Investigation & Litigation
How Agencies' Use of Surveillance Technologies, Including Wire-tapping, Impact Current Criminal Investigation and How the Use of DNA Has Propelled the Criminal Justice System Into the 21st Century

Moderator: Professor Melissa Breger[*]

Panelists:
Jennifer M. Assini, Michael Deyo, Eric Galarneau, Stephen P. Hogan, Kimberley F. Wallace

Professor Melissa Breger:

Thank you. Good afternoon everybody. We are in for a treat with a spectacular panelist line up and our keynote for tonight. Congratulations to Julia, our Symposium Editor, who really pulled all of this together. It's going to be a wonderful program, I know it.

So, as Julia mentioned, our first panel will address the use of surveillance and technology, including wiretapping and the use of DNA, and how that juxtaposes with privacy rights of defendants. And we have five very impressive speakers. I'll introduce each one before they speak. That way you can hear one at a time.

We're going to start with Jennifer Assini. Ms. Assini is an assistant district attorney in the Schenectady County DA's office where she has been employed since 1991. She currently is the Bureau Chief for intelligence and investigations. And she

---

[*] Melissa Breger has been teaching at the law school level for 19 years, first at The University of Michigan Law School and then at Albany Law School since 2002. Professor Breger teaches a variety of courses at Albany Law School, including Evidence, Family Law, Criminal Procedure: Investigation (4th, 5th, 6th A), Gender & the Law, Children, Juveniles & the Law (hybrid online), Domestic Violence Seminar, and Children & the Law. She was the Director of the Family Violence Litigation Clinic from 2002 to 2010. Professor Breger is the co-author of NEW YORK LAW OF DOMESTIC VIOLENCE, a two-volume treatise published by Reuters-Thomson-West, as well as the author of numerous law review articles regarding issues of family law, gender, and justice. Prof. Breger received her B.S. from the University of Illinois and her J.D. from the University of Michigan Law School.

supervises the county's public surveillance camera system and the car program. She will be speaking to us about Schenectady's surveillance camera system as well as other systems in place. Miss Assini.

Jennifer Assini[†]:

Thank you. Thank you very much for having me today. Julia and I go way back, right? No, I appreciate the time. We have approximately eight minutes. When I took the one-page document that I sent to them and it exploded to six pages as I was trying to do bullet points and things, so I'll see where I can get on it. My focus, my personal focus today is going to be on the public surveillance camera system that the county of Schenectady has. It started way back in 2005 with about five cameras and one of which was wedged in a window. And if a big truck hit a pot hole, it fell down and we ran up and we put it back into place. And that was the start of a system that's exploded to about ... over 200 cameras.

A lot of the data that we have with our camera system, including locations and the views that they will capture, a lot of it, as in all of it, we maintain secrecy of under the foil exception, law enforcement. For multiple reasons. And one of which is people's privacy. And the reasons we started the camera system to deter and prevent criminal activity. To capture evidence. To store the evidence for use in criminal prosecutions. And to use it in conjunction with ongoing live police activity. And for police protection and safety. If they're going to arrive on the scene, you want to have eyes on, if you're able to.

Most of what we do is browsing, so it's after the fact. You don't know where crime will occur and our bank of cameras does not utilize full time live monitors. There's not a chance to cover all of that. But the camera system itself, so you know of capabilities can be a fixed camera. Can be a 360 degree came. Can be a 180

[†] Jennifer Assini is an Assistant District Attorney in the Schenectady County District Attorney's Office since 1991. She currently is the Bureau Chief for Intelligence and Investigations, and supervises the CARP Program and the County's Public Surveillance Camera System. Additionally, since 2011, as a member of the FBI-led Safe Streets Gang Task Force, she is cross-designated as a Special Assistant U.S. Attorney in the Northern District of NY, working with the task force to combat violent actors and street groups or gangs. She graduated from Vermont Law School in 1987 and from Bucknell University in 1984 (Biology, Political Science).

degree camera. And PTZ cameras which are pan, tilt, and zoom. So you have various capabilities of cameras. You have emerging technology so that our cameras can age out very quickly. And just practically funding is a big issue. Public and private funding can keep us limited. But our system is a wireless system of point to point system. And it's based on line of sight. We do not utilize fiber. We would love to have fiber, we call it our "F" word. But we don't have the funding for fiber yet. We're working on that.

We definitely worry about privacy issues. The cameras view people in the public domain. Because they have the capability to zoom in and out, they have the capability to zoom somewhere that's not public. And we write a policy, we require certification of the utilizers, and we'll do spot checks, and we try and audit. Just to make sure that people aren't looking where they shouldn't be looking.

Practically, servers only have a certain capability, a certain amount of data they can hold. So our retention policy is 60 days. So as far as litigation, that's a practical concern. The request to store the data, to retain the data, needs to come in in a timely fashion. That means you educate your officers, you educate attorneys, prosecutors, defense attorneys, if they are putting in a request. But again, we utilize it exclusively for criminal prosecution, criminal investigations, and it is not something that is available to the private industry. Testimony from a defense, or from our chief technical resource officer would go to the accuracy, how it's stored. Chain of custody would only go to the weight of the evidence. But we have a policy of procedure and an evidence log and there is a chain retained.

The beauty of the camera is that it can capture what is happening out on the street. And that can work both ways. And it works to get to the bottom line and what is just and what is fair and what is real. Simply, don't be afraid of the facts. We are catching what is going out on the street. And we can confirm events that happen. And we can disprove statements that are made. And we can utilize it when we're interrogating and questioning witnesses. And we can pull up a clip and show them and test their story. Test the facts that they have. And it's been utilized to great success. To confirm facts, and to confirm that a story is false. So, we're looking for truth. And it's a powerful tool when someone sees themselves in video footage to say, they got me.

It's a cost saver, and a time saver, and for this system because people, once they often see that video, will decide to take the plea that we will offer. It has been used to disprove claims. We've had a couple of claims of sexual activity on the street. Someone takes someone into an alley, we review the video, confirm time, and show that there wasn't any activity on the street there. And you can push to get to the facts that way.

Let's see. Talked about funding and foil ... the technology that's a lot of what we're talking about here is technology. The technologies that are developing right now, first you have the basic system when you're taking a lot of video data. But you may have, for example, a burglary that happens. You go away for a weekend, you leave on Friday night, you arrive home late Sunday, your house has been broken into. That's three day's worth of video. If it's exported, it's stored in three day's time. Now that takes a detective or a person to ...

It's a lot of down time for a person to sit and wait until you see movement leaving the house. Or say they go in the back door and the camera view is from the front. Technologies are being developed to scan times, you put in parameters, algorithms in software are being developed. And you might say that you're looking for movement. Period. You might say, out on a street event, someone says the guy had a blue hoodie on, red Nikes, and was running in a northerly direction. The technology that is being worked on now is allowing you to check those boxes and scan.

An example of a company that does that is called Brief Cam, and they have 56,000 hours of video from the Las Vegas shooting. It's estimated to take six months for normal review of that to find the facts. Brief Cam can, per their promise the other day, because we're looking at their software, is put it into the system and get that review done in eight days. That's a significant, significant savings for everyone. And you get to your fact finding much faster.

With those concerns you have, implicit biases that you need to be worried about. You have human error and assumptions that can get made. You have large time periods that we're talking about that can work for fixed cameras. But we find the PTZs, the ones that you can have move, have much more function for us often, especially in a live review situation ... not review, a live scene situation, where we're responding to a scene. And the

ability to zoom in and capture, for example a plate ... a license plate. Then we jump to the other technologies that people are going to be talking about and you combine your crime analyst with your video data, your LPR data, the license plate reader information, your databases of addresses, and again you condense your time to fact finding.

We do not utilize body cams yet for our cases on a routine bases. The Schenectady police department is getting body cams now. But one of the things that is ... with technology comes the CSI effect. And there are eight million and one crime shows, police shows, law shows, on television, and it's a real effect that we have to be aware of. And even [inaudible 00:13:29] juries, in jury ... in [inaudible 00:13:32] in the beginning all the way through to the jury instructions at the end. Because it's a real known effect, it's documented. And people expect that there is a camera that will capture video.

My ADAs expect ... they're just so deflated when they don't have video data. And they say, "Oh my god, we have to do it the old way." So, it's not only just jurors, it's throughout all of society that we expect that it will be wrapped up in 45 minute times. But TV is entertainment, not education.

And so, I'll wrap up because I know we'll move along. But just around the world, it's estimated there are 245 million surveillance cameras. New York City monitors 9,000 cameras. Chicago is installing up to 30,000 cameras. They hope that that will put the reigns on some of their violence that they're enduring. And London is the most surveyed city in the world. Although China is ... the numbers aren't fully reported out of China. But with the technology and the emerging technology there, the cameras, video surveillance systems are pretty much blanketing the country.

So I will wrap that up there, I'm sure we'll have questions later on. Thank you very much.

Professor Breger:

Thank you, Ms. Assini. Interesting material. We are now going to turn to Michael Deyo who is Deputy Counsel to the New York State Police. He has worked on a wide variety of computer crime, information assurance, privacy and data security investigations, over a span of more than 15 years. He will be speaking to us about how the laws in Supreme Court jurisprudence has been

evolving surrounding the use of cell phones, GPS, and cell tower data. I'll turn it over to you.

Michael Deyo‡:

Thank you. Good afternoon.

So, how many in the room have a cell phone with a data plan? So, when I was asked to talk on the topic of surveillance, technology surveillance, it immediately occurred to me that I should probably say something of respect to cell phone tracking. And it's interesting because cell phone surveillance, and we're talking about location tracking, the tracking of movements, either historically or real time. It is, at the same time, the most effective, widespread and pervasive form of surveillance that exists to today.

What with respect to cell site records, maintained by carriers, which is the primary source of location tracking information, it's actually not surveillance at all. It's not government surveillance of citizens. It's actually a data set that's created out of the mere operation of a cell phone contract between a subscriber and a provider. So just a little context on how it works.

We all know that in order to use our cell phones, we need to connect to a tower. And in fact, we usually connect to multiple towers. So, as we move around, service isn't disrupted. And our phones are constantly switching to connect to the strongest signal on each tower. Cell phone towers have at least three faces on them. Which face in different directions. So, if we're connected to say, three cell phone towers, and more specifically a particular face on one of those cell phone towers, the provider knows exactly which face we're connected to. They make a record of that and they retain that record.

If we were to look at any point in time where a cell phone was connected, we could triangulate with a reasonable degree of precision, where that phone is located. Just by knowing that

‡ Michael Deyo is Deputy Counsel for the New York State Police. In this role Mr. Deyo provides a broad range of general legal counsel services, with particular emphasis on legislative drafting and guidance; electronic surveillance laws; novel legal questions pertaining to electronic evidence; federal and state laws related to criminal and counterterrorism intelligence functions; and the investigation of crimes facilitated by the use of electronic devices. Mr. Deyo received a B.S. in Criminal Justice—Economic Crime Investigation from Utica College of Syracuse University in 2000, and his J.D. from Albany Law School in 2007.

there is one tower here and the phone is connected to the north-facing face of that tower. There's another tower here and the phone is connected to the east-facing face of that tower, and there's another tower here and the phone is connected to the south-facing face of that tower. And there's a signal strength indicator associated with each connection. So, by pinpointing the direction and the signal strength, within 3 to 400 meters with today's technology, we can identify where a cell phone was a particular point in time.

And these connection records are created when a phone call is made, when a text message is sent or received, when an email is sent or received, using social media, when there is data transmissions between the phone and the tower. So just as a rule of thumb, let's say that there's 100 locational data points created everyday for each cell phone user. And that's based on old numbers, that doesn't reflect today's usage, but that's kind of been the benchmark we've operated on. I'm going to suggest that we're active 16 hours a day, and let's just say for argument's sake, there's 10 data points created every hour that are active during the day. So, there's 160 locational data points created each day.

Multiply it by 365 days a year, and the carriers retain these records for five years. So, we extract that out, for any one of us, there's about 300,000 locational data points that exist today. That your cell phone provider has in a database. Now that can be highly useful information in criminal investigations.

It's not surveillance though. That is not government surveillance. That is how cell phones operate. We voluntarily subscribe. We purchase cell phone, subscribe to cell phone service, and part of the contract, part of the service agreement is that we expect our carriers to connect us to their network. To make sure that we have good connections. We have connection wherever we roam so there is good coverage, there is good strength of service. And for the carriers to do that, they need to track where those connections are occurring. They maintain those records and they keep them for typically a five-year period.

Needless to say, that's a vast amount of data that exists. That can be accessed by law enforcement in the context of the criminal investigation. Now historically, this information enjoyed no constitutional protection whatsoever. And the reason is because, believe it or not, it's not private. At all. Under the fourth

amendment. And the reason it's not private is because it's a business record created and maintained by a third party, under the third-party doctrine, or the voluntary disclosure rule. Which is premised upon the assumption of risk doctrine.

If I voluntarily convey my locational signal to AT&T, so in exchange I can get their service and connect to my email, I know that I've relinquished that locational information. And they can in turn release it to anybody they choose. The government, law enforcement, some marketing aggregating company who uses that for whatever purpose they want to use it for. But it's not a search.

So, the third-party doctrine can probably be described as an exception to the fourth amendment protections. And you may not like that. You hear there are 300,000 data points about where you've been over the past five years right now sitting in some database in the cloud somewhere. And instinctively you might say, well that's awfully private. That should have privacy protection. And as a policy matter, maybe you're right. As a constitutional law matter, there is no privacy protection under the third-party doctrine. So maybe we should pass a law. Maybe congress should pass a statute giving privacy protection to these records. And that's what was done with the electronic communications privacy act, and the stored communications act, to give privacy to electronic communications.

So, all of this remained true until June. The *Carpenter* case came along. And you've probably all heard about the *Carpenter* case by now. It's been called a game changer, revolutionary, and maybe it is. But it's probably not as much as a game changer as you might think. So, what I thought I'd do is just kind of solidify everybody's understanding of what *Carpenter* does and what *Carpenter* doesn't do from a precedential basis.

On the facts of the case in *Carpenter*, the Supreme Court created an exception to the exception. They carved out from the third-party doctrine, one specific type of record. Cell phone locational information. And left the rest of the voluntary disclosure doctrine in place. They essentially created a new legal doctrine out of thin air. And the doctrine goes something like this: Some activity, which is not a search, becomes a search if it's pervasive enough. And that's never been a principle of constitutional law before. That's like saying, if police go into a residence and conduct a search for six minutes, that's really not a

search. But if they do it for seven minutes or longer, that is a search. Or by a more apt analogy, police tail a car for six hours on public streets. That's not a search under the fourth amendment. But if they tail that same car for seven hours or more, that becomes a search. Because aggregated together, that information invades a privacy interest. Somebody might not think they're going to be followed for seven hours or more, but they might reasonably expect that they'd be followed for five or six hours.

The legal basis for the court's decision was that cell phones are essentially unlike any technology that has come before. And that's true. It's absolutely true. There are unique privacy concerns raised by the locational records that follow cell phones. And let's face it, smart phones are an anatomical extension of our bodies. They go everywhere with us. If you want to track somebody, you don't necessarily track their vehicle, you track their phone. The phone is essentially the person.

The Supreme Court also relied on making an exception to the exception by saying that cell phone usage in today's society is not voluntary. We can't meaningfully interact with society if we don't have a smart phone. I'm not sure that's true. My personal view, it's voluntary. Nobody forces me to buy a smart phone. Nobody forces me to subscribe to AT&T with a data plan. I choose to do that. It would be very difficult to not do it. It would be inconvenient, painful, I'd feel like I was left out in many respects. But it's voluntary. It's entirely voluntary. I could stop today if I wanted and cut myself off. Or so I say.

So, the legal basis, in my view, is a little bit questionable. It seems to me that the third-party doctrine has been mangled. When the right solution was probably legislative in nature. If we thought that locational records deserved more privacy, legislative action should have been taken to do that. Now we have a third-party doctrine that's starting to get chopped up based upon the type of information that's at play.

But the real point that I want to get to: *Carpenter's* a narrow hold, probably much narrower than you expect based upon what you've read in the media. The holding is if police obtain more than six day's worth of historical cell sight locational information, that is a search that requires a warrant. And that's it. Six days ... more than six day's worth of historical locational information. There's different purposes for how police use cell sight locational information. And there's basically, I boil it down to three

categories. The first is to build a case. To build a criminal case against a known suspect. The second is to develop a lead when there is none. And the third is to apprehend somebody who needs to be apprehended.

So, with respect to the first category, building a case on a criminal suspect. You've got a suspect identified. You've identified the phone associated with that suspect. If police want to compile evidence of past movements over a period of a week or more, that's a search that requires a warrant. That's Carpenter. That's it. If police want to compile records for six days or less, that's not a Carpenter search. So, it could be five days' worth of locational records, it could be one day this month, one day the next month, one day another month. If it doesn't add up to seven days or more, it's not a Carpenter search.

So how might this be done? Let's say that there is a string of robberies. Maybe police have a suspect identified. So they look at the robbery date. There's six robberies. They look at where was that phone on these six dates. If we can link that phone to these locations to the time of these robberies, even though we're going right after a particular suspect, that's not a Carpenter search.

Lead development, there's a concept known as a tower dump where, instead of looking at a particular device, police look at a tower. So, let's say there's a murder that occurs on the corner of New Scotland and Holland Avenue. Police have no leads. Police know when the murder occurred, however. How about we go to the towers closest to that intersection and determine what devices were connected to that tower at the time of the crime. And link back those devices to the subscribers and determine if there's any connections between the victim and one of those people who were present at the time. Develop leads. That's not a Carpenter search. The supreme court carved out tower dump from the Carpenter rule.

And it's a good thing they did. Because we could never obtain a warrant based upon that. There is no probable cause if you're looking at lead development as opposed to trying to build a criminal case based upon. Carpenter was dealing with many days' worth of locational information. Over one hundred days, in fact.

The final point, apprehension, real time data. It's possible for police to contact a cell phone provider and ask where a particular phone is right now. Connect to that phone, ping that phone, tell

me the tower it's connected to, the face on the tower that it's connected to, and signal strength so we can approximate where that phone is. And by extension where that person is. And this can be done for very good purposes, like if somebody goes missing, if somebody is kidnapped, if there's an Amber Alert. It can also be done if somebody needs to be apprehended. If we have a violent felon on the run who needs to be located. Real time locational information can be obtained. That's not a Carpenter search. That's carved out of Carpenter.

So all of these different purposes that cell site location information is used for, just be mindful that what the Supreme Court did in Carpenter is ... decided a specific case that was before it. And nothing more. The Court found it unnecessary to set a demarcation point exactly when something which is not a search becomes a search because it becomes so pervasive. Suffice it to say that seven days or more worth of historical records is sufficient to be considered a search. And just be mindful that there's a lot of push to ... want to simplify it?

Let's just say that access to any cell site locational information requires a warrant. Let's cut out this six-day, seven day rule about how long it takes to become a search and just say anything. Even instantaneous or one day's worth, and what I suggest is that's not workable. That would compromise hundreds of thousands of very important investigations around the world because although our policy, particularly from our office, the advice is always get a warrant if you're able to. If you've got probable cause, get a warrant. Just get a warrant, you want to be safe. Sometimes you can't get a warrant. Sometimes you're using this information to develop leads for very legitimate public safety purposes.

So, what I tell anybody who is willing to listen to me is be very mindful that we don't push the pendulum too far. And cast constitutional privacy protections over a category of records on a wholesale basis that really it should not be applied to when there's impeding public safety interests that are very, very important.

Professor Breger:
Thank you Mr. Deyo. And my criminal procedure students in the class in the audience are now thinking that was a great review session for the final. Thank you.

We now will hear from Eric Galarneau who serves as the Albany County DA Bureau Chief for the financial crimes unit. And also oversees the Public Integrity Bureau. He is also the 2018 recipient of the New York State District Attorney's office Associations Robert M. Morgenthau Award, a prestigious award. He will be showing us a Power Point and addressing the interplay between technological evidence and criminal investigations as well as the challenges that prosecutors face in obtaining information from companies like Apple and Facebook and so on.

So I'll turn it over to you. Let me see if I can grab your power point for you. Is that it? Okay. Oh there it is. Okay.

Eric Galarneau[§]:

There we go. Hi, how you all doing? Maybe I'll just talk from here. I'm Eric Galarneau and this is the guy that inspired me to be a prosecutor. And if you're a prosecutor, you do it because you want to be in the court room and you're a bit of a ham and you enjoy attention. So that's why I stood up for this. But this guy inspired me to be a prosecutor. When I was going to law school, I thought what prosecutors did was call witnesses to trial, get their side of the story and then make an argument to the jury based on that testimony. And what I realized when I got older and got more experienced, I've been in the DA's office almost 20 years now, is if that's the way you're building a lot of your cases, it's probably what I would call prosecutorial practice. You cannot just rely on witnesses anymore.

Sometimes you're forced to, sometimes that's all that you have. But to the extent you can get other types of evidence, that's really what you need. And obviously in a criminal trial or any trial you're left with two types of basic avenues to direct evidence and your circumstantial evidence. And I recall when I was in a local judge's chambers recently, there was a discussion among some younger attorneys and the judge about what kind of cases you prefer. Do you prefer a case based on direct evidence, the witness based case where the witness gives it to you, I saw that guy rob a bank. Or do you prefer more circumstantial evidence type case. I got cell phone records that put this guy at the bank. This surveillance footage was in there too. There's some text messages

[§] Eric Galarneau serves as the Albany County DA Bureau Chief for the financial crimes unit and also oversees the Public Integrity Bureau.

with conspirators that talk about what they're about to do. What kind of case would you prefer doing?

And a lot of the younger attorneys said they would prefer the direct evidence case. And I thought they were foolish, and I told them so. I said, you should always go for the circumstantial evidence case when you can. Juries like circumstantial cases. And one of the reasons your direct evidence cases are very often based on high witness testimony. I would.

Often based on eyewitness testimony. Eye witness testimony is subject to a lot of challenges in addition to your biases that a witness might have, the misperceptions they may carry with them. Their biases, and when we're talking about bias, we talk about not only a motive to lie, but implicit biases they might have. They may make mistakes.

Circumstantial evidence doesn't really have those issues. Circumstantial evidence has things like DNA. This is kind of what I thought I'd throw in there just to how do you ... this is Prometheus here: how can you tear out my liver? Well, before you're accusing me of something so serious, you better have proof. I see you doing it. Studies have shown that eye witness testimony to be shockingly unreliable.

Having said that though, there's too many instances where eyewitness testimony can lead to wrongful convictions. It's something that, although we can laugh a little bit about, it's also a very serious thing. And our job and what we try to do as prosecutors and investigators, we try to do the next step. We don't simply stop at getting an eye witness and that's the end of your case. We go beyond that.

So what am I talking about with circumstantial evidence? I'm talking about the technology available to us, technologies such as DNA and fingerprints, which I think Steve will speak to you in more depth about, electronic evidence, emails, text messages, eavesdropping warrants, cell phone communication, cell tower information, GPS information. All of this can actually put together a very compelling case even where your eye witness may be lacking.

As an example, I want to invoke a case I did a couple of years ago, People versus a Kareem Murray and Russel Palmer. In that case, we had a shooting that occurred on Grand Street here in Albany. A man was shot walking down Grand Street. There were no witnesses to the homicide. It was about 8:00, 8:30 in the

morning, absolutely no witnesses to the homicide. But there was evidence and there was lots of evidence. There was evidence from surveillance cameras, there was evidence from cameras at a liquor store, in fact. The liquor store called actually captured our victim walking down Grand Street shortly before he was shot. The liquor store also caught the image of a black Yukon driving away from the scene. We've got our first glimpse of the Yukon.

At the same time the New York state police had been up on an eavesdropping warrant on some particular people who were involved in some narcotics activity. That eavesdropping warrant revealed some calls where people were talking about what had happened. In and of itself, maybe nothing, but something that gave the state police a heads up we ought to be looking at this. The state police then communicate that to the Albany police department.

The Yukon is stopped at a hotel, the Desmond Hotel in Colonie. There are two guns recovered from that vehicle as well as some drugs. But for our purposes, the guns we're interested in. Two guns are recovered from that vehicle: a nine millimeter and a .45. Those guns are ultimately sent to the New York State Forensic Investigation Center where, believe it or not, we get touch DNA on one of the triggers that comes back to the passenger in that vehicle.

Left at the scene is a smattering or a spattering of shell casings found on, if you look at this picture here, probably on your right side of Grand Street, they're all kind of distributed there. But in a moving fashion like down the road, they're not just stationary. So, what do we have? Then we were able to actually, using the image we had of the Yukon SUV and the wire taps, we then employed the services of a detective with the Albany Police Department who religiously searched all the city cameras, all surveillance, CDTA buses, anything that he could find. He grabbed video from everything. We were able to trace that Yukon all the way back to the Desmond Hotel, leaving the Desmond Hotel at eight o'clock in the morning, coming to Albany at about nine and then leaving and getting back to the Desmond by 8:45.

Using cell phone records from the ... and we did a search warrant because we weren't sure at the time what the law would turn out to be. But we found out that the search warrant hit off a couple of towers, again going from the Desmond and Colonie all

the way to Albany, just enough to get us to corroborate what exactly happened.

So what this revealed to us, we had all this evidence and then we just put it together. Okay. What you had was you had ... oh, I forgot to mention one thing. Ballistically, we were able to establish that there were two different shell casings found at the scene. Well, two different types. There were about nine shell casings. Some came from the 45. they were able to ballistically establish that. Some came from the nine millimeter. So, we established that the murder weapons were in that vehicle. But we have two people in the vehicle. So, we thought, we didn't know. That's the problem. What we did have though, we had all the shell casings distributed on one side of the street.

So, there's two scenarios possible here. Because they were distributed in indicated that it was a drive by it. It wasn't like I stopped the car shoot, shoot, shoot and left. I was driving as I went. But they're all on the same side of the street. That was a little tricky for us. So why are they all on the same side of the street. You got Yosemite Sam in the vehicle shooting, while he's driving the car with his elbows? And then looking, going back at the video we saw, as the SUV is emerging into the picture where that liquor store is, we saw the back seat, driver's side, the window going up, which told us that the two shooters were on the same side of the vehicle. One was in the driver's seat, one was in the passenger seat. Putting that all together, we were able to get a conviction using all the technological evidence you're hearing about today: surveillance footage, cell phone records, DNA, which you'll hear about in a minute.

That's really what we're doing. When I say to ignore this type of evidence as a prosecutor is malpractice, I mean that. It becomes a much more compelling case than if someone just saw a glimpse of a car and said, "I saw someone get out and shoot him." This is much more compelling.

There are, however, challenges. The wiretap gave us the motive. The video gave us the vehicle. Shell casings gave us the ballistics and the DNA, while the cell phones gave us some cell site information. There are challenges to this. I mean part of this; the state police were up on a wiretap. I'll briefly address the wiretap issue and I'll be available for questions if you have any more, but wire taps are not common to what people might think. They're not that easy to get. You don't just get ... a police officer

doesn't go up to a judge and say, "I want to wiretap," or, "Here's my search warrant for your wiretap."

You need a political authority, by statute, it requires a political authority either the district attorney or an attorney general or the person in charge of the organized crime task force, or the Attorney General's office to make application for the wiretap. So, it's going to be a political authority who's politically accountable. You then have to show a three-part showing of probable cause, which probable cause to believe that a crime has been committed, probable cause to believe that the facilities, is what the statute says, but the phone's going to capture communications pertinent to that crime, and three that the device within facilities, the device that they're using, is commonly used by your suspect or leads to them or something like that. So, three parts showing of probable cause. Then you have to show them necessity. In other words, a wiretap cannot be the first thing that you use in an investigation. Very often what you have to do is exhaust other traditional investigative techniques.

That's a very, a simplified analysis of wiretap law. The statutory term for it is actually a necessity. You can either show that something has been tried and failed, which is exhaustion. Or you can establish that it's unlikely to succeed, even if you did try. The third way is you can say it's too dangerous to employ. For instance, I don't want to introduce an undercover police officer into this violent gang, because that officer may get killed or injured. That's something I don't want to do. So that would be something that's too dangerous to employ.

So they're not available for the asking, they're very difficult to get. But some of what's making it more difficult is our technological companies out there, our Apples and our Facebooks. Because you remember the San Bernardino case, Apple would not help the FBI get into the suspects' in the San Bernardino case, into their own phones. That's very problematic.

I liken it, what if there's a missing child? Apple won't help you. Apple is not going to help you. That's very troubling from a law enforcement perspective. Even with all the statutory protections you can have in your phone, their still not going to help you. And my own viewpoint on this is companies like Apple and Facebook that say they're protecting your privacy right, I say, "BS." They'll gladly sell your data to some marketing company. They just don't

want to give it to the government. They don't want to lose the proprietary information they have in a lot of these devices.

Just to close with something about Facebook messenger: what's going on currently is that Facebook messenger is, once again having an issue with the FBI. The FBI wants to acquire voice communications that are occurring over Facebook messenger. What Facebook messenger is in essence saying is, "We're not required to comply with you. We're not a telecommunications carrier. We're not covered by the Communications Assistance to Law Enforcement Act of 1994. Therefore, we don't have to provide this to you." Again, it has to do with encryption. They don't want to give up their encryption.

So those are some of the challenges we're facing and we're going to continue to face. I think a lot of the bad guys, unfortunately, know this too. But they, like in the Facebook case, what they try to do is hold Facebook in contempt. That leads me to one story I'll close with.

Years ago, we were trying to do an internet intercept on a computer. Time Warner at the time was not responding to it. A local judge had signed the wiretap order. He goes, "Well hold them in contempt and make an application." So, we made an application. The judge signed the order and off it went to Time Warner. The next morning, he stopped me. He goes, "You know, I signed that order." I said, "Yeah. Thank you." He goes, "They shut my cable off." So be careful what you wish for.

Professor Breger:

So, there's some food for thought and some lessons there. Next, we are going to hear from Steve Hogan, also of the New York State Police Counsel's Office where he's worked for decades. He's also taught as a faculty member at U Albany and the New York Prosecutors Training Institute on issues of criminal justice, science, and scientific evidence, where he's also earned various awards. He's going to speak to us about how emerging DNA technologies can invite a collision between important and sometimes competing social values.

Steve Hogan[**]:

[**] Stephen Hogan is an attorney for the New York State Police. He serves as the representative of the State Police on the New York State Domestic Violence Advisory Council. Steve also works with state and federal prosecutors on

Thanks. I need to stand up, because I have trouble containing my enthusiasm for the issues we are discussing today. We are living in an important moment as the history of the criminal justice system in the United States. Your generation will be attempt to meet the challenge of successfully harnessing the potential of emerging forensic DNA technologies without allowing seriously compromising privacy interests that relate not just to our data, but to our genome. I view this historical moment with awe and with apprehension. The awe is based on the what I know about what forensic DNA technology has done and will do for our criminal justice system. The apprehension is based on certain latent dangers to cherished civil liberties if some of the emerging DNA technologies if they are pushed too far and or are put into use without thorough consideration.

I want to use the time I to attempt to do the following: 1) describe the benefits of the DNA technologies currently in use including DNA databanks; 2) compare them to the investigative techniques and forensic technologies that contributed to wrongful convictions; 3) describe some of the issues social and legal issues that are related to DNA databank searches; 4) offer a note of caution about some recent developments related to private DNA databanks.

Once you learn how the DNA databank system works, you will see that it is pretty amazing. By combining cutting-edge DNA technology with the power of super computing, the Combined DNA Index System ("CODIS") can valuable investigative leads in criminal investigations. Another way of saying it, is that through CODIS, we now have the ability to make connections between crimes scene DNA profiles and the DNA profiles of the possible offender that could often never have been detected.

I won't go into the statistics, but since the CODIS system became fully operational its main benefits have become clear: 1)

---

matters related to admissibility of scientific evidence. Before joining the New York State Police, he prosecuted sex crimes and domestic violence cases as an Assistant District Attorney in Rensselaer County. He is a member of the faculty of the National College of District Attorneys and the New York Prosecutors Training Institute. Steve has served as Adjunct Professor of Biological Sciences and an Adjunct Professor of Criminal Justice at the Justice at the University at Albany since 2002. Mr. Hogan holds a J.D. from the University of Notre Dame Law School, an M.A. in International Affairs from American University and a B.A. from the Rockefeller College of Government and Public Affairs and Policy at the University at Albany

it helps police investigators solve criminal cases (such as rapes and murders) that otherwise never have been solved; 2) it can be used to identify active serial offenders. This benefits society retrospectively by identifying the possible offender of a past crime. In some case, it can also benefit society prospectively because if the serial offender is successfully prosecuted they would not be free to commit violent against others; 3) it has been used on multiple occasions to exonerate the wrongfully convicted. In fact, in some cases, it has been used to identify the actual offender after indictment but before the possible wrongful conviction takes place; and 4) in an era of limited resources, the CODIS system and its state participants generate invaluable leads in criminal investigations for a relatively small amount of money compared to some of the traditional investigative alternatives.

Very briefly, here is how it works: Forensic crime laboratories use cutting-edge DNA technology to develop a DNA profile from crime scene evidence. The DNA profile appears in a digital format—essentially 22 sets of number that are unique for everyone except identical twins. These digital "crime scene" DNA profiles are put into a DNA "crime scene" database. There is another important database. Let's call it the "offender" DNA database. It is populated with the digital DNA profiles of persons who are required to give a DNA sample under their state's DNA databank laws. These digital DNA profiles are normally kept at state DNA databases and many of them profiles are uploaded to the National DNA Index System ("NDIS") maintained by the Federal Bureau of Investigation ("FBI").

The marvel of DNA databank searches is that, through the use of super computing, the digital DNA profiles from every crime scene in New York State can be search against the digital DNA profiles of every "offender" in the United States.

Not only that, but every digital crime scene profile in the New York State DNA Database can be searched against the digital crime scene DNA profiles maintained in the crime scene DNA databases in each of the 50 states. This allows police investigators to detect circumstances where the same person committed crimes in different part of country even if their DNA profile is not contained within any offender database within CODIS.

Beyond that, it is even possible in some cases to search digital crime scene profiles against the digital DNA profiles of offenders in other CODIS partner countries in Europe and Asia.

Think of that! Consider this slightly modified description of an actual case. A man breaks into a woman's apartment in Los Angeles in 2010, rapes her, stabs her to death and then flees the scene undetected. The case remains unsolved for years. Fortunately, the offender left DNA evidence at the crime scene that was used to develop a digital DNA profile. The crime scene DNA profile is uploaded to CODIS in 2010 is searched weekly but no investigative DNA "hits/investigative leads occur. Fast forward to 2018. In that year, the offender is convicted for Grand Larceny in Tel Aviv, Israel. By law, he is required to provide police officials with an offender control sample to be kept in a DNA database in Israel.

Several months after the man's conviction, an authorized international DNA databank search is performed. The result of this search is an apparent match (described as an investigative lead in the DNA hit letter) between the digital DNA profile of the person who likely committed the 2010 rape/murder and Los Angeles and the digital DNA profile of the known offender who is in prison in Israel. Additional police investigation confirms that the suspect was in Los Angeles at the time of the rape/murder. At the conclusion of the investigation, the man is arrested for the 2010 murder and rape in Los Angeles, extradited to the United States and subsequently convicted.

Now as you consider the benefits of the CODIS system ask yourself. If you were the Los Angeles Police Chief and you had billions of dollars to investigate this one case; would you expect to solve this cold case rape/murder using traditional police investigative techniques? Of course not! The DNA Databank architecture allows for billions of searches every few days. These digital searches have already detected hundreds of thousands of "needle in the hay stack" investigative leads for police investigators that would not otherwise be expected to be found.

And please don't forget. Those "investigative leads" are so much more than numbers on a spreadsheet. They represent real people and the people who love them and depend on them. These are people whose lives damaged or destroyed by violent crime. We should also not forget the victims who could be spared the trauma of violent crime when DNA technology is used to solve

cases involving serial offenders that would previously be unsolvable.

To fully appreciate the benefits of current forensic DNA technology, it is helpful to consider how far we have come in only a few decades.

If we consider the way rapes and murders were prosecuted in the late 1980's and early 1990's, it is less difficult understand why that era produced so many wrongful convictions.

As a sex crimes prosecutors in the late 1980s my cases often consisted of three types of evidence: 1) eye witness identification testimony; 2) evidence of confessions; and 3) forensic evidence such as A/B/O blood grouping that could be performed in certain cases.

Some have called 1980's, the era of "Flintstone Forensics." By contrast, modern DNA evidence has been described as "the silent witness." Today, DNA testing is simply performed and the results are reported. In some cases, the DNA test results remove the cloud of suspicion over one or more suspects. In others cases, the DNA test results (depending on the facts of the case) provide compelling evidence of the defendant's guilt.

Here is a question: how did the limitations of forensic science permit, or in some cases contribute to the hundreds of wrongful convictions—for examples those described on the web site of the Innocence Project based out of Cardozo Law School in New York City.

These who study wrongful convictions often point to several contributing factors. They include: 1) the problems associated with eye witness; 2) the demonstrated incidence of false confessions; 3) the over-statement of the probative value of certain forensic tests that during that era.

Do you see the danger? Back then, if an eyewitness in a murder cases was mistake, there was modern-era DNA test to corroborate the testimony. A similar problem existed in criminal cases that were based largely on confessions or in confession cases corroborated by confidential informants. Here again, there was no "silent witness" to answer critical empirical questions.

So how did hundreds of people with the help of dedicated attorney walk out of state prisons for crimes they were convicted of but never committed? I think you know the answer.

Over time the forensic DNA technology advanced to a point that in certain types of cases (if the critical crime scene evidence

had was properly preserved) and modern DNA testing could be performed, the wrongful conviction could be detected.

I would urge you to read the web site of the Innocence Project where you will see another benefit of modern DNA testing. In a large number of cases involving post-conviction DNA testing, not only was it determined that the person convicted of the crime was actually innocent, but the post- conviction DNA testing helped to identify the actual offender.

Modern DNA testing has provided inestimable benefits to the criminal justice system. And, as I said earlier, DNA databanks have been a force for good in New York State and throughout the nation. However, in recent years, two changes to the DNA Databank regulations have engendered controversy. The first is the release of the name of an offender whose DNA profile "offender" is in the New York State DNA Index in the case of "partial matches." The second is the very rarely employed practice of performing "familial searches" of the New York State DNA databank.

I don't have time in my portion of this discussion to explain the details of the New York State "partial match" and "familial search" polices. However, all the relevant information is available on the web site of the New York State Division of Criminal Justice Services (DCJS).

There is a common theme to the critiques of the New York State "partial match" and "familial search policies." The first part of the critique is that the vast majority of the digital DNA profiles in the New York State DNA Index System are taken from control samples of person convicted of designated classes of criminal activity. If you were to examine the demographic data of persons in New York State convicted of the qualifying crimes, you would see that persons of certain demographic groups appear to be over-represented relative the percentage of such individuals in the overall population overall. This becomes relevant when policies allow for the release of names of close relatives of persons who digital DNA profile is in the DNA database.

There are potential perils on the horizon. How many of you have heard of companies like "Ancestry.com," "23 and Me" and "Family Tree?"

I suspect that some of you out there have used them. Of those of you that have used services like these, how many of you read and understood the genetic privacy statements?

Please understand that I am not disparaging any of these companies. Many of my friends have used these services and have been thrilled to learn about their ancestral or medical history. However, we live in an era where we are often tempted to trade away our privacy for convenience or some other benefit.

To many of us in 2019, be have become accustomed to living in a time of reduced digital privacy.

But what about a medical privacy? What about employment discrimination? Medical genetic testing since the time the human genome was has already provided great benefits. However, the promise of even great benefits must be weighed against the dangers of losing our medical privacy, or at least having it compromised.

One case that demonstrates risk associated with medical genetic testing involved the Burlington Northern Sante Fe Railway Company (Burlington Northern). In Burlington Northern, it was determined that the company required its employees to undergo physical examinations. These examinations involve blood work which without employee knowledge had genetic tests for markers predictive of carpal tunnel syndrome. A complaint was made to the United States Equal Employment Opportunity Commission. For alleged violations Americans With Disabilities Act. Burlington Northern settled the case for $2.2 million.

In 2019, federal law and the law in most states prohibits employment discrimination based upon genetic predisposition. However, there have been reported cases in which violations of genetic privacy laws have been alleged.

My advice to you is that before you send in that swab or sign any type of genetic consent form you read and understand the fine print.

I mentioned earlier the controversy over governments policies such as familial searching. However, while these battles have been fought relatively slowly and often in the public forum a sea change has been occurring in the world of private and open source DNA databases.

How many of you here have heard about the 2018 arrest of the "Golden State killer.?" For those of you who don't a serial killer rain terror across the state of California intermittently between 1974 and 1986 was arrested and charged with committing more than 50 rapes and 12 murders.

The defendant, Joseph James DeAngelo, was identified by police officers who used crime scene DNA profiles to search an open source DNA database known as GEDmatch that contains approximately 650,000 genetic profiles.

After querying the GEDmatch database, detectives constructed forensic a genealogy tree of possible relatives of the serial killer. Using the genetic information, they obtained from GEDmatch and hundreds of hours of traditional investigative work, they were able to identify DeAngelo as a suspect.

After identifying him they obtained a control sample from property he had abandoned. When the digital DNA profile developed from the control sample was compared to the digital DNA profile from the crime scene evidence the connection to the defendant was established.

Solving a complicated serial killer cold case was a phenomenal achievement for the police investigators. However, it was a reminder that the police use of public DNA databases and or DNA profiles obtained from private DNA testing services is likely the next frontier.

Once again there are important competing social values. Once again, society and the criminal justice system must work to evaluate the tangible benefits to the criminal justice system of emerging DNA technologies and attempt to ensure that these benefits are obtained without sacrificing privacy rights.

As I said at the beginning, we are living in an important historical moment. A moment of great promise and some peril. I appreciate opportunity you have given me to share my thoughts with you.

Thank you.

Professor Breger:

Thank you, Mr. Hogan. And now we will hear from our last panellist, who will be refreshing because she's the only one who's going to be speaking from a defense point of view. We've had a lot of prosecutors today. So Kimberley Wallace is currently an associate at the law firm of Carter Conboy and she has served as an assistant public defender out of Dutchess County and briefly as an ADA out of Albany. She will talk to us about some of the privacy issues raised today and respond from the defense point of view about the increasing erosion of our privacy rights.

Kimberley Wallace††:

Hi everyone. So as a defense attorney, I have a love-hate relationship with technology. I love it when, obviously, it helps my client and I dislike it when it doesn't. I've had several cases where it's either helped or harmed a client. Earlier this year I did a felony DWI case. My client refused, which worked out in our favor. But there was no body cam, dash cam, no surveillance whatsoever. We live in a society right now where if it's not on video, did it really happen? I always joke around with my friends. I say, "Oh, I went to the gym."

They're like, "Well you didn't Snapchat the fact that you did go. So did you really go?" So I really, in that trial, played off the fact that the troopers ... sorry.

Sorry, everybody all around. That they didn't have any sense sort of surveillance. It was at the toll booth. It was at night. It was in February. Did you really step off of this imaginary line? We don't know. That casted a lot of reasonable doubt and I won that trial.

On the other side, I've had surveillance where a client, I remember vividly in Dutchess County. It was a petty larceny, nothing crazy. But my client was adamant that she was not there. She didn't go to this store. She didn't know what they were talking about. I got the surveillance video and it was the most beautiful HD quality video that you could ever see. She came into my office and we watched it together and she said, "That's not me." She said, "She's at least 10 pounds heavier than I am."

---

†† Kimberley Wallace is an Associate at Carter Conboy. She represents individuals and businesses in white collar and corporate governance matters and investigations, as well as members of law enforcement in matters involving discipline, critical incidents, criminal defense, and civil litigation defense of constitutional and civil rights issues. Additionally, Kimberley defends various transportation companies, commercial carriers, manufacturers, and professionals in State and Federal Courts throughout New York, as well as before administrative agencies and in mediation and arbitration matters. Before joining Carter Conboy, Kimberley was an Assistant Public Defender and Assistant District Attorney in Albany and Dutchess counties, where she managed misdemeanor and felony criminal cases from inception through trial. Ms. Wallace received her B.S. from Sage College of Albany, Law and Society, Oxford University (2012) and her J.D. from Florida State University College of Law (2012). She is a member of the New York State Bar Association, the Capital District Women's Bar Association, Capital District Black and Hispanic bar Association, the Albany County Bar Association and Sage College of Albany Alumni Association Board of Directors (2081- 19).

And I sat there and I looked at the video, I looked at her and I said, "You're wearing the same cheetah print tights in the video that you have on right now."

So needless to say, we took the deal, case. But technology at this point is so advanced that the courts aren't in line with technology. Mr. Dale mentioned cell phones and records and placing people in different locations to make a case. But technology is even more advanced than that. It brings up a lot of privacy concerns. One particular device that I've read up on is called the Sting Ray. Has anybody here ever heard of it? A couple of people have.

So that device basically mimics a cell phone tower. The government can use that to actually pin point where people are, basically using it as a tracking device. Luckily for the defense, in 2016, there was a case in the Southern District of New York where Judge Pauley ruled that they needed a search warrant to use on this particular device. What's troubling about the Sting Ray is that it not only pinpoints one particular device, it actually allows other devices that are in a short radius to connect as well. So innocent bystanders, people who are in that general vicinity there information is being transmitted to this device unknowingly. We don't know what's happening with that information, how long it's being stored, and what it's being used for.

Ms. Assini mentioned something earlier that stood out to me, the use of the license plate readers. Is anybody here driving here today thought, "I wonder how many times they scanned my license plate today?" Nobody. You did? Oh! What were you thinking?

A lot, right? So, I see the laws evolving and there being some litigation in that aspect because most people, except one, they drive to and from work, to and from appointments. They drive everywhere. What we don't really think about, most of us here are law abiding citizens. I'm sure. Worst case scenario, hackers get into a system with, for example, your scanned license plate. One or two scans, no big deal, but over a big period of time you can basically track somebody's life. Right? You know that Kim Wallace is driving to work around 8:45 every day and she's passing this location. So that means I am not home. And who knows what can happen with these technologies.

So, I mean, my hope for the future is that the courts catch up to technology. Because once these cases are in the courts, we see that the courts lean more towards suppressing certain searches and requiring that these agencies, law enforcement, get a search warrant. So I think that the cases are evolving but it's not as fast as technology is advancing. Who knows whatever else is out there? Let me just say, police know some other technologies that are advancing that there are privacy issues associated with them. So for the future that is my hope.

Professor Breger:

Okay. Thank you, Ms. Wallace. So this has been a terrific panel. Lots of food for thought. While I have plenty of questions for the panelists, I thought it would be better to see if you did. So we have Nick Berwick, who's going to come around with a mic. If you have a question just raise your hand, for any of the panelists or even just general questions are fine. Just raise your hand.

Audience question:

This question is for Ms. Assini. You mentioned about the video camera footage that is stored, or that Schenectady has access to. You talked about the way that that can be used to disprove statements or confirm a fact, to confirm whether or not a story is true. I'm wondering to what extent, either defendants are able to get access to that information or someone who are able to get access to that information or someone who's dealing with the situation of alleged police misconduct?

Jennifer Assini:

All of our video is connected to, or a production of it, is connected with a criminal case; a criminal investigation. And we denied foil requests, under an exception to that. You don't want to reveal your investigative techniques. You don't want to put at risk your information. Your technology as far as ... people can look up and see it, but it can also blend in. And there are multiple reasons that the exception applies.

After a case is completed, normal subpoena routine may allow access to that if police misconduct on ... sometimes it can be used for internal investigation within the police department, and/or if it becomes a criminal investigation. That's where it becomes available to the prosecution. Defense under discovery, they would

get it under normal discovery timelines. We're not going to get it; we don't have open file discovery in felony level cases. So, it's going to follow the normal protocol.
It would have to go to the police department, and a case file would be opened, and then the case would be ... the video footage would be reviewed in the normal course by the crime analysts or the chief technical resource officer. And that gets made part of the case. Again, in the normal process it would become available as the case would proceed under discovery. I don't know if that's ...
Professor Breger:
Good question. Any other questions? We have one over here.

Audience Question:
Yes. Okay. Similar question about the use of DNA. When an individual does, typically a private investigator seeking to perform DNA on in a divorce proceeding, where the wife wants to have tested judicial precaution, at least in New York State, the Civil Rights Law requires that DNA testing performed for identity purposes.

Steve Hogan:
It is my understanding that testing performed for purposes other than forensic cases—criminal cases-- must be in the manner prescribed by the New York State Health Department in compliance with applicable statutes and regulations. For forensic DNA testing (testing for use in criminal proceedings) you look to Executive Law Article 49B and the associated regulations.
Audience Question:
I worked for the health department, regulatory program responsible for the approval of DNA testing labs outside of public conflict potentially, because there are certainly many circumstances where a private citizen did not meet the context of approval law proceedings. He's interested in evidence that might, and it also raises the issue; DNA didn't settle everything. It wasn't the perfect solution. And there is flawed forensics, and misleading DNA testing that's gone on in not so recent memory. Human enterprises are not always infallible. Quality is important, and public labs like the state police crime laboratory system that Dr. Wickenheiser runs, are committed to improvement.

Steve Hogan:

What Dr. Willie did was she ran a lab where, if you're going to take a specimen from New York and have it independently tested, New York basically says you couldn't take it to a garage band DNA lab and then come back and report the results, because there are clinical standards that have to be met. And I think that's one area where prosecution and defense always agree; constant improvement. Let's make this science better and let's not step on each other because the better the science, again going back to my original point, we had crap science and we had massive injustice. We've got much better science, but we've got a way to go and the quality can always get better.

Professor Breger:

Okay. I think we can take one more before we have a break.

Audience Question:

So, right now there's a lot of research has been going on into DNA technologies. Is there, like with biome research, is that something that you guys are looking into or is it something that seems really promising for the future?

Steve Hogan:

I could tell you, but I would have to kill you. The microbiome. I just went to a lecture and was pretty blown away. The idea is that we're constantly shedding cells, and that this ... we create our own atmosphere. Think pig pen, I'm Charlie Brown, and within the microbiome you can learn things. The presenter, from an Illinois University, was able to tell, in a controlled experiment, using DNA testing of a simulated micro biome was able to accurately tell us many things about the person involved in the staged burglary.

My best estimate is that forensic microbiome testing is perhaps ten years down the road minimum to be something that's a readily usable. It's tremendously fascinating. And it also reminds you that you're in a tough spot because you can't stop shedding your DNA. You just can't. And so, you are a little bit of a tough spot protecting your 4th Amendment rights since you can't stop "abandoning" cells in which you no longer have any reasonable

expectation of privacy—at least under current law. Shedding really isn't a voluntary act. .

In New York State, it's still a biological specimen derived from the human body. And it would require an analysis, and generally the only application for a microbiome specimen microbiology lab, where looking at the cells.

Professor Breger:

Okay, I think at this time we do have to stop questions. We are going to have a break in the back of the room. We'll have a break, and then we get to hear from our keynote at five o'clock. So, thank you to our panellists.

Julia Kosineski:

Thank you to all of our panelists, we have a gift for you from the Albany Law Journal of Science and Technology. And if everyone wants to take a break and go out this way, that's where the restrooms are, and we have coffee and cookies. And then just try to be back in the room in ten or twelve minutes. Thank you.