obtained it from. Speaking from the non-scientific point, just fixing photo arrays was a big deal. I taught in the three levels of fingerprinting training in New York that is put on by the Division of Criminal Justice Services. Level I, Level II, and Level III. Level III was the highest I taught. During Level III, they have to go through moot court and we videotape their testimony, and it is a really good program. There is a very good reason why now they've implemented a waiting period between levels. You have to wait a year between Level I before you may embark on Level II, and then another year before you embark on Level III. The way it is, in most agencies, upon completing Level III and a probationary period, you can offer expert testimony in fingerprints.

One of the problems that I saw, prior to that one-year waiting program, you take a guy from a small PD, anywhere in the state, and they would become the evidence guy. They would say, "Joe, you are the evidence guy" and they would send you to a fingerprint school. Joe went to fingerprint school Level 1, then two and a half months later Joe went to Level II, then four months later he goes to Level III. They then claim Joe is a fingerprint expert. Joe does not look at a fingerprint for the next two or three years. The department then gets a very serious crime. Joe develops a fingerprint at the scene. Joe then sits down with a print card of the suspect they have and the latent fingerprint. As he is doing this, he's got three detectives and the chief hanging over his back, asking Joe if it is him. Well, it's a whirl and it's a whirl, yeah it is him. He then goes and testifies and that is no good.

You've got to have a system, not to toot the horn of the State Police, but our system is very good. To have three people verify, or two people verify, and then an independent quality assurance review, this leaves really no room for error. In order to have some kind of error, there needs to be some kind of mass hysteria that made everybody see something that wasn't there. A lot of the things that have been implemented, just in the past 10–15 years, have really improved the way business has been done. Remember, I was there in the dark ages in the '80s when everybody came in the crime scene, come on I will show you around, this is our body and this is blood spattered, that's all changed. We change gloves between every piece of evidence we handle, because we have to, because of how sensitive DNA evidence is.

Ann Willey:

I suspect that the whole goal of science is progress and innovation. As we developed new, generalizable knowledge by applying new theories to evidence and coming up with new interpretations, we will find that some of the things that we said before might not be correct, or we will find new things that we could do to that evidence to uncover the whole area of DNA. The forensic labs in New York State are currently being asked, by the Division of Criminal Justice on behalf of the FBI, to identify all cases that involve hair analysis, trace analysis of hairs. Particularly, in those labs are the expert analysts, who have performed hair analysis, that is, they got a hair from under the fingernail and they got hair from the suspect and they got the microscope. If the analyst was trained by the FBI lab, the best lab in the world, back pre-1990, I believe it is. The FBI has determined that they perhaps did not adequately mention the error rate in hair analysis. That analyst, who was called to testify about the observation that they had made using criteria for preparing the hairs, you know what color is it, how kinky is it, that they may have overstated the value. In other words, not that this brown hair is the same color as the hair from the suspect, that this brown hair is from someone with curly hair like the suspect. Rather, they said something like this hair came from this person. They have now been asked to identify all of those cases, to notify the district attorneys and the defense in all of those cases, to retrieve the testimony in all of those cases, to determine if hair analysis, scientific forensic evidence, to determine if the case decided on the basis of that evidence, and perhaps no other physical evidence. Personally, I would hope that there are not any cases like that out there. They are not there, right? The defense bar is adequately trained to question the analyst to make sure that they got the error rate right.

Audience Question:

The state has this magnificent lab, is the laboratory available to the defense lawyers? If it is only available to the prosecutors, is that just?

Ann Willey:

The system or the evidence as it is analyzed?

Audience Member:

Can the defense lawyer submit material to be analyzed?

Ann Willey and Melissa Mourges:

I do not think so.

Ann Willey:

It raises a different issue. There certainly are private, non-governmental labs. In New York State, forensic toxicology labs and forensic DNA labs operated by entities other than government entities must be certified by the New York State health department, and their evidence is not admissible, under most circumstances, including labs out of state. I think there is a distinct difference between the expert offering an opinion as to evidence tested by someone else, state police, and the testing of.

One of your questions is, does the defense bar have access to the material?

[Undiscernible audio from audience member]

Ann Willey:

I think it is an interesting question. You should know that on the Forensic Science Commission, which is one way to look at all of this, that it is well represented by the defense bar. Some of the most outspoken members of the Forensic Science Commission do raise these issues, about access by the defense bar (1) to the raw data and the documentation that comes out of the investigation and certainly out of the labs, (2) and access to the material, and requesting an aliquot of the material to be tested in a second laboratory.

[Undiscernible audio from audience member]

Professor Christian Sundquist:

Is this an access to justice issue? Should our procedural laws be modified in order to provide better access to DNA evidence and potentially exculpatory evidence? Is this a constitutional right to hoarding the access?

Melissa Mourges:

In New York, where the defense bar is relevantly well-funded, and the legal aid and institutional defenders, the defense attorney will submit a request to the court for public funds to hire DNA experts, for public funds for DNA testing by private labs, or that they want a fingerprint expert. This is all made available. I have not seen a situation where it has not been, and I really cannot speak to a smaller jurisdiction. What I do know about the OCMJ lab, is that the defense attorney is equally welcome to come and have a trial prep with the criminalist as the prosecutor is. There is no rule that the prosecutor is invited to this, they are not specifically. I cannot get a criminalist tell me what the defense attorney wanted to know.

I think that perhaps more defense attorneys should be availing themselves of this right, then do. The same way that I walk into OCMJ with the forensic biology file, which is the exact same file that I am obliged to turn over to the defense well in advance of the trial. I walk in and sit down and talk with the criminalist and say, "walk me through this." The defense bar, according to the rules of the OCMJ, has the exact same right and access.

Professor Christian Sundquist:

I am going to circle about to an issue we discussed briefly, and it relates to this current discussion as well. Steve and I were talking before this panel began, and he mentioned similar remarks during his presentation, that perhaps one struggle we have is to locate the sweet spot between junk science on the one hand, the sort of scientific evidence that may confuse or mislead, or distort jury decision-making, and rules of evidence that will allow juries to be presented with useful information that they can use to exercise their functions. With that being said, unfortunately there

have been miscues at forensic laboratories; there have been some failures at laboratories throughout the country on the processing and handling of forensic results. There are a couple of key reports that came out that I know our panels are familiar with. One is a national research council report in 2009, which generally stated that the procedure involving DNA evidence was reliable and sufficient, but due to a lack of funding, staff and accreditation standards, they found that much of non-DNA science could lead to unreliable results. Most recently, this past month or so, the President's Council of Advisors on Science and Technology issued a similar report mirroring in some respects those conclusions. I suppose my question is, what can we do to prevent those failures? What steps are already taking place and what additional steps should we perhaps consider to stop unreliable evidence from being presented at court?

Ann Willey:

DNA has spoiled us all. The molecule is a remarkable chemical molecule. It is remarkably stable and easy to manipulate, not in a bad way, we can take it and amplify it and sequence it. The technological error rate, if there is DNA present, and our ability to amplify that DNA using polyamorous chain react to a chemical process. The error rate of PCR, which has an error rate, which introduces errors in the sequences of DNA that it copies, but we can calculate what that is. Once I have enough DNA, I can put it into my sequences devices, either for the actual sequence or the short tandem repeat sequences. The error rate for each of those technological chemical processes is known. When I multiply out the error rate, the analytical error rate in DNA, because of the remarkable biology of the chemistry, is very small. When we talk about the reliability of DNA analysis, yes, we can get to 99.99%, and that is before we talk about comparison and probability of matching. The error rate of the probability that ballistic marks on a bullet are going to be identical, physically, after shooting the gun ten times, into the same piece of jelly. If you take those bullets and line them up, there is a physical error rate. The marks will not be the same as the tenth on the first, or on the fifth bullet as it was on the fourth bullet. It is not a matter of the order, it is the physical attribute of the molecules. The error rate in ballistics is not .0001, it is, I am not sure, but probably in the 15–20% rate. What we have to do is better educate ourselves, that reliability of forensic evidence, we cannot expect it to be what it is for DNA. That does

not mean that it is not good forensic science. It does not mean that the analyst made a mistake or that it should not be admitted. It just has a limit.

Stephen Hogan:

A lot of folks are familiar with the council report from 2009, that the professor mentioned. As an administrative and practical matter, especially since we are supposed to be talking about evidence and cutting-edge forensics, what came in the wake is what we now have, which is the National Commission on Forensic Science. That includes its various subcommittees and its connection to the National Institute of Standards in Technology (NIST). They have been promulgating best practices and trying to work to improve the overall methodology, having realized that county-based lab systems do not have a monopoly on the kind of improvement that we should perhaps want collectively. There are a lot of federal resources that are going to increase the benchmark for quality. This is so that we can all enjoy greater confidence and forensic results across the board. What is interesting about that, especially concerning evidence, is the way it sort of sneaks in. For example, minding my own business to a certain extent, I get a call from the state crime lab director, Anthony. Anthony is from Buffalo and SUNY Albany and was kind enough to bring me here. John Simmage, who is the lab director, he said that they do not use "generally accepted" in the relevant scientific community anymore. I think to myself, "oh dear God, when I went to law school I learned, you know, offer, acceptance, consideration, and my whole world is going to come apart." I asked, why that is, and he had said that it was because the national commission recommended, by follow-up letter from Loretta Lynch saying you shouldn't be using it. Additionally, followed by the potential prospect of federal funds being diminished. The next thing you know something that happened in the 202 is changing something that happened in the 716. There [are] sort of two veins going on here. There is the improvement that is sort of through the national commission and various experts. There is also this evidence piece. We would be right to think our sovereign, our evidence, statutory, and common law should be decided by us. As a practical matter, it may be changing under our feet, and I think that's kind of interesting.

Ann Willey:

That is what gets it in. Now how reliable is it, is the underlying science.

Professor Sundquist:

I think one last question. During your presentation, Steve, you had a few slides that referenced the fact that, as we expand the grounds upon which DNA samples can be collected, and as CODES itself expands, that there has been a greater possibility of solving cold crimes and certainly a greater use to law enforcement generally. My question to everyone, not just Steve, of course, is whether you believe limits, from a constitutional or perhaps a mere policy perspective, should be placed on the collection of DNA samples? As you are all aware, there has been an expansion of so-called genetics surveillance within the last two years. The Supreme Court, in *Maryland v. King*, upheld a state statute which allowed the collection of DNA samples from arrestees suspected of committing serious crimes. This was a significant change in the law in some respects, you may disagree. Many federal statutes until then allowed the collection of DNA samples from those convicted of certain offenses. I was wondering if you could speak to that?

Stephen Hogan:

I'd be happy to. In the open forum, I would be particularly interested in what you folks all see. That is because this is one of those clarifications issued because *Maryland v. King* was a bit of a Super Bowl, there was a buildup to it. It raises very interesting questions. It was decided largely on, most of you have learned the special needs exception and arguments that DNA profiles, my DNA profile, is a series of twenty sets of numbers plus the XY designation indicating that I am male. It's generally unique.

What happened in King was that it was determined that, for pedigree purposes, that a DNA profile is very similar to your fingerprint. This is, in the sense that it was unique to you. Although we actually have, I believe, seventy identical twins. This is because if you're a monozygotic twin, you have the same DNA profile, and you can have a legitimately based evil brother who actually did it, at least from a forensic standpoint. We have had to do a lot of work, as far as that is concerned. At the FBI lab in Quantico, people rotate through each other's sections. The

fingerprint folks like to torture the DNA people because the DNA people are Mom and Dad's favorites. They say it is the only forensic discipline that can distinguish identical twins because of random fiction matches.

Melissa and I had been talking about a case. Twenty-two years ago, in West Village, East Village a person was raped at knife-point. We had said that the John Doe indictment and the cold case project, among other things, that she has worked on, this guy was arrested as a result of, I do not think that this word has been used in an academic form, "Paul Blart encounter." He was fishing coins from a fountain, the Fort Lauderdale mall fountain. Paul Blart took issue with that and took a bite out of Paul Blart, felony assault upon the Pinkertons. They took his sample and it hit to the vagina swab sperm sample of this case. He was recently convicted. This was great stuff for that woman and your colleagues. The case was ultimately dismissed. This was because they didn't find sufficient injury or whatever it was, for the Paul Blart part of this. A cynic might say it is dangerous to give the government the opportunity. We are often being asked to run this person through the DNA database. I am, in some respects, the DNA databank no-ticky-no-searchy. You do not get an offender DNA profile through our lab unless you submit a hit letter, with 75 bells and whistles settled. A prosecutor that asks me "can we have a little nip" or something like that, I would say something if you can do five years solid in Wendy, then sure you can. We take this, the databank has very limited use. Some have argued that cops would make bullshit arrests, and if it goes away at least they leveraged this mass search tool. There is probably a legitimate basis for that skepticism. How does that measure up against the societal benefit? Then you take it to the next level.

To me, the interesting question is, I know of some important cases that have been solved by familial search strategies, but there the other issues, the privacy issues are, I think, really compelling. This is what I love about this. As you folks work in your law careers, especially those who are in criminal justice, you know where the rubber meets the road. This is where some decisions need to be made. Hopefully, that's where we can find as much common ground as possible because the cornerstone of all this is the truth. At its best, DNA properly presented is the silent witness. It is without fear or favor, reports its results and conclusions go with what they may. We will never get to perfection; we will always be trying.

Ann Willey:

As far as that question, as to when we should collect DNA, understand that the New York State health department is in possession of DNA from every infant born in New York and they keep it special. They have started keeping them back from 1997. They currently keep them for 7 years. None of those samples and their DNA have been analyzed for medical markers. None of the samples have ever been used for forensic purposes. They have been used for civil litigation purposes: parentage, child identity. We have DNA, potentially, from everyone born in New York State. We have used it in criminal prosecutions. The same DNA, just different methods.

Remaining questions from the audience.

III. PANEL TWO: THE ROLE OF TECHNOLOGY IN ADVANCING EVIDENTIARY PROCEDURES

Rebecca Harp:

I would like to welcome everyone to the Albany Law Journal and Technology symposium. I would like to thank again our moderators and esteemed panelists for dedicating their time to participating in today's symposium. Our moderator for the second panel is Professor Michael Hutter. Professor Hutter has been a faculty member at Albany Law school since 1976. Currently, Professor Hutter serves as a Commissioner on the New York State Law Revision commission. Professor Hutter teaches New York Practice, Conflicts of Law, Trial Practice, Evidence, and Business Torts. Thank you very much, Professor.

Professor Michael Hutter:

Thank you. Good afternoon. The second part of today's program is billed as the Role of Technology Advancing Evidentiary Procedures. Essentially, you should view it as CSI on steroids, in addition to the idea of what technology has done and revolutionized. As I can think back with my 40 years here, and what we're at now, just the legal side. In fact, the law school had no electronic research, nothing like that. It was not until 1982 that the law school first got a Lexis terminal, a single terminal. The terminal used to be in the library sitting right in the middle. Now, obviously, technology is all over the place. We certainly cannot

practice without technology. Not only is it assisting lawyers, but certainly in the profession of law enforcement. It becomes very critical to see all of this and how prevalent electronic evidence is. Back in 1999, when electronic evidence really started coming to the forefront, a very distinguished federal judge in Texas, when he was asked to admit a posting on a social website and he said, not in my courtroom, this is voodoo evidence, we will never ever let it in. Now fifteen years later he is eating crow, and recognizes that, yes, there are a lot of problems with electronic evidence, but with carefully laid foundations, like reliability established, it can come in. Now we are in the midst of this revolution.

Our speakers today come with very vast experience in this area, and a well-rounded background. Just briefly, you have the bios in the pamphlet, and then also remember that a lot of us put together some papers and they're available online with the program materials. Our first speaker will be Michael Deyo, who is an assistant counsel for the New York State Police. Before the state police, he practiced doing litigation with an excellent Albany law firm, the Cunningham Isman Firm. He comes now with some very broad-based experience in this area, especially with the state police, with the work he's been doing. Next, we will then hear from Michael Fox, who is an adjunct professor at Mount Saint Mary's College and a special counsel to the Newburgh law firm, excellent litigation firm, Catania, Mahon, Milligram, and Rider, in which you have been involved in doing a lot of work with electronic evidence, especially e-discovery. Next speaker will be Terrence Kindlon. I think most of us know who Terrence Kindlon is. He is exploited as being one of the more veteran defense attorneys in the area. Terrence has been trying cases for about 42 years throughout the capital district and elsewhere. He obviously now is going to bring to you his experience in dealing with all, and now keep in mind that he is the special director, head of training of the Albany County Public Defender. Our last speaker is a very distinguished, retired now, unfortunately, I think lawyers will say that, is Steve Herrick. Mr. Herrick sat for many years as the Albany County court judge, presiding over a lot of the trials, hundreds if not thousands of trials. He will bring a unique perspective from being the judge in a lot of these cases involving electronic evidence. Mr. Herrick now has a new position as the Public Defender in Albany County. As you can see, we have a very well-rounded group of presenters that will bring some very good insights into this area. We will start with Mike Deyo to give his material presentation.

We will go through each presentation, then I will start posing some questions, then there will be time for questions from the audience.

Michael Deyo:

Thank you, Professor Hutter, and thank you for inviting me here today. I teach here at the law school a course on Wednesday evenings titled Electronic Discovery. I have been teaching that now for eight years here at Albany Law and couple of semesters at Western New England College of Law as well. What we talk about in that class is a broad range of the issues that are presented through the use of electronic evidence in civil and criminal proceedings today. We are going to touch on probably many of them here today.

I thought what I would do first is to take an opportunity to describe the nature of the work that I'm involved in today, and some of the challenges that I see with respect to electronic evidence. As Professor Hutter said, I'm currently in counsel's office for the New York State Police, and in that role, it truly is the General Counsel's office for a large organization. Not unlike a corporate organization, we face issues pertaining to personnel, finance, litigation of course, and various types of contracts and transactions. We do so with a very specialized view on the enforcement of criminal laws in the investigation of criminal offenses.

Part of what I do is I manage a caseload of civil cases, both in the Court of Claims and in Federal District Court. The Attorney General's office, of course, is the attorney of record on these cases. Our office is in charge of managing the cases. A big part of managing litigation today is managing electronic evidence; it's managing the volume of electronic records that are relevant in litigation. Some of the challenges I see right now with respect to civil litigation that we are working through are really the challenges of volume, and the challenges of cross-jurisdictional problems that arise. In terms of volume, lawyers today are left with the task of finding what's relevant within literally a sea of noise, the sea of noise that I talk about is everything that's contained on any organization's email system, servers, backup tapes, any other data sources that might exist and trying to pull from those pieces of relevant useful meaningful evidence in the context of litigation. This is time-consuming, expensive, and sometimes requires some specialized expertise. Managing that volume is a challenge right now.

The other challenge is, of course, jurisdictional issues. In today's interconnected cloud-based world, data, of course, is no longer at corporate headquarters, rather it is kept throughout the world. Dealing with the trans-border issues that arise between privacy laws and discovery, keeping in mind that United States laws are typically inconsistent, if not completely at odds, with international laws in this respect, requires some careful consideration and can sometimes be difficult to navigate through the discovery process. Looking to the criminal side, the other piece of what I do is that I provide legal support to the statewide intelligence operations for both criminal and counterterrorism operations that are run out of the New York State police fusion center. The Department of Homeland Security has set up so-called fusion centers throughout the country. The fusion center that serves the state of New York is operated by the New York State police. The fusion center performs intelligence operations with both a criminal focus and a counterterror focus. The legal issues that often arise come about in the context of uses of surveillance technologies and ensuring that individual civil liberties, civil rights, and privacy interests are upheld. Of course, we have competing interests of privacy and safety.

In a perfect world, we would all have total privacy and complete safety but the two cannot coexist together. There are constant trade-offs and balances and compromises between privacy and security. The world of the Fourth Amendment laws, as we know it, evolves constantly and is ever-changing and depends upon what's happening in the world that we exist within and contemporary views of privacy and government technology, used technology by government. Electronic evidence and surveillance techniques are becoming crucial to law enforcement right now. Criminals, of course, are using technology to facilitate crime and it's incumbent upon law enforcement to use advanced methods to detect and prevent crime. In terms of challenges that are faced today, the two biggest challenges are really different forms of the same thing. The biggest challenges are the phenomenon that's called "going dark" and a related phenomenon which is encryption.

Encryptions are probably well-known to everybody here; it is simply a method that can be employed to render data unreadable, indecipherable. The problem, of course, is that once data becomes encrypted, it cannot be viewed. It can become encrypted while transmitted from point A to point B or can be encrypted while stored on a device. The challenge is that even if law enforcement

can establish probable cause, that a neutral detached judge signs off on and issues a search warrant to search a computer or cell phone or any other electronic device, that search warrant is worthless if the police cannot read the data contained on the device. Without a method to decrypt encrypted information, no effective search can be performed.

We are probably all very well aware of the DOJ Apple controversy that occurred last year. It played out very publicly and it highlighted very public challenges the law enforcement is facing today. The "going dark" phenomenon is closer related but somewhat different. There's a complete underbelly of the internet today, which is the "darknet." Things like Facebook, Twitter, Amazon, and eBay, they all operate on the public internet. There are different applications and different corners of the internet that operate on what's called the dark web. These areas cannot be accessed unless specialized software is utilized to view those areas of the internet. When criminals, including potential terrorists, switch from communicating with one another over publicly-available, publicly accessible sources that can be monitored, using appropriate, accepted means under current jurisprudence, and instead go to a dark platform that law enforcement cannot track, they simply go invisible. You can be tracking activities of the terrorist cell for months, when they decide that it's time to go dark and they go to one of the underground communication platforms and their communications simply stop.

The question becomes, have they stopped communicating because something has happened to one of them because their plans are no longer in place, they are no longer going to carry out what it is they were talking about, or have they advanced to the next level? We simply don't know because they have gone dark to us. This leads us to not knowing what's being done out there.

This is just a summary of the challenges that I see today with respect to electronic evidence. We can talk about reliability and hearsay basic evidentiary issues. Those issues are being hashed out in the courts right now. The other issues are the more practical issues that are facing both the civil and the criminal side. I look forward to a more thorough discussion of all these topics. Thank you.

Professor Michael Hutter:

Our next speaker will be Michael Fox.

Michael Fox:

Thank you very much, and thank you for having me here today. We were hearing earlier about the dinosaurs in the DNA panel. We don't have to look as far back for some of the dinosaur-epic of technology in the courtroom and technology in discovery. As Professor Hutter mentioned, 1999 was a time when judges would look at this as voodoo evidence. We do not have to go that far back. As far back as 2005, we had paper discovery rules that had to be analogized for purposes of electronic discovery. In 2006, the Federal Rules of Evidence and the Federal Rules of Civil Procedure had amendments that started coming through. Now, we have specific mention of electronic discovery rules for electronically-stored information. That then led to an explosion of case law, court rules, procedural rules, and ethical opinions concerning electronic discovery, electronically stored information, and everything that stems from that, including things like jury *voir dire*. If you are selecting a jury, can you research the jurors on the internet to understand better what their thoughts, what their predilections might be within relevant ethical guidance? Accessing electronically-stored information, can you access that? Absolutely. So, we will go into some of that now briefly. You have a lot of material but let me hit the highlights, since we won't go into all of the materials.

Electronically stored information and discovery: email, Twitter, Facebook, MySpace, anything and everything, voicemail, and text messages all are now subject to electronic discovery rules and discovery demands. When you think about electronic discovery almost anything is encompassed within that. If you don't take a piece of paper and write a note, and that note never sees a scanner or digital camera, and that note is then taken and shredded, burned or thrown in the garbage, that's about the only thing that we have these days that is not in some way tied to electronics. Billions of documents every day are created electronically, whether on Word or Word Perfect, by text or email, or any other fashion and that all leads to electronic discovery. Then you have the metadata behind that information, data about data.

Sometimes you might have a smoking gun in there. For example, you have an employment case, where there is a termination, and there's a suit for wrongful termination based on discrimination. There may be a defense that's put forward by the defendant, where there is a write-up and the defense says this is the write-up that was given to the employee prior to their termination, and it set

forth what they had done wrong in violating workplace policy and they were terminated. There have been cases where the metadata for that information was requested—the data about the data, in the WordPerfect or Word file— and it showed the document was actually created after the termination. A case may hinge on that very issue. It is cutting-edge stuff, it is important; and it is potentially relevant and admissible in court. We have authentication issues. For authentication, you have a piece of electronic evidence—it is a Word document, an email or text message—there have been cases, criminal cases, where text messages have been cut-and-paste from the phone to another document. That was admissible evidence because the victim on whose phone the text message came through testified about those text messages, and there was corroboration by a detective who had seen the information on the phone and had corroborated that the information that was in the cut-and-paste was a reasonable likeness, it matched the information that had been on the phone. That was admitted into evidence.

Now that's a simplistic review of the case. What do we have for authentication, one, we have to authenticate the document; two, it has to also be relevant; and then, after all of that, there may be other layers of evidentiary issues, such as hearsay, which you need to overcome. For example, the case *United States v. Vayner,* Second Circuit 2014. In that case, in the District Court, there was a conviction. The Second Circuit reversed and remanded saying that the District Court had not properly allowed the authentication of the evidence - it was as if the electronic information were a flyer on the street, and the prosecution picked-up the flyer, attributed it to the defendant and obtained the conviction. But, there was no showing the flyer was in any way connected to the defendant. The same thing here [in the *Vayner* case] with the electronic information, there was no showing the electronic information was connected to the defendant. There was nothing showing that defendant had any control over it, exerted any authority over it, exerted authority over the content, creation, or the promulgation of the information. The Circuit said there's a base level here under Federal Rule 901—the base level of authentication of connectivity to the defendant hasn't been shown. There was a reversal and it lead to a whole series of cases on authentication.

For example, then we had *Louisiana v. Smith*, 2016, this year. New Orleans police officers offered evidence in the form of

Facebook posts, which were allegedly made by the defendant. The trial court denied a motion to exclude, the appellate court reversed it. You need at least "circumstantial indicia of authenticity" is what the court said. Circumstantial indicia of authenticity. The prosecution in this case did not have the option of presenting the testimony of the alleged creator, the defendant, because it was a criminal case. The prosecution needed to present circumstantial indicia of authenticity in some other fashion. This could include testimony of others, such as forensic evidence, witnesses - as in the other criminal case with the text messages—you need some circumstantial evidence, some circumstantial indicia of authenticity, in order to use the information. There have been cases where websites have been proffered. You would think that a website, where you type in the URL and the website comes up, that the court could take judicial notice of that website. The courts cannot by and large take judicial notice of websites. Something has to be presented to the court, in the form of evidence—perhaps a witness who typed in the URL and the URL brought them to the webpage, and the webpage is for Albany Law School. They typed in *www.AlbanyLaw.edu*, up came the main page, they've seen it 100 times before, that was the page. This may be sufficient, but you need somebody's testimony providing information authenticating what was there on the website, not judicial notice. Your problem may be worse if you have a situation where a website is being used and the party against whom the website is offered is saying that's not my website, I did not create that, I have never seen it before. It is not a matter of a question of "okay was something else posted on there," but it is the entity's website. No, the party is saying, "This is not my website. I have never seen it."

Now you have to go deeper, now you need an expert witness, perhaps a forensic expert, who can go behind the information on the computer. That expert can say when the URL was typed in it brought them to this website, they compared the IP address, the server address connected to the service provider, something more to give indicia of certainty and authenticity to it. Again, we have Federal Rule 901.

You also have the hearsay rules on top of that. There are many cases where you might have a situation where it's authentic, it is relevant, but it is hearsay. There have been cases where the parties on maybe a motion *in limine* have not addressed the hearsay issue in defending why that evidence should be admissible, and the courts denied admissibility based on hearsay.

Although it's authenticated and although it is relevant, it is that last hurtle. Keep that in mind when dealing with authentication of information.

Just finally, and there is a lot more in the materials, so look at that. One thing to keep in mind is that our electronic world is constantly changing. Aside from the discoverability of pretty much anything electronic that we touch, there is a growing wave of service of process by electronic means. Not just using information in court as evidence, but actually hauling someone into court to begin with. There have been a series of cases now, and a growing trend, that if you have an individual who cannot be located in any other fashion—you do not have a physical address whether it be business or residential—but they are actively on Facebook, email or Twitter, and there have been interactions. There are cases in the materials where they cannot find the individual physically but they can find them because they have been emailing back and forth. There was a family law case where the spouse that they were trying to find had recently posted and liked Facebook photos of the other spouse, so they knew it was an active account. The courts have said that if there is a reasonable degree that they could have notice to understand that there is a litigation pending and that they are being hauled into court, and it is reasonably calculated to provide notice to the party that is being served, then service can be accomplished by electronic means alone. In New York, it would be under 308(5) of the CPLR. You can be served by Facebook or Twitter account, there are cases out there like this now. Our world is really becoming digital. Our world is really moving from paper analog to online in almost every form and fashion. It is a cutting edge brave new world. Thank you.

Professor Michael Hutter:

Thank you, Mike, our next speaker will be Terrence Kindlon.

Terrance Kindlon:

When Rebecca called me on the telephone and said would you come to the Journal of Science and Technology Symposium, I said, "Okay but why me: I am neither scientist nor technologist?" I said that the last technology that I held in my own hands was my amateur radio station 50 years ago, when my call sign was WP to

FNA. I jokingly said I can do this in Morse code if you like since that's about as technological as I go. She then explained that it is from the lawyer's perspective, and I think that I could handle that.

One thing that I want to say that relates back to the first panel on DNA, one of the speakers spoke about a case in Rensselaer County where two men named Baptista and Barry, were exonerated by DNA. This was a horrible case involving a murder that took place actually ten years prior to the trial in the case. It was ten years prior to the indictment and then there was another trial. What had happened was Baptista and Barry were what we in the criminal defense lawyer business refer to as the usual suspect. You know they were both a couple of guys who had a checkered past. The case involved very emotional elements and the Rensselaer County District Attorney made a terrible error of judgment and indicted the usual suspects. They were brilliantly defended by a couple of lawyers from over that way. About a month before the case was set to go to trial and it was a murder in the first-degree, that is life without parole if convicted. Overall a conviction of this used to be a death penalty offense before New York eliminated the death penalty.

About a month before the case was set to go to trial, CODIS system set up a DNA hit. What happened was a man from Saratoga County had gotten into a domestic dispute with his fiancée at home, and he was taken down [to] the police station. When he was taken to the police station and they took his DNA sample. Unbeknownst to him, it hit. It hit on what had been DNA left at the murder scene. This murder scene was worse than anybody's worst nightmare. It was a place in which a man and a woman were both killed, each was stabbed over 35 times, with a knife, pen, anything sharp that happened to be around, it was just a horrific scene. I have to say even though I am a defense attorney, that the police were brilliant in this case. This is because they knew that just having this guy's DNA at the murder scene wasn't going to be enough. They knew that somebody would be able to walk him away from the charge, which was coming. Instead they decided to talk to him. They talk about the dead guy. Well it turns out in the conversations that they had with this defendant, future defendant, rather than exercising his right to remain silent, he started to talk. The police recorded these conversations and the police also recorded every telephone call he made from the jail to his finance, in which he discussed the cases. What happened was they had his DNA at the murder scene, there was blood

everywhere, the walls, ceiling, bathroom fixtures, and in the bedroom underneath a mattress on the underside, there was blood. This blood contained the individual's DNA. The police did not tell him about the DNA, they just talked to him, until he dug himself a deep hole making up excuses for something that he was not even being accused of. When they finally pulled out the DNA the case was basically done at that point.

Then they also had the series of conversations on the telephone electronic part with his fiancée. He was very stupidly trying to make her make-up an alibi for where he supposedly was at the critical moment. The DNA in that case, first, exonerated two men who were falsely accused, and secondly ended up indicting my client for murder in the first degree. We had what I thought was a fascinating five-week trial in Rensselaer County Court. I kept thinking of the Hatfields and the McCoys because two families were involved in the court with one side of the courtroom full with my client's relatives, and the other side was filled up with the decedent's relatives. They were snarling at each other, and coming into court every day was like walking in galt—it was incredible. After five weeks and two weeks of jury selection, I regret to say that he was he was convicted. This is a classic perfect example of DNA not only exonerating two innocent people, but also resulting in the conviction of a person who the jury, Appellate Division and the Court of Appeals have all determined that had committed the crime.

As a criminal defense lawyer, I just want to give you a few examples of the kinds of things that we run in the electronic medium. Some of these things are things that I've experienced in my own practice in last couple years. One of my favorite things is Facebook because it is a gold mine. Facebook is an amazing idea. I have that image in my mind, you know the treasure chest with the big gold stick out the top. My wife Laurie Shanks, who was a professor here for many years, and I, we defended a very difficult, very gruesome sex case early this year. It was our position from the beginning that the complainant, who was a 14-year-old girl, was lying. This is not a popular position to take in front of a jury. Juries do not want to hear when the name of the crime involved is predatory sexual assault of a child, some old man come in the court and stated that kid is lying, but she was. We knew it and we were able to conclusively demonstrate with her Facebook information. The information was right there for anybody to walk up and get it, you didn't even have to be her friend and I wasn't her friend. At

risk to be a little bit vulgar, my favorite part of the proof that came from the Facebook information was this this young girl considers herself to be a better than artistes when it came to make up. One of the things that she really did, and I have the Facebook page to prove it, one of the things that you really did was she had a category called "Dicks can be Pretty too." She would decorate with makeup the penis of some of her adolescent friends, who were obviously guys. It was right there on her Facebook. My client was vilified, he was a very respectable guy, and he was vilified. His bail was set at a quarter of $1 million, he was lucky he was not killed in his neighborhood by disgusted neighbors. Once we got past the "dicks are pretty too," it was all downhill from there.

In the criminal defense world, we also run into issues with confessions. When I was a young lawyer, I use to always complain and say what Thomas Edison invented sound recording in the 1800s, why is it that these always people are confessing and we can never hear an audio. The reality is that sometimes the individual does not say what they need to say. So, let me just tell you about a videotape confession and this case as actually from this year, January of this year, my client was charged with a serious assault. In the case, it was about 98% depending upon the confession that he gave to a police officer during 3 1/2 hours before video camera in the police station in Albany. My client had been around the block, don't think I'm saying he was an angel. We had real trouble with the electronics in this case. In fact, I was on my fifth DVD of the videotaped confession before I got one that worked. It came just at the last minute. It came on New Year's weekend. In the videotaped confession where my client laid out all the details about the assault, the police officer—and he was not a kid—he had to begin by giving the Miranda warning. Now, I've got a ten-year-old grandson who could recite the Miranda warnings word-for-word—it's not a secret. The Miranda warnings that the police officer gave some my client, "Mac you know that I need to tell you about your right." Mac says, "Right." The officer says, "You know that you have the right to remain silent and all that shit right?" Mac says, "yeah." Then the officer says, "Are you good with that," and he got no response. That was the Miranda warning he got. In my 42 years of practicing law, I never saw anybody blow the Miranda warning. It was my great fortunate that the toughest judge in upstate New York, Thomas A. Breslin, himself was the judge presiding in this case. I finally got this DVD on the weekend and I needed to track down a court reporter to transcribe the first

20 pages and attached those to a motion. First thing I guess it was the Tuesday morning I think, and I said, "Your Honor I have to make a motion to dismiss." The judge goes, "You know you're a little late aren't you." I explained that there was some new evidence that became available to me and said it's a DVD of the statement of the client. I said this is a transcript of the statement that my client gave Officer McGillicuddy. The judge read this and said to the District Attorney that you surely have a written waiver, and the District Attorney said no. The Judge then says to me, "Do you have a motion," and I said, "how's that," and the judge said, "Granted." My point is that I am not here to tell war stories but a defense lawyer is going to look upon this electronics stuff as just a wonderful new world to go into. There is so much out there with electronics. You know there's always the result of the human factor you know about the warnings don't you, that sort of thing. A couple of other things that we defense lawyers have to put up with these days or have to deal with is sometimes we have some videotapes of actual crime itself being committed. I had a great videotape of the guy taking a rifle and shooting at somebody who was running down the street in Troy. There wasn't too much dispute about what had happened. The jail phone calls are always recorded now, always. They are not only always recorded but they've gone digital. What happens now is every call that a defendant makes from the jailhouse to his mom or his girlfriend or co-conspirators or whomever is recorded and it's digitally recorded and the recording company, I think it's a private contractor, makes a print-out. This print-out is then provided to the DA and eventually to the defense lawyer if you're lucky. Those jail phone calls can be a killer because people convict themselves all the time by what they say on the phone from the jail. Text messages are another gold mine. Authentication is another issue, and this is the last one I will tell you about. I had a case a couple years ago, I did not do the trial, just the appeal. There was this guy in a nearby community and what had happened was he had gotten really drunk and so had his friend. They came home that night after drinking; these are two guys who have had a relationship with each other. When they were in college, they had a sexual relationship but one of the guys had lost his interest in homosexual contact, and my client had not. What happened was there was a video camera in the bedroom of the house. My client, by the way, shared this apartment with two women who were both straight women and he was he was a gay man. There were three bedrooms

in the house. My client was there with his friend from college who was visiting, and what my client did was he performed an act of oral sexual intercourse on his passed-out friend. My client recorded this and then forgot that he had recorded it. The video tape was not his that he recorded it on, it was one of his housemates. You can't make this stuff up. He left it where it had been, and the woman didn't look at it for a couple months. Then, one day she was going to go out and film a soccer game or something and she sees look at it and she saw that there was something recording on the machine. She watched it and said, "Oh my God" and she called the police. and the police then went forward. Without doing anything except looking at the video tape of showing oral sex that was performed by my client on his drunk friend, they charged him with a number of serious felony offenses. He was arrested and charged. There was a motion to suppress that was made; it was sort of a boilerplate one. They played the video at his trial and he was convicted. He got giant numbers, it was like 27 years, it was an enormous amount of time, and that is when we got involved. The whole appeal was based on the failure to authenticate the video. The Third Department said, "Yeah you're right" and they tossed a couple of counts and they sent the rest back down for a retrial. He made a plea bargain, and he's out today, not locked up. You know it can be such a joy to get this stuff even if you don't exactly understand the technology. If you understand the technology that is great, if you do not you go talk to smart people who understand it and have them explain it to you. I'm proud to say on behalf of my boss, Judge Herrick, we just had two acquittals right in a row in the public defender's office in Albany County. In these cases, the acquittal came because expert witnesses were called. I just emphasize for those of you who go into public defense or trial law of any sort, you can't try a case without an expert witness anymore, I don't care how smart you are. We used to carry little books like this to look things up, and now I got everything from the federal rules to Lexis on my iPhone so I can find a case in court if I need it. Thank you very much.

Professor Michael Hutter:

Thank you, Terry. The next Speaker is Judge Stephen Herrick.

Judge Stephen Herrick:

What I came prepared to say will take about five minutes, so I am going to continue with a war story or two. I will take it from R rated down to PG. For any of you who did not know I am now the public defender, Terry was the acting public defender. I was a public defender before most of you were born. I was an assistant public defender with Terry, then I was in private practice. Following private practice, I was a judge for 22 years. I am electronically deprived because I had a law clerk, a secretary and staff that took care of that. So, I go back beyond hand radio operator, I don't have the call number. I also don't have Lexis on my cell phone. I want to tell any of you who go into criminal law, when I was the city court judge for seven years, here in Albany, it was a very busy court. It actually used to be called Police Court because it was in the police station. When I was there, I would argue with the police chiefs, there was a series of them, asking why don't you video or tape record statements by the defendants. You would hear about a three-hour interview and you get a single sheet of paper that is supposed to be what the defendant said while in custody. It didn't serve anyone's purpose, in a misdemeanor case, which is what I was handling down there. It basically, in many cases, prevented ongoing prosecution. If you recorded it, it also would protect defendants' rights. I think the last week that I was there, one of the staunchest opponents to having a recording done at the insistence of the defendant, he said he'd only talk if they taped it! That is the first time, to the best of my knowledge that the Albany police recorded an interview.

We were then trying to get audiovisual recording of interviews and it took years of me as a county judge to push the Albany police and other police agencies to do that, and finally with some state and federal funding they did. They were very reluctant to do this because they thought it would undermine their investigative ability. It turns out, and you should be aware of this if you practice defense work, it is the greatest tool to convict someone even if it turns out that they were not guilty. This is because the police in their interviews, and the jury gets to hear the interview if it is not suppressed, the jury gets to her the entire video. The police will go over and over their theory, so that the jury will hear it five or six times, and the defendant is just still there and saying no, or acquits to certain things. The interview goes in and the jury gets

to hear the entire communication between the defendant and usually two police detectives.

If you are representing anyone in a criminal proceeding, as we now tell all of our clients, do not saying anything to anyone except your attorney. One other thing about electronic evidence, in most cities, including Albany, if you are in the downtown area, virtually everything you do in public is video recorded. I have had several murder cases, in the past two or three years, where they had from different cameras, public and private business locations and sometimes on residents recording step-by-step what happened. The CDTA, newer buses, have multiple cameras and on the interior of the bus there is audio recording. Therefore, anything that you or your client may do in public, in Albany, is recorded and generally is able to be authenticated and will come into evidence. This is something that is very new and it has been very helpful to the prosecution in the resolution in the cases, that I have had very violent cases.

The cold case files that we were talking about earlier, I actually have a cold case cap. I had one of the first DNA cases that resulted from a CODIS hit, DNA databank hit, on a misdemeanor. The defendant was convicted of misdemeanors, when they first started taking DNA on misdemeanor. The hit came back on a murder and a rape here in Albany. It resulted in pleas of guilty on two very violent offenses. What I am here to talk about, is a judge as a gate keeper, the judge keeping out junk science and junk technology and make sure that only reliable expert testimony is allowed.

New York State is what we call a *Frye* state. Generally, *Frye v. United States*, is the test that is used in determining whether or not scientific and expert testimony opinion evidence can come on. That is a 1923 case of *Frye v United States*, the thing from which the deduction is made, must be sufficiently established to have general acceptance in the particular field in which it belongs. That was and to some extend is still the law. New York calls itself a *Frye* state. I think that *Frye* and what I am about to mention have merged in some extend over the years.

In the mid-70s the federal rules were modified [with] Rule 702, dealing with the introduction of expert testimony. This changed the rules substantially and shifted the burden of scientific evidence to the judge and jury. There is a four-point test, whether the theory or technique has been tested in the experts' community, second, whether the theory or technique has been subject to peer review, three, any potential rate of error is, and four, whether the

theory or technique is generally excepted in the expert community case. This rule was utilized in several famous Supreme Court cases, the *Daubert v Merrell Dow Pharmacy*, which was relative to Bendectin, I think it was a drug to help women with morning sickness and it ended up being the subject of litigation for causing birth defects. In that case, the evidence was precluded because the court, this was a federal trial, and they use the *Frye* test and not Rule 702. Rule 702 has a lesser burden. The Supreme Court reverse and remanded, so it went back and was subject to re-trial using, I think the less strict rule of 702. After *Daubert*, which was in 1993, and 1997 was the *G.E. v Joiner*, which is a PCB case. The appellate review of that case determined that only an abuse of discretion in a trial court, would cause a remand. The federal appellate court, often find abuse of discretion. The federal rule and I think also the *Frye* decision and the general acceptance rule, were made applicable to non-scientific experts, and that would be the technical things that we've been talking about today. There are two interesting, fairly recent cases, and one of which I'm sure most of us here remember. These are Florida state cases; Florida is also a Fry state. The people called an expert in the case *Florida v Casey Anthony*, that was a case where the mother was accused of murdering her child. The people called an expert on an issue of the chemical makeup and odor chemical makeup of certain articles that were found in the trunk of the car, including carpeting and the DNA in odor analysis of decomposing human remains. The testimony was pretty sketchy in that case, and, in fact, the test that was used the defense in that case was able to have their own experts and use the same test and come up with a totally different result. The judge allowed it in.

One of the things we as gatekeepers are tasked with doing is to that junk evidence doesn't get in front of the jury. In that case, it did get in front of the jury and resulted in a conviction. Notwithstanding the opponents or defendants' opinion which was diametrically opposed. Some of the tests that were used are now being looked at, and there are skeptics that they would have applied as testified as to by the people's expert in that case. My opinion based on looking at the Casey Anthony cases is that that may very well been because of the facts of that particular case.

In other Florida case in 2003, the *Sybers v State*, which is a Florida case, the issue in that case was the presence of a toxic chemical in their corpse that was not found until nine years after the murder. The court allowed in proof that the tests that they

used were appropriate in the field, but they did not get sufficient evidence of whether or not it would apply to the facts of this case. In other words, whether a nine-year old corpse, was there any test results for the percentage of the error that could be demonstrated any reliability of the tasks in that particular case. The court did not allow that into evidence. The people failed to provide independent and impartial proof of the application of the technique to the facts of the case. So, I think that there's been somewhat of a merger. You might have an opinion on this, but I think it's been some kind of merger over the years and I think Fry has been diminished to some extent. I think it was a higher standard and was intended to be a higher standard. Based on what happened on Election Day, I think it will probably continue to be diminished over the next few years. Thank you.

Professor Michael Hutter:

Thank you, Judge Herrick. As you have seen evidence concerns delve on, revolve around reliability. As you know from basic evidence reliability concerns are addressed by the hearsay rule and authentications. The problem though with a lot of kinds of electronic evidence is that there is no person to cross-examine, it is all machine generated, there is a print out. Authentication, you have the emails, no person to really assess the reliability at all. The real question that comes up nowadays is how do you decide reliability of electronic evidence. I just use two examples, then I will open it up to the panelists to address separately. For example, say it is a child pedophile action, and the defendant now says, I don't do that, I don't get involved with children that's not me. The state police in their typical thorough investigation got a search warrant, grab his personal computer, and they go the history and the history now turns out that comes up on the screen and it shows that he has constantly been hitting on numerous child porn websites. Can that website information now be gotten in, or what about ATM receipt or E-ZPass? If the state police try to show that there's opportunity, the defendant was in the area. They will certain go the E-ZPass and they'll find out what has been going on with this person, they will check out the account. They will then see that this person now had gone through tollbooth 23 or 24 at a certain time, which puts him in the area. They want now to get in that print out, how do they go about doing that? How do we assure reliability? Certainly, the prosecution, the state police have the initial burden on that respect to establish reliability. How then

does the defendant approached it? Mike, do you want to address that initially?

Michael Deyo:

Sure, I mean with respect to whether or not electronic evidence is reliable, first, then how to ensure its reliability. I guess the simple answer is that it either can be reliable or it can't be. I know that it's a typical lawyer answer, I know it is. It is very dependent because of the precise nature of electronic evidence it's easily manipulated, either intentionally or inadvertently. The first key is focusing on how that information was acquired: was it done in a sound, hopefully forensically sound manner, to ensure that been preserved appropriately, which goes directly to the heart of reliability. Beyond that what is important for any piece of electronic evidence is to provide proper context to it.

Proper context can be established in a variety of ways, but two of the best ways are, one, the metadata that's associated with the electronic piece of evidence. So, it's one thing to have, for example, the documents that is . . . from the computer and is presented as an authentic reliable document. It might be important to know though when that document was created, [and] the user that was logged onto the computer at the time it was created. You can then tie where that person was physically within the world at that point in time, were they at that computer or were they somewhere else. Another important piece of contextual information is live testimony. Electronic evidence standing alone is helpful, but it should not necessarily be dispositive of any factual contention. There is live testimony that should supplement to describe what that piece of electronic data really means. A lot of people are wearing Fitbit bracelets, for example. Now I think after Christmas I will be joining the ranks as well and may have one. I don't know how they would work. I know you put it on your wrist and it somehow reports steps that you take and it is GPS enabled somehow. I know that the data that comes off that bracelet is transmitted somehow it clouds somewhere and connects to your phone and it does this in some way. However, I can't describe how the steps that are actually generated or where they're stored or how they're retrieved if they become a piece of evidence in either a civil or criminal case. I'm also not sure how the GPS functionality works.

There are a lot of things that I'm not sure of. To take, for example, a piece of evidence that says how many steps I took in a

particular day or where that bracelet was, depending upon location and heartrate, really means very little without understanding the calculations in determining the steps, heartbeat and other functions. This all needs to be established by an expert. Mr. Kindlon said that you cannot put on any case without the assistance of expert testimony and I think that is especially true today because it is so specialized. In sum, to make sure that electronic evidence is reliable it needs to be given in the proper context. The electronic pieces that relate to the piece of evidence and also the testimony of someone confident of what the evidence was and how it was generated and, more importantly, what it really means.

Professor Michael Hutter:

Terry, I know that you are chomping at the bit, but I will get to you in a minute. On the civil side, the other Mike, initially talked about metadata. Mike Deyo mentioned that metadata is very significant. The question that comes up is, how do we access this metadata? Do you need an expert to do that, or can we find out ourselves in using the laptop?

Michael Fox:

Yes, so again it is going to depend on a case-by-case basis. I teach at Mount Saint Mary College downstate, and I tell my class all the time you have the black letter law, but the cases may be gray, because it is a case-by-case analysis. When I was first speaking, I tried to cover things very quickly. This is an area that Mike Deyo can attest, I can talk for hours and days on. You have one hundred and twenty-seven slides just on this. When I was up here talking before, I barely dinged the surface, much less scratched it.

Let's talk about discovery as it concerns electronic information, for example Facebook or Twitter. Just because someone has a Twitter account or Facebook account doesn't mean it's automatically going to be discoverable. However, if this is a public Facebook page or a MySpace page, which was so prevalent years ago before people really understood privacy settings, that is different. You have one of the majority cases, *Romano v Steelcase, Inc.*, where an individual fell off of an office chair and injured herself. She sued the makers. In the allegations in the complaint, of course, were the allegations of loss of enjoyment of life, and physical injury. There were postings on the public Facebook pages

or MySpace pages, showing enjoyment of life, vacations, travel, skiing, whatever it was. Well that was the opening of the door. But, in New York, under the matters of *Tapp v. New York State Urban Development Corporation*, and *Patterson v. Turner Construction Company*, and a slew of other cases that have stemmed from those, you need a factual predicate to get into the private side. That means that anything behind the privacy shield of Facebook or Twitter or any of those kinds of social media accounts.

The factual predicate can be established by any number of things. It can be simply a matter of you have a private investigator who has followed the individual in the personal injury action, and between that and some deposition testimony you have, you set forth the factual predicate. You can issue your discovery demands. When the discovery responses are produced, you may have a chain of custody to possibly be concerned about, you have the authentication elements of what is produced from the Facebook or Twitter account. But, if you don't have the factual predicate, it is a little more difficult. Sometimes there will be a subpoena served on the service provider.

Now in the case, for example, of *Romano* or others, the service provider argued Stored Communications Act, which we really have not talked much about today. [The] Stored Communications Act is a federal act that can protect the service provider. If you don't have the permission from and the release of the user, then it can be very difficult to get behind the Stored Communications Act to get to the service provider. What courts are often finding, if you have a party and there's the factual predicate, and the party can provide the release and waiver to the service provider, the court will order that as part of discovery. So, that solves the problem – the party signs the authorization and release, and the service provider will provide the information. That is all well and good if you have a situation where there is no dispute over the fact that the Facebook or Twitter account is that party's account.

But let's talk about what Professor Hutter discussed, which is the nightmare scenario. You have an individual who is prosecuted for child pornography that is on, allegedly, their social media account. This happened in the case of *Lemon Juice v. Twitter*. In the criminal case, those were the allegations. Fortunately, because the individual was innocent, they were acquitted at trial. It turned out there was an individual who set up a fake account (and in the *Moroccanoil, Inc. v. Marc Anthony Cosmetics, Inc.* case and others the courts acknowledge that fake accounts can be set up, or mock

accounts can be set up). This is the same concern we had about websites when I talked about that earlier. Here you have an individual who established a Twitter handle that was very close, basically identical, to the criminal defendant's account. Fortunately, it was proven that it was not their account, rather it was a mock account. The plaintiff, the criminal defendant who became the civil plaintiff, wanted to sue. They wanted to sue the individual that created the account for all of the damage to their reputation, for their emotional distress, and pain and suffering. The problem was that they could not find them, because Lemon Juice was not their name. So, they bring an application to get the information from Twitter, wanting to know who established that handle. Twitter objected and said that they cannot turn that information over, that user information. The court resolved it by simply saying that what happened went beyond all bounds of decency in a civilized society, and the court found an exception and ordered the information to be turned over by Twitter. The Twitter handle could be identified, the user could be identified and could be sued civilly by the individual who had been wrongfully prosecuted because that other person who had created this account basically operated as them.

So, that's a way that by utilizing subpoenas and discovery demands, there are ways on the civil side that access can be achieved for Facebook or Twitter, or any social media accounts. Emails are generally by discovery demands or subpoenas. There was an interesting case just recently this past summer [*Microsoft v. United States*], Microsoft successfully defended against a government subpoena in a criminal investigation wherein the government wanted to subpoena Microsoft for information on servers located only in Dublin, Ireland. Microsoft's attorneys argued if another country and their prosecutors tried to do the same thing here—this was actually the argument to the court—"we would go crazy." The court basically agreed and said that if it is purely and solely held outside the United States, on a server that is not in the United States, there is a limit to subpoena power. There are certain limits in the criminal context, civilly there are a number of avenues that attorneys and parties can follow to try to obtain the information from these accounts, and then utilize the authentication process.

Professor Michael Hutter:

You raise some interesting issues about privacy, but I want to go back to my initial question, that Mike addressed. Judge, what do you do when the government now gives you the evidence and says that this is what we are going to do, and this is a print out of the social media of your client, and the client argues someone hacked them. How do you handle that?

Terence Kindlon:

That has not happened yet, but I am waiting for it to happen. Let's assume that there are some evil people in government, and they want to destroy someone. It would be very simple, I am certain, with people with the right access to technology, to create a phantom crime and to attribute it say to me. They could set up an account that looks like mine, and the account could look at child pornography and distribute it, and then all of the sudden, the Secret Service would be at my house and take my computer. I would then be arrested and on the six o'clock news. I would be saying I didn't do anything but no one would believe me. I think it's going to happen sooner or later. I hope it doesn't happen to me but it's going to happen to somebody and then we are going to have to call on all of our technical resources to demonstrate conclusively to some judges what exactly has occurred here. It is a dangerous situation.

Professor Michael Hutter:

I will follow it up because obviously, you need the expert and the money. State police have access to a world class organization and they are investigators, and they are all top notch, and they have the ability to explore all that. Judge Herrick, from a public defenders' perspective, do you have the budget to allow you to hire these experts to challenge that electronic evidence, isn't that kind of unfair?

Judge Stephen Herrick:

I was telling the Dean, when I arrived three weeks ago, right at the end of the budget process, I looked at the executive's budget proposal to the county legislature and it had requested less than $10,000 for expert opinions and assistance. We had a bill sitting there from Terry's predecessor of $4,500 for one expert for ten hours. I gently raised it to 25,000 and will see what happens in a

week or two. There are federal cases, as I read, that say that if the prosecution has an expert witness, you have a responsibility as a defense counsel to have an expert review the opinion to make sure that it is not a junk evidence opinion. This may include getting your own expert to testify, if the court will allow it in. You need to rebut the people's expert. This is a responsibility that costs money.

Professor Michael Hutter:

We talked about privacy, a couple of questions then we will open it up to the audience. People do not have any rights of privacy in their email, their private pages. The government can come in and get a subpoena. Isn't that kind of evasive now, or is that accepted that you lose your right of privacy?

Terence Kindlon:

My take is that when you send an email to somebody, it is like when you send a postcard to somebody. It is there for anybody to read, and it is not protected in any way. You have given up your right to privacy by the action you have taken. It is a problem that I encountered. What drives me crazy are these calls from the jail. People are in jail, and there is a big sign there that your call is being recorded. They read that then confess to their girlfriend on the phone about their crime. The DA then comes in with a smile on his face and then you are cooked. You know I am thinking, I'll bet, that if he was some rich guy and lived in an exclusive neighborhood, they would not routinely be listening to his telephone calls with his lawyer or his girlfriend. I did have this happened to me. I finally got a print out of the case that involved the 14-year-old girl, and all my clients call from jail. Now, fortunately all of his calls from jail were to his relatives to set up bail. But, as I was going thought this thing, at about page five, I came upon his conversations with me. His conversations with me were recorded with comments by the police officers who listen to them. Now I was a little baby lawyer, and electronic surveillance consisted of wiretaps together by the FBI, and two guys sitting in a van with their phones on. I mean in those days, if a conversation was confidential in nature, the listener was required to minimize. They had stop listening at that point and turn the machine off. Obviously when you got this mass produced digital record of jail

calls that no one knows that. It was a little disconcerting to read, me in the middle of the discovery of my client's jail house calls. I certainly didn't give up my right to privacy.

Michael Fox:

It is interesting when you have a sign up, that's one thing, or if you are in public. As was mentioned, before walking on the street you can pretty much assure yourself that someone is filming you. Walking in New York City over the years, I am sure that I am in many people's photo albums, that I am in the background when they were in Times Square taking a picture, and as I was walking in the background. Another thing to keep in mind, in terms of privacy expectations, the Fourth Amendment is still alive and well. In 2014, in a 9-0 decision in *Riley v California*, it held that a warrant applies to a cell phone search. So, the police officers cannot search the phone prior to an arrest. The one phone was a flip phone and the other was smart phone, and the court held that smart phones are really computers these days, not phones. The court applied this across the board, even though flip phones and smart phones are different. So, warrants are still required for certain police searches regarding cell phones or computers, so there is that protection. It can be a very big concern about waiving a privacy interest.

It is the same thing on the civil side. Say for example, your client and you are communicating email to email. If that client is using someone else's email account, whether it's their spouse, friend, cousin or employer. and this is their private case, not their employer's case, where they are representing the employer, the communications across that server to you on email may lose attorney client privilege. So often best practice is to advise the client to establish an account with Hotmail or Gmail or Yahoo, doesn't matter, make up your own account and use that account so we can communicate without losing the privilege. Especially with employers, often there is this statement right in the employee handbook which will say use of our computer system or our email system is a waiver of your right to privacy. There's no expectation of privacy. It is a slippery slope and there is a sliding line. There are some protections but there is some loss of protections.

Professor Michael Hutter:

One last question as follow up, Mike talked about search warrants and privacy. How does the state police go about making sure that there is probable cause and that the search warrant that they are seeking will past scrutiny? Can you briefly just address that process?

Michael Deyo:

Sure. With scrutiny, I assume down the road at a suppression hearing, the process that is followed in order to obtain a search warrant is to put in an affidavit by a police officer with personal knowledge of facts, sufficient to establish probable cause in the mind of the judge who is going to issue the warrant. The bigger question comes in when it is time to execute the warrant to make sure that how the warrant is carried out is defensible and legitimate, and not subject to challenge. A lot of this comes back to really defining what is going to be searched, and where the data is that is going to be searched. One of the challenges that we have experienced over the years, not just the state police but rather law enforcement and government in general, is what do we do in situations where you've got, for example, a criminal investigation in New York State which touches upon communications or other evidence generated from or stored in a computer somewhere else. The judge signing the warrant only has jurisdiction, typically within the territory in which they are authorized to act. One of the challenges has been how do we execute a warrant for example for Facebook or Twitter. If a warrant is issued giving police the right to access content generated on one of these platforms and the warrant is then somehow delivered to one of these service providers, how can we ensure that it's going to be defensible down the road and there is not going to be a question about execute, place of execution, jurisdictional authority to execute beyond the state. What we have been left with is the practical solution. Execution is putting the warrant on fact, or an email or some delivery mechanism for the out of state provider. The execution occurs in New York state, the actual work of pulling the records in response to the subpoena happens somewhere else because it has to be. This is the challenge that we deal with. As information goes out into the cloud and is no longer kept on a person or close to a person.

Terence Kindlon:

Can I ask you a question: has anyone challenged that yet?

Michael Deyo:

Formally, I am not aware of anything.

Judge Stephen Herrick:

I have signed many search warrants for out-of-state, electronic information, and generally they find a New York state office and then they send the information internally and it is taken by the police agency in New York.

Michael Deyo:

That is, assuming that there is one.

Professor Michael Hutter:

That is a big assumption.

Judge Stephen Herrick:

The question that you ask Mike is "how do the state police prepare" and are they trained. I would have a pecking order depending on the police agency that would come in for an application for a search warrant. I would pretty much know their format. When I am reviewing it, the state police are very good in what they present. However, you get some local agencies and state agencies that are not. For example, the New York State Tax and Finance, I do not know who taught them how to prepare applications but they're not the best. The police agencies, I wouldn't say the higher you go because I think the state police does better applications than some federal agencies, but it is the training. It is part of when you become an investigator or a senior investigator you are trained on how to do it.

Questions from the audience.

Rebecca Harp:

I would like to thank you all for coming, and thank all our panelists and moderators today who participated in this year's Journal of Science and Technology Symposium.