Transcript - Digital DNA at the Crime Scene: Leveraging Mobile Signals to Uncover the Truth

Welcome, everyone, to the National Criminal Justice Training Center webinar. Our topic today is Digital DNA at the Crime Scene, Leveraging Mobile Signals to Uncover the Truth. My name is Katie, and I will be your moderator for today. Don't miss these upcoming training opportunities. To register or view the most current dates and times, please visit ncjtc.org/contracting. Today's webinar is brought to you by NCJTC and NW3C.

The National White Collar Crime Center, NW3C, and the National Criminal Justice Training Center of Fox Valley Technical College, NCJTC, are pleased to announce their partnership in hosting the Solving Crimes Through Emerging Technologies Conference, taking place from January 13th through the 15th, 2026, in Las Vegas, Nevada. Two great organizations coming together with one great mission.

Today's presenters will be part of our 2026 Solving Crimes Through Emerging Technologies Conference that will be held in Las Vegas, Nevada, January 13th through the 15th, 2026. Please join us at our conference to learn more. We will be bringing law enforcement professionals and industry leaders together to explore emerging internet of things, IoT, technologies, discover investigative methods, and consider how navigating the landscape of the IoT can help solve crimes and make communities safer. To view this conference and other current conference offerings, please visit ncjtc.org/conferences.

With that, let's try our first poll question. The question is, which of the following best describes your current role or affiliation? Your choices are professional support staff and public safety, victim services, victim advocate, court, judicial, sworn active law enforcement, retired but still supporting the mission, community member, or private industry supporting law enforcement, or other. Please respond to the poll now. As you can see from the results, we have a plethora of sworn and active law enforcement. Coming in second is professional support staff and public safety.

We are pleased to introduce you to our presenters today. Kevin Branzetti is the CEO of the National Child Protection Task Force. The NCPTF provides investigative expertise and resources to law enforcement agencies worldwide on cases involving missing, exploited and trafficked children. Their goals are to bring children home, bring predators to justice, and train investigators based on lessons learned. Mr. Branzetti is a former deputy chief of intelligence at the Manhattan District Attorney's Office, assigned to oversee terrorism and cyber crime-related investigations.

He retired from the NYPD in 2015 after 22 years of service, and during the final six years in intel, he was the commanding officer of the Cyber Intelligence Unit. He has been involved with the criminal, financial and terrorism investigations, cyber intelligence, human intelligence, source development, and intelligence collection analysts, and dissemination.

Captain Pete Glogoza is a veteran of the Indiana State Police, with an impressive career in various key units such as the Methamphetamine Suppression Unit, Technical Support Unit and Electronic Service Unit. He currently leads the intelligence and technical service section of the Special Investigations Division. Pete's work has played a significant role in numerous state and federal investigations.

He was even handpicked for the esteemed technical fellowship program by the National Domestic Communications Assistance Center, NDCAC, at the FBI's Operational Technology Division. His leadership has led the Indiana State Police electronic surveillance units to work over 700 cases in 2022, resulting in locating of 294 wanted individuals. Thank you for joining us, Kevin and Pete. The time is now yours.

Well, good afternoon. Thank you. I appreciate everybody for taking time out of their days. I know life is busy. Work is busy. Do more with less. So thank you for that. Quick disclaimer and some other things, and then I'm going to go right back to Pete. One, Pete and I will go over a whole bunch of things here. Different jurisdictions have different rules. Some places, it's a subpoena. Some places, it's a judge's order or a search warrant, or some places, you're not allowed to do it. That's not our job to figure that out.

We're just giving you things that we have seen and done, or been a part of in our careers. So it's for you to figure out with your lawyers, your executives, prosecutors, if you can or can't. Before teaching anything, I go over the three golden rules of doing stuff. My suggestion to everybody out there, if you're teaching something, if you're putting together presentations, you're writing documents on behalf of your agency or your department.

Treat everything as a standalone, put things in there to make sure that if the general public got hold of it, they would understand a little bit more about what we do and why we do things. Golden rule in life. First rule, we use the least intrusive way possible. Second, everything we do has to be for legitimate law enforcement purpose. And the last is, we protect everybody's civil rights and liberties.

This is the standard we all work by every single day in our careers. I don't know an agency that has a different standard. But I feel it's important to say it because, again, people on the outside, when these things are through freedom of information or other things leaked, it's good to remind the public who only knows about us through the news and crazy TV shows. So with that, thank you. And Pete, you're up.

All right. Good afternoon, everyone, or morning, depending on where you're at. I'm Peter Glogoza. I'm with the Indiana State Police. I've been with the Indiana State Police for 28 years as of Monday. Quite honestly, we never thought that I would still be on the department, and definitely never would have thought that I would be a captain over our investigative support section.

You will see two QR codes on here. One is my contact information. Feel free to reach out to me at any time. If I can't answer the question, usually, I have enough contacts that I've established over the years that I can find someone to help you or answer the question, or get you to the right person on our team to answer your question. You'll also see there that I have the investigative support section's search warrant repository.

Unfortunately, this is designed for law enforcement in Indiana. But one of the things that I wanted to combat back in 2007, when I came to the covert side of law enforcement, was overcoming fear of writing warrants in the technical world. And our answer has evolved to this search warrant repository. So even if you're not from Indiana, it sure would be a helpful starting process. If you're trying to do a warrant that is technically based, that is something that you haven't done before.

The only part is, obviously, it may reference Indiana IC codes. And it'll have the statutory heading for the Indiana State Police. With that being said, since 2007, I've been on the covert side. And I was the administrator to the Indiana State Police's wiretap capabilities. And in 2014, I went to our fugitive unit, where I started to really get involved in cell site analysis and real time data to support fugitive apprehension.

2017, I came back to the electronic surveillance unit because we saw the evolving use of historical call detail records and cell site location information to support investigations. So my job at that point was to start developing our team that can handle all these things. So right now, I'm supervising our fugitive and threat response unit, our cell site analysis unit, and our covert technologies unit. And once again, my biggest thing in speaking to everybody today is, I'm probably going to talk at about a 30,000 foot view of what's going on, because we don't know the capabilities of everybody that is listening. So we'll cover a little bit of everything.

Kevin is a visionary at what he does. I'm more of, what do we see in the cellular environment that the rubber meets the road, and what are we doing now, and what are we being successful at. Kevin understands terms and conditions, and privacy policies, and what capabilities may exist out there that we are not taking advantage of as of yet.

Also, I'll probably mention throughout some automated tools. I'm not a proponent of any specific tool. I will tell you right now that I've used CellHawk, I've used Nighthawk, I've used Gladiator, I've used LexisNexis tracks. But if I focus on any one given tool, I'll probably talk about CastViz, which is a free mapping tool through the National Domestic Communications Assistance Center. That way, I'm not promoting any specific item that has a value or a cost to it.

So let's get into what we're going to talk about today. So we're going to talk about digital DNA at a crime scene. As it applies to me, that means I'm going to talk about cell phones and how they affect your crime scene, and how we can leverage that data to reconstruct events, locate witnesses, refute alibis, and ultimately, support your case. I'm going to talk about cell site location information.

And everyone on here is probably going to be familiar with the cell site location information side, so that'll be kind of a quick "this is how it works." And then timing advance. Well, we've all become familiar with timing advance, which is the measurement of distance from the tower to your phone, back to the tower, measurement of the speed of light. All three of the major providers have a version of it. We'll talk about some of the things that have been happening recently as the tech guys talk about bands and how we can best use this to our advantage.

Something I often don't hear about when I'm on presentations or even when I'm at conferences, is real time data. So I will hit on pings and pen register, trap and trace. These things cost money. Pen registers require special equipment. Pings do not. But we need to understand their value to a case, whether it's historical, or whether it's an ongoing case. And then what I really think is the game changer in our world today is connected cars and how we should be approaching them as a data set.

Since 2021, we can pretty much assume that a connected car is much like a cell phone, and that data is going to be held by the service provider. It's usually T-Mobile, AT&T, or Verizon. AT&T has pretty much won the market at this point and have a high percentage of the connected cars on their system. But that also means that we have to talk about the legal landscape. Obviously, I'm not a lawyer, but I will talk a little bit about area searches and tower dumps, and where we are at with those right now, and what we could see in the future.

And if it seems like I'm bouncing around a lot, I don't know my time zones very well, which is a shame. So I started my coffee intake two hours early. And I've had more coffee and more coffee, so I am pretty pumped up to talk today. So our objectives today, like I said earlier, I want to talk about some cell site location information. Not a bunch, but I will talk about timing advance and Verizon's version of timing advance, which is the real time tool, RTT data.

And I want you to understand their values, their limitations, and then how they play into other things that we are going to do at the crime scene, such as an area search, and how that data is derived to support your case. I'm going to hit on connected vehicles. There's a lot of free training out there. The best thing about COVID right now is free webinars, like this one, where you can start learning.

Connected vehicles. I would always check NW3C. I would check NCJTC, see what free trainings they have, see what paid trainings they have. Connected vehicles are going to be the boon. And we have to think of them as on the cellular network. But because you're not paying for service for these vehicles, there's a reason that the manufacturer is activating that. So not only are the service providers, AT&T, Verizon, and T-Mobile going to have that data, but the manufacturers are going to have data that can be crucial to our investigations, as well.

I will hound on this throughout that data preservation, understanding the shelf life of records in the network is extremely important. If we don't preserve that data in time, or we don't have a good understanding of those shelf lives, which they've made it very convenient for us, and all the providers have a different shelf life for every record, then we can miss perishable data that can support our investigations. And then lastly, I'll talk about United States versus Smith, which was a geofence ruling out of the Fifth District, and how that could potentially affect us, and whether or not we think that it'll make its way to the Supreme Court.

So in its essence-- and this has not changed probably since I came on the department in 1997. And yes, I'm dating myself, and it hurt a little bit to even say it. Every mobile device that we have continuously interacts with cellular networks. And it creates a persistent, passive digital footprint that we can utilize to our advantage in law enforcement if we know how to ask for it, and we understand the shelf life of that data. And it can prove very advantageous to one. It identifies suspects, it identifies victims and witnesses.

These phones are as important to them as your eyes are to us. I could ask us all in attendance today, how many of us have one cell phone? Everyone's going to say, yes, I have one. And 3/4 of us are going to say, we have another one. So our bad guys are not any different. They are going to have multiple phones, as well, and we should be aware of that and at least be suspicious of it, on top of the fact that, hopefully, they have a car newer than 2021, and we have another mechanism.

Within this, I'm going to talk about tower dumps and area searches. In the past, when investigators would call me 10 years ago about tower dumps, I would just shake my head, and I would know immediately that they probably don't have an understanding of what that really means, because the perception was, every device is going to be on this tower dump. Well, in 2025, I think that we have a better understanding of investigators, that we have a better chance, especially if it's AT&T, that device would be on a tower dump. But still, with T-Mobile and Verizon, we're only going to have Voice, and there's going to be shelf lives for that, as well.

But within those area searches, as we're talking about timing advance, we're going to talk about how are the providers, and specifically, T-Mobile and AT&T, how are they using timing advance to fulfill an area search request? Because if we understand how they're doing that, we as practitioners can better design our request based on the density of cell towers that are available to us. And just as importantly, those connected vehicles are another data point that will be inside either the tower dump, or potentially, if it's not AT&T, and T-Mobile, and Verizon area searches. Just another data point that can be important in resolving our case.

And then once again, because I don't hear enough about precision location or real time location information in pings or pen registers, we'll touch on that. Of course, it requires special equipment for pin registers that not everyone will have. But sometimes we are only as powerful as the people we know and the contacts we have that can assist us in these cases.

Our next poll question. When requesting an area search, do you know that there are carrier-specific limitations on distance and time? Yes or no? As you can see from the results, 78% said yes, and 22% said no.

So to me, that means 78% of you are hearing me instruct something that you probably already know or have a good impression of how to accomplish it. So don't worry. The visionary stuff from Kevin will be coming up when I'm finished. And he amazes me when he starts throwing things out that I haven't thought about to resolve a case. My imagination is good in the cell site world, but sometimes it needs to be expanded in other facets.

So how does cell site location information work? This is the stuff that I'll try to be quick going through, because we understand that your phone, your cell phone connects to the highest quality tower. It doesn't need to be the closest or the strongest. It depends on efficiency, and your phone will make those decisions for you. I can specifically relate to my house. It definitely doesn't go to the closest tower, especially if I'm at the front of the house.

The golf course behind me has a huge tower right outside the back door. If I'm at the back of my house, that's the tower I use. When I'm at the front of the house, I actually use one that's four miles away at the interstate. So all this data, or our phone calls, or our text messages are recorded by the providers as call detail records. So we have a record of that that is available to us. And that record includes dialed digits, duration, the tower, the sector, and those things we are used to utilizing in supportive investigations. And we know that tower and sector, it's an estimation of where our device is.

And to give an idea just in case, there are individuals on here who don't remember or just need a refresher. A cell site and a sector just gives us an approximate area. It's not a GPS. If we run into a problem on the stand, it's usually a over estimation of location. So as we talk about just a phone call and a tower and a sector, it is a general coverage area. And we do have records available to us that we'll talk about that do limit that.

Now, I've been questioned on this on the stand, where I've been able to say, or I've been asked, so is this the best you can do? And on occasions, the best you can do is shrink the world down to a city, down to a tower, and a sector. And when you think about the cellular network and the Earth, that's pretty amazing. But we do like it when we can do better.

Timing advance data. It's just a simple-- it's a measurement of the speed of light to our device, and back to the tower. And we use the heck out of it, and it's changed, and it just keeps getting better for us. And we'll talk about the bands. And when I hear forensic analytics, who's given some free webinars on NW3C, which is Joseph Hoecht and Martin Griffiths, who Joseph actually wrote the book, which is funny when I say, no, he wrote the book. And I really mean it's the only book. So if you don't have that book, and you're a cell site analysis practitioner, it'd be good to have.

But they've really dove into timing advanced data over the last year, year and a half. And I would say two or three years ago, our Fugitive Unit and myself, we would routinely find bad guys using timing-advance data. It is very accurate, but we're always striving to be more precise. So in the 2G world, the band's associated, the timing arrival could be 550 on the arc. And then 4G, which we're still mostly seeing, it's 78 meters. So you go back to shrinking the world down to a tower and a sector, and an arc on that sector that is 78 meters wide, which is pretty impressive.

And then where we all want to be is in the 5G world. That can be from nine meters all the way up to 78 meters, which is an absolute game changer if we get it to where it's going to be nine. And this stuff is only going to get better. And this isn't going to go away, whereas we worry about some things disappearing from us because of court cases, just standard call detail records and engineering records. I don't see anything happening to those.

Now, there are some limitations that we'll talk about as far as multipath propagation. I live in Indiana. That's a factoid there. And our state's pretty flat, so I don't get to worry a whole lot about that. On top of that, we don't have any real major cities other than Indianapolis. And quite honestly, in the 15 or so years I've been dealing with cell phones, downtown Indianapolis is not really anywhere that I've had cases. So I haven't had to worry about a whole lot of the multipath propagation that we're going to talk about.

So when I talk about bands, an example-- and this is from forensic analytics. And if you don't have a relationship, or you haven't taken a class, either through in NCJTC or in NW3C, look on NW3C. This is one of the papers that forensic analytics has written just on timing of arrival. And you can reach out to me afterwards, too, and I'm sure they'd be OK with me sharing that with you, as well. So when we talk about the 4G and the 78 meter bands, 78.07, and we use the example on the left of that sector and your azimuth in the middle there. And we could go out to 19 different bands.

And that's the information we're getting in the call detail records when we get timing advance or RTT from Verizon. And once again, you can think about a shrinking the world or wherever. If we can shrink it down to my bad guy was in this band or within one of this band based on this paper they wrote, that's 78 meters. Your bad guy better say that he was there and not somewhere else, or this is going to be very damning to them. And this is the same information you would get from a connected car that is communicating with the network if you get the TA from AT&T, T-Mobile or Verizon.

So this multipath propagation that I was talking about that I don't have to worry about too much in Indiana, because, really, all we have is Indianapolis. And quite honestly, it's not like we have a bunch of high rises in Indianapolis either. But in Chicago, New York, a lot of places on the East Coast and West Coast, you would be susceptible to this, to where the TA arc may be a little bit farther away than where the device is. And still, it's just a measurement of the speed of light.

Now, how do we combat that? Well, I'm going to show you a slide here in a few, where on an important case on a homicide, we actually had seven different towers that provided us timing advanced data. So even if we had some multipath propagation, our accuracy was good, and we had multiple Timing Advance arcs. So we were even more precise, and I'll talk about the difference between accuracy and precision. We're always trying to elevate our case to have more precision. But these Timing Advance arcs are accurate.

Once again, I'll hit on the real time data, pings and pin registers. And there's probably a lot of people on here that have had the opportunity to ping, usually, probably associated to an exigency case, maybe a missing child, kidnapping, homicide, where we think the person is moving on to a different one. Or you're working in the drugs side of law enforcement, in which case we do a lot of pings.

We've seen these evolve or devolve from 2014, when I initially started with the fugitive unit, where it was not uncommon for us to do a ping and have 10-meter accuracy. And that really made hunting fugitives pretty easy. And then Android and Google, Android and Apple both figured out a way to obfuscate the location information. So now what we end up with is, 300 meters to 3,000 meters. And you can imagine that a 3,000-meter ping does not really help you all that much.

As far as pen register trap and trace, we will do those in exigencies and, obviously, in support of drug investigations. The problem is that you have to have special hardware and software to accomplish those. So maybe ask yourself, who in your area has these capabilities? In Indiana, it is, honestly, just the federal agencies and the Indiana State Police. I'm not aware of another agency that can do a pen register or a trap and trace.

For those that aren't familiar with a pen register, pen register is recording anything that you do outgoing, so a text message, a phone call, or data sessions, and providing you a duration, the associate number, and the tower and the sector that that call happened on. And that's happening in real time. The trap and trace side records everything that's incoming.

Now, that's obviously not really how it happens in the digital world that we exist in. But originally, when pen registers, trap and traces in 2007, when I came into the unit, we still actually went out to junction boxes, and we would have to plug in and find the lines for our target land line. So that's been a really good change, because I was not very good at that back in 2007 when I had no technical capability, pretty much whatsoever.

These things do cost money, and it can get expensive fast, especially pen registers, trap and traces, because what they like to do is, even if you're up for a day, they'll charge you for 30 days. You don't have to worry about this on the exigent side. They aren't charging you for exigence. But you only get 48 hours worth of data when you do an exigent as far as moving forward.

Our next poll question. Do you know who in your area of responsibility has the equipment registered to complete a pen register report, trap and trace? Yes or no? 59% said yes, and 41% said no.

So for those 41% that said no, your federal agencies are going to have the equipment necessary. There's really only five companies that supply this. And they'd be JSI, Penlink, Scitech, Gladiator, and I might be forgetting someone, so I apologize to that someone. And like I said, these require special equipment and special connections to the providers. So there's an investment there. If you're one of those 41, and you want to send me a message, I'll find out who in your area has-- some states, there are numerous agencies that have this capability. If you're from Indiana, yeah, like Kevin said, it's me.

And so is my pregnant pause word. I apologize for that. Some of the analysts are supposed to come in here and spray me with water if I use that. Hopefully.

This would have been so much more fun if we were sitting next to each other, because I would have sprayed you.

[LAUGHS] I don't blame you. Let's talk about the connected vehicles and why these are important. It's not just because if it's newer than 2021. And I'm not saying discount before '21, because some cars are connected before that. But what I want you to think about is how that can be incorporated into, one, your imagination, and to your crime scene if you have a connected car. And think about how important it is to have cooperation and data, because quite honestly, I don't like testifying all that much, because I don't do it enough.

So if I can have enough data to corroborate what I'm talking about, that I don't have to worry about being on the stand, big fan of that. So not only am I thinking AT&T, T-Mobile, or Verizon. Leads online has a toolbox that has some great information on helping you identify what provider is associated to connected cars and how to go about obtaining that information.

We don't make it simple. Some manufacturers, all you need is the VIN. And AT&T could potentially resolve it to your car. But unfortunately, sometimes they need the phone number associated to that, because if you have a connected car, there's a phone number associated to that car, and then T-Mobile and Verizon. So it involves reaching out to the manufacturer with the VIN to find out that information. Or there's another way to obtain it, which we're going to talk about here in a few minutes.

But I'm going to use Stellantis because I have a Jeep. Yeah, I have a Jeep. And if you buy a Jeep, and it's a connected car, and you didn't pay to have this SIM card activated to utilize, but I'm telling you, it's still on and it's communicating, why? Why is because Stellantis is collecting data. And they, along with all the other manufacturers, are trying to figure out how to be the next Amazon, the next Apple, and the next Google. So they're trying to figure out how to utilize that data to make money, which means they are collecting that data.

So think of that as the next step. Not only is it connected, but they may have better information. When we talk about the TA arcs, what's even better is a GPS location, which they may have. So don't overlook that as far as an opportunity to improve your case. So what I'd like to get into is, we all understand that we can get call detail records for our suspect, for our victim, and we can support our case like that.

But I wanted to talk about tower dumps and area searches, and how we can navigate that world, and what in that world is going to support our investigations, and, as I said several times, more about shelf life, and more about preservation of records. All three of the major providers now have easily accessible portals to support our investigations. It's not like five or six years ago when, to get on the horizon portal, you needed an abacus to do it. Now it's pretty simple, and you can get that stuff preserved.

T-Mobile has improved their portal significantly over the last 10 years, really, in the last two. It's really become useful, and a great way to deliver your search warrants. And AT&T is using a third party provider to take care of theirs, and that's helped as well. So what are tower dumps? Tower dumps are a law enforcement technique, where we request and receive data from cell phone companies about devices connected to a specific cell tower or multiple cell towers that we have identified during a specific time period for a specific location.

So we're giving them a crime scene or a GPS location, and we're asking for-- we'll use the example of an hour. And we want to have all the data for that hour that served that area. One of two things. We can let the provider pick our towers, or you could go into NDCAC's cell site database and download the tower list, and map it. Then you could try to pick the towers that you want. Where that has become valuable to me in the past is, if you deal with a lot of phone records and ask your fugitive guys if you have a fugitive team, we see towers farther away that service certain areas. And we see TA from multiple towers.

So depending on the type of case, I will let the provider pick what towers they are going to dump to service an area. But sometimes I want to pick my own. We can use these to identify potential suspects, persons of interest, potential witnesses, and we'll talk about. The value of it. Is the value of it in one location, or is the value of it in multiple locations? And what data is kept? The nice thing about AT&T is they keep voice, text and data sessions for three years. And that becomes important, because if I talk about data sessions, then that means in a tower dump, you are also going to have your vehicles.

And this is an extremely large amount of data that you're going to obtain in your tower dump, depending on your time. T-Mobile, they're going to keep voice for two years, and then Verizon is the complicated one that we need to think about for shelf life. They're going to keep voice calls for one year. But part of a tower dump with Verizon is going to be their real time tool data, so their RTT data. And that is only in the network for seven days. Now, you're going to hear people say, well, it's 7 to 10 days, or it's diminishing. Well, it diminishes a lot. I would lock in on that seven-day thing.

And if you're preserving on day six or day seven, you need to follow up with a phone call to Verizon to reiterate. They do say that in the portal, if you preserve RTT, it preserves it itself without them doing anything. I would still call. It is perishable. And if they don't get it done, or there's a problem in the system, then you would lose that data. And that would be-- it's a lot of data and we have had great success since 2014.

I understand that in the state of Indiana, outside of Indianapolis, Verizon is still my number one carrier. I have preemptively given permission for my guys to preserve whatever tower data they want within that seven days for Verizon. And I can think of 7 to 10 times right off hand, where a suspect was developed much later. That had a Verizon phone, and we were able to then serve the tower dump request to Verizon and be able to recreate that footprint for that device.

Hey, Pete.

Yes.

Quick question. How are vehicles identified in those dumps?

You will see them. Actually, Christopher Mount took care of it there with the APN column. But once again, I would go to leads online to that toolbox. And they have the connected vehicles, and they have a breakdown of where in the record you would see that. And honestly, it sticks out all the providers that will be in there. It'll be obvious to you.

So it'll say Audi, or BMW or something.

Yes. So while the example I just gave you were the ones I've done, just because I knew we were running out of time, and I thought it was important enough. And I understand the dynamics. And the geography of Indiana is a single location. Well, we don't send a crime scene. We don't send crime scene investigators in to a crime scene and have them not document everything. And because there's a shelf life, then why wouldn't we-- maybe not for every case, but I like to say, all cases are created equal, but they're not.

There are cases where it would be beneficial to preserve that entire network, whether it's seven days, or 30 days for T-Mobile, or a year or two years, two years for T-Mobile-- sorry-- on the tower dump side, or three years for AT&T. We don't want to risk losing that data for the investigators to develop a suspect later, that we can then come back to that original set of records and re-create their footprint inside that. So you do have to know the exact timeframe. This is going to cost money.

In the old days, this was cost-prohibitive. You could spend a lot of money. We had an eight-year-old in a suitcase that we found in the middle of a field. And while we were trying to narrow down the time, I was not willing to lose those Verizon or AT&T records, just in case. And I, by making phone calls or having a good relationship with the FBI cast team, I was able to preserve 72 hours worth of our AT&T data.

And yes, that did cost me-- not me. It didn't cost me a dime. It did cost the state of Indiana $20,000 just to Verizon. But there are cases where I am not willing. And I understand that I am lucky and have the support of my agency when I do that. And if someone here is in Indiana and doesn't have that support, reach out to me, and I'll take care of it. I pay plenty of bills for other agencies. That doesn't bother me in the cell site world. I'm not paying other stuff.

So we do need to identify what cell sites service that location. Or like I said, we can let the provider pick that. And then, we need to act on preservations. With Verizon, on day six, I'm going to preserve and I'm going to follow it up with a phone call. And I'm actually going to get into when we talk about area searches. AT&T is the same.

So depending on what we ask for, we're preserving-- in a tower dump, which is just what I'm addressing right now-- we're preserving that outgoing, incoming, text messages and the data sessions for AT&T, the voices, voice for T-Mobile, and the voice for Verizon. In area searches, we're going to be asking for all the stuff, but we have to define that much differently than we define the tower dome.

So hopefully, I answer your question here in a second, Robert. Where are tower dumps the best? It's when we have multiple locations. We have multiple scenes or we have other information through the investigation, which, when we're doing tower dumps, it involves your investigator doing a great job, or it involves us using our imagination. We had a case recently and it plays into the area search side, as well, where it was a homicide, and they had cut camera feeds. So we were pretty certain that they probably had their phones off, as well.

But they had a very identifiable vehicle, and we were are able to find that on an LPR the day before coming into the state of Indiana, and the day after, leaving the state at a different location on LPR. So we did a tower dump on all three locations. We also did an area search at all three locations. And actually, they didn't turn their phones off. But because we were able to compare and just look for common devices, we were able to find that common device in three locations.

So this is where I believe they're most conducive to a good outcome, is multiple locations. But you have to use your imagination at times. Maybe you know an ingress. Maybe you know the egress. There are things that can help us be successful. So educate yourselves and educate your investigators, or have them take some of the free webinars that are available through NW3C, and NCJTC.

And I'm probably going to skip this slide. But we're going to talk about United States versus Smith from the Fifth Circuit here in a minute. And although it applies to geofences, the way they wrote it could potentially be problematic for us. Area searches. This is the magic along with connected cars right now. But we have to understand how to accomplish it. So an area search is going to be that passive data, that timing arrival data from AT&T and T-Mobile.

So it's going to be a more specific data set that's accurate. But we're going to talk about where they derive that information to accomplish it. So we're just going to give them a radius around a crime scene with some parameters. T-Mobile will only let us go out a mile. AT&T will let us go 10 miles. It doesn't necessarily mean that's what we want to do, because we need to understand our environment.

So the big distinction between the two is, one, we have to give them a radius to go by. And two, this is data that's engineering data that happens in the network from your device, or from your car. And you can't control whether it's happened or not, but it's not a part of the call detail record. When I talk about using your imagination, as we go forward, we'll talk about daisy chaining. Maybe you know that your suspect traveled down a certain road. Can we design these radiuses to give you opportunity to have multiple locations for your area search, so that you're just looking for a common device?

The common device is the magic in the design. And obviously, we need separation by time and distance. So we do have to-- we need some separation, and I've tried to do this with homicides, or a double or triple homicide, where they've been pretty close together with no one's. And it's just tough if they're too close together because there's so much data, so many devices on the network, especially in a city, that it became not helpful.

So where does this data come from? How are they fulfilling this request on an area search? Well, I'm going to use this as an example, which is actually the crime scene that you'll see in the next photo. It's going to be pretty much on that azimuth, and that's my house. And I burned dinner. That was the crime scene, according to my queen. And that's not like it's the first time that's happened. But I'm going to talk about the cellular network here.

So there's the tower that's on the golf course by my house. This is the sector my house is on. I'm right on the azimuth, which is the midline. And then the timing of arrival arc, you can see that is a band, and it's a 78-meter band. So it's a 4G connection to my device, which I will-- my department device. I will get the records from Verizon so I can look at them every once in a while, just to help as practice scenarios for new investigators. Now, you're going to see-- actually, this is going to be my T-Mobile department phone.

Within that timing arrival arc, you'll see that black dot. Well that's the estimated latitude and longitude. That is the best guess of the network at where my device was. And the fugitive team would tell you that rarely do they find their bad guy where the estimated latitude and longitude is. And that's proprietary information from T-Mobile and AT&T. So that's also something they're not going to come testify to. And we need to understand that it's not exact. It's not a GPS location of where our actual device is. It's their best guess for engineering purposes.

So you will see where my estimated location is versus where my house is, and where I was, because I was there. So I know I was there, and my phone was there. And I looked at hours of data, and my estimated location was never over my house. My estimated location ranged from all the way up at that 116th Street, all the way down to me and the pond. And this was the most common one, and I don't know why. So the radius I picked in this case, knowing the density of towers in Fishers, Indiana, with 0.25 miles.

But when I looked at that data, I would have missed 33% of the estimated locations. So if I pick the wrong time, the wrong radius, I might not have seen my device at that area. I felt pretty good about 0.25 miles. And as I said, 70% of them were in that predefined area that I utilized. So that's how they're deriving the location to fulfill your request for an area search.

Now, sometimes TA is perfect when it supports our case, and why we think I've done tower dumps where in this case where T-Mobile gives me three towers, and that's what they've given me calls from, three towers. But then I do the area search, and in this one, we did a mile because we had some other good data. But you can see immediately that we had readings from six different towers that put that device at our crime scene.

Now, is it always going to work out like this? No, but that's the design of timing arrival is, we have the advantage that multiple towers can provide us information. And if we give them a 0.25 or a mile, or whatever, and we look at the density of the towers in the area, our likelihood of success is increased because we have data from multiple towers.

So how T-Mobile approaches an area search is they really don't want anything for more than a mile. Does that mean that you can't do that? It means it takes a phone call and maybe a relationship, so if you can't narrow it down more. Or they like only an hour. And if you can't do that, it's probably going to take a phone call. It doesn't mean they can't do it. It means it's going to cost you more, and they probably have to get a supervisor to say yes to it.

This data is retained for 30 days, so there we are. There's our shelf life for that timing of arrival data-- timing advance data. So keep that in mind. 30 days. So for now, we've talked about we have seven days of RTT from Verizon before it disappears. So preserve, preserve, preserve. T-Mobile, 30 days. Preserve, preserve, preserve. And then we're going to talk about AT&T, which why I would expect T-Mobile in this slide, I would expect T-Mobile to give me an estimated latitude longitude that is on my arc, because they're using timing arrival data and their proprietary system.

So it's pretty much always going to be on the arc. But with AT&T, they're using the location database of record. They're using historical mobile locates. They're using Timing Advance. They're using a lot of data. So it's not always going to be on that arc. The good news and bad news is they retain this data, the TA data for 13 months. Well, that is true.

And while that is true, it does diminish after seven days. I don't know how much it diminishes, but it does diminish. So it's another one that I would consider, depending on the case you're working, that maybe we want to preserve the area search data before the end of the seven days so we can get the absolute best data available. And as I beat this horse, Verizon seven days.

Pete, let me just throw something in there because the question came in about, would a VPN affect or corrupt this.

No, it wouldn't. You're still going to be connected to the tower, unless you are in airplane mode. Then if you're in airplane mode, and you're on a VPN somewhere, then I could see that being a problem, but that would probably get into more of your visionary stuff.

Yeah, the VPN is more the afterwards. You have to get to the internet first. And then once you're on the internet, you go from your internet connection to that VPN. So this is the pre.

Yes, and we have no control over what the networks are keeping. If your phone is communicating with the cellular network, then there is passive data that exists on that.

And if your phone is there, if your phone is being picked up by the towers, it is physically there. It is in that area. It is near it. It is not using a VPN. VPN would be different. It's not through cellular.

Yes. The short of it, it ain't going to affect it. But dealing with somebody who's using a VPN is a whole different set of presentations and complications to figure out where they are.

Yes. Then we get into push tokens and how that can help you with a VPN. And that's more of that stuff that we'll cover more at the Solving Crimes Through Emerging Technologies Conference. Did you like that?

Beat me to it, Pete. I was just going to do the plug myself. Yes, at that conference, that'll be covered.

So what I'll talk about at the conference is more actionable intelligence, specifically, as it applies to missing kid cases and exigency. If a child is missing for five years, and you get new information, is that exigent? Well, absolutely, that is exigent. But you have to have a plan and you have to understand what verbiage the providers, whether it's Facebook, Snapchat, Instagram, TikTok-- you got to understand what they're going to want you to say to them at that moment to accomplish that exigent.

But actionable intelligence applies to, in my mind, any case, whether it's a threat that we're dealing with, or just an investigation. But back to the area searches. We do have to be-- the problem that we're going to talk about with the Smith ruling is, we have to establish a good probable cause. We have to establish a process. We have to understand what the carrier's requirements are. And once again, NW3C has great templates. NCJTC teaches classes where we're talking about templates. Leads online in their toolbox has great templates.

So know the people around you that have great templates. A site that I go to is the K Loving group, where if I come across something new, I'll check there to see if they have the template. If not, I'll research it and just develop it myself.

Next poll question. Have you ever sent a preservation letter to a mobile carrier to prevent the deletion of data? Yes or no? All right. We have 61% said yes, and 39% said no.

And I need to get Kevin on here to talk. So I'm going to, once again, preserve, preserve, preserve. I've given you the shelf life of records. And oh, and here's another question for everybody.

The next poll question. Are you familiar with the legal implications of the United States versus Smith ruling on broad data collection warrants? Yes or no? 21% said yes, and 79% said no.

It's super important for us to pay attention to rulings and things that are coming down, and Supreme Court judgments on things, and notify our command, because they may be able to help push legislators to get the changes we need. We can't just sit back and watch.

Yes. For that 79%, the Fifth District, it was a Google geofence warrant. And the Fifth Circuit ruled that was a general warrant, and that's a violation of the Fourth Amendment. So it was too general in its request. And so that, although the ruling wasn't flipped out of good faith, but what happened later is there was a ruling in Mississippi district court that found that tower dumps were material indistinguishable from a geofence warrant. So they should apply the same standard.

And the problem is that in there, they likened it to, we're looking for a needle in a haystack that we decided to develop. And so we went from a big to a small. So we're trying to develop our own PC at the end of it. So there's some concern. I see the value in it. I see how we can get through this. But we have to write better warrants, we have to have better PC, and we have to establish what our process is going to be if we're trying to look for that single needle in the haystack. And why this is not the rule of the land, we need to be aware of it and keep our eyes on it, and make sure that we write better warrants as we go forward.

And I'm going to say that I believe it's the coffee that has caused me to talk more than I wanted to. And I like listening to Kevin talk, so I'm probably going to skip this last slide and get to Kevin.

So I'm going to briefly go into this and to remind you of some stuff. Pete said some stuff I'm going to go into that location is not always perfect. We can get a GPS coordinate that puts you at the middle of that circle, but remember, your target can be in the middle, it be on the edge. It can even be outside that circle slightly. It's not perfect. It is very good stuff.

Myself, I'm a fan of getting more than one source. If AT&T has location data on your, target and Snap has some, and Meta has some, I want all of it. And then you can really, really pinpoint it. But let's just be careful with that. IoT data stuff, information, electronic signals, it's everywhere. And because it's everywhere, because it's in almost everything we use, and in the future, it will be almost everything we use, you can't move without your signals being taken, maneuvered, pushed, pulled your phone collecting, their stuff collecting. Data is constant, constant, constantly going to be collected, and there's no end in sight.

So with that, we need to think differently about how we investigate things. I continue to listen to Pete all day, and I have listened to Pete present a whole bunch of times, and it's very precise, and his knowledge on cell towers and cell tower stuff changes, and I learn things each and every time from it. It's going to keep changing. The way data is collected is going to keep changing. Who has data is going to keep changing.

I have been in-- I'm retired from law enforcement, but I'm in the private sector, still working with law enforcement. I've spent the last 14 years running units that are in charge of finding people online, finding their presence, their locations, things they post, their location histories, all these wonderful things. And for the last 14 years, every year, every other year, I hear the sky is falling. We're not getting it. We're not getting it anymore. It's going to be encrypted. It's going to be hidden. It's going to be this. And yet we're still here and we're still getting data.

I'm going to ask my one poll question. Who here thinks Google does not have location data on end users? Geofences are over. Their public statement is, location data is now on everybody's phone. It is not being kept by them. But I'll ask everybody to raise their hand. Who thinks Google doesn't have it? And since nobody raised their hand, we're all on the same page. The data is there somewhere, but we have to be able to think differently, learn to ask more questions, do better research, spend some time on ChatGPT and other AI Search engines, and ask those questions.

Ask about location that Google collects on end users. Ask about what Amazon collects and Meta collects, and then start digging deep into it, and you'll see. Our crime scene goals, bad guys, witnesses, victims. We want to mention vehicles. We want to use some of the stuff to help us with time frames. There's a lot of things we want to do with crime scenes. But really, as investigators, our number one job is to, really simply put, find the truth. And in that, we need to find as much data to me as possible.

And I'll actually look at it from a different direction. Put yourself on the stand as a witness, and you did the cell stuff. You got that location data. The person's within-- I don't know-- 500 meters, 150 meters in a circle or whatever, or on the arc. And you're on that stand, and defense attorney comes to you and says, well, did you get any location data from Meta? Did the person have a Meta account? Did you get from Snap? Did they have a Snap account? And your answer is, yeah, they have those accounts, but no, I didn't ask. No, I didn't ask.

Well, Detective, isn't there a possibility that there's more location data that you don't know, that could either hurt or help my client? It puts us in a tough spot. There's a lot of tech. There's a lot of things out there, and it becomes complicated or cumbersome. It's hard to do it all, but just remember, there's more than one reason for doing it all, but it still comes down to that, let's find the truth.

Data sources in our crime scenes. Your victim is a data source, your witnesses, your suspect, the location, the cell towers. Everything is a data source for us. Data doesn't stop. Who's collecting? Everybody. Big tech, social media, businesses, advertisers. Advertisers are the real Wild West that not many of us at all in law enforcement really deal with. Anybody out there-- you could put it in the chat-- have you ever done legal process to an advertising company about somebody's location history?

How do they collect? It's through your device. Your Wi-Fi, your Bluetooth. We're going to go through each one of these things individually and some other things that there's tech in our phones we don't even realize is there that exists. This is something we'll talk more about at the conference. If I had more time today, I would bring it up. But we also got to think towards ourselves, and tracking, and protecting officer safety, and crime scenes. One, there are so many devices nowadays to track somebody.

Do we have a system in place to look for those devices? Do you have a witness who could have a tracking device in their car? Is there a patrol car out there with a tracking device? Is there a narcotics undercover who's got a tracking device in their car? When we go to crime scenes, how do we look for cameras. I'm doing this a long time. It's my eyes. How many cameras do you think you miss? And how many of those cameras are giving off a signal that we actually can use the device to look for, and measure, and find.

Just again, we got to start thinking differently. We got to start going forward. We're a reactive business. We need to get more in the proactive space. Your Wi-Fi, Wi-Fi networks, your smartphones, we all know it connects to Wi-Fi. But it does more than just connect to Wi-Fi. There's Wi-Fi connectivity that happens out there when you're not using your Wi-Fi. So the companies-- and this is just a few. In this presentation, I've thrown in Amazon and Meta. They're examples. Meta. It could be the weather app. It could be Snap. It could be any app under the sun. This is the policies and things they have and the ability they have to do.

Google has been collecting the SSIDs, the information on routers, forever, and they've been mapping this out. So you have a router in your house, routers in Starbucks, routers in different places. They know those routers. They know where they're located. They know the SSID number. That's that public facing name of the router, and they have the Mac address, the serial number for it. So your phone throughout the day, they will take your phone unbeknownst to you, send the signal to nearby routers, measure the speed in which it comes back, and locate you.

This happens all day. All the companies are doing it. You can research this. You can look it up yourself. I'll show you later on. I'll show you where it's in your phone to show you Apple's telling you they're doing it, but we don't pay attention to what they're actually doing. The example would be, if your phone sees Starbucks Wi-Fi, Google can know exactly where you are because that Starbucks Wi-Fi is near you. Nothing to do with your GPS, and you're not connected. This is not connected. Connected is even better, makes it a little stronger, but it exists out there.

Bluetooth and Bluetooth beacons. We all know our phone has Bluetooth. It's a lovely little thing so we can connect to things that are very, very close to us. Very close, so we can connect to those. We can work those things, my AirPods, whatever else. My mouse is on one. All those things are out there. But that Bluetooth also has other things. There are Bluetooth beacons. They're in stores. They're in businesses. They know the second you walk in the door. Facebook knows you walk in the door of a store. Your apps all know.

I walk into Target, that Bluetooth beacon that's in Target-- and there are lots of them in there-- will immediately let Facebook know I am in target. It'll also let them know where in target you are. If you stand in front of something for too long, if you stand in the section for computers, you're going to get ads for computers for the next 48 hours at least. You're going to get them on your home computer and everything like that. They measure, they keep, they're using your phone all day long.

Each one of these things, though, is a potential for us. This is something that has nothing to do with connection, but it's there. It exists. Now, do I know any investigator who's ever gone to Target and say, let me get the people who hit the Bluetooth beacon of your store last night at 4:00 AM? No. Does it mean we can't? Of course it doesn't. But in law enforcement, for us, it's always best to wait for the right case to push the envelope and try new things.

Cellular triangulation. Pete went through this. The companies use this, as well. Amazon, Meta, Google, all of them are using this data, as well, to help enrich your location. We'll go into deeper later on of what they're doing with that. GPS and GPS assisted, so an A-GPS. This is using your GPS from your satellites right, where you have to hit three satellites up in the sky. It measures where we are, trying this where we are. But in some locations, buildings, and mountains, and things get in the way, and it doesn't work perfect.

Lower Manhattan, big tall buildings, this, the old school one didn't work very well where it was just GPS. I remember years ago walking Lower Manhattan, using my phone and Apple Maps, and it kept making me walk in circles because it kept losing me. And it took me forever by following my little arrows of where to go. Today, that wouldn't happen because today, it uses the GPS plus, Wi-Fi plus cellular, plus other things to really understand where we are.

Google uses this. Apple uses it. Our apps are using this. They want precise location. And all of this comes down to not because they were just making sure you know where you are so you don't get lost in Lower Manhattan. It's advertising dollars. All of these companies, Apple to a lesser extent, but Google, their main source of income for this is ads based by location. It is why it will still-- they will still have location data, even though they tell you it's on your phone.

They're still collecting it. They still have to. They'll still have ads. Their stock prices haven't gone down. So we know they're still doing it. If Bluetooth is off, yes, it will still work. You'll still exist. There's no such thing as off for them. The best way to always look at your phone, it's not your phone. You lease it. You borrow it. You don't have the ability to every function in the core of that phone. It's not yours.

Ultra wideband. This is one of the newer ones that's in your phones. This is to help get more precise location data. This is how the AirTag-- after an AirTag, I put an AirTag in a piece of luggage, and it's the other side of the city. It has to hit a cell phone, some sort of Bluetooth. Once it hits that Bluetooth, the information from that AirTag makes it into the network, and the information can come to me. There has to be something connected to it. If you took my piece of luggage, and you put it in the woods, not near any device, it wouldn't show anymore. It's causing it to shut down.

In my house, though, when that thing's in my house, my AirTag, I can find it within inches. I will circle my house. The lines will help me walk me right through my house, boom, which draw it's in. That's ultra wideband. That is what is giving. It's giving that super signal to really get precise when I start to get closer to an item. So it is something else that is out there that is nearby. If you have one of the cars that your cell phone can start your car as you walk towards your car, it is hitting your car. Ultra wideband is hitting your car sending that messages. Your car knows that's Kevin's phone walking towards it.

These are texts that they're using for these small things, but it's going to be for bigger stuff. What we've seen over the course of time is they take Bluetooth, Wi-Fi, cellular, GPS, and they keep combining it to get a better, and better, and more precise picture of where you are. When you're walking around a mall, they want to know where you are at that moment. When you're in Home Depot, they want to know you've been standing near lawn mowers for six minutes, because that means you're interested in lawn mowers. And so they can send you a better ad, not just an ad to Home Depot, or an ad to Lowe's. You're going to get ads to the other stores, as well.

NFC short range. This is that Google Pay, Apple Pay, quick hits. Crowdsourced locations. This is using us, the people out there, to understand where things are. So if myself, Pete, and the 200 of us who are on this thing actually were in a room together, we'd all be hitting the same bluetooths, the same routers, the same everything. Google, Apple, and these companies would take that information, go, they're all hitting those same routers. Their GPS, all their coordinates are showing us where they're standing. So those routers are there. This information is there. That Bluetooth is there. They use this to help locate things.

How do we know? This is from my phone. Go into Location Services. Look this up right there. I put it up a little further. What are they collecting? We use GPS, Bluetooth, crowdsourced Wi-Fi hotspots, and cell towers to determine your location. They tell us they're doing it. Are we listening?

Here's the other end of this one. App and the ad stuff. So this is software development kits. This is the data that's sent back to the companies. What's the right term? Programs and data that's-- I'm a non-tech describing tech. So sometimes you'll have to forgive me. Those who are super techs out there, don't get offended when I screw something up with the right terminology. But I'll explain it.

In our apps, this is the technology that's out there that the STKs that exist in our apps. We have zero control over it, but they can use that to collect data for the purpose of ads location, the information you're doing, what you're searching. All of those things are done, and they're done by these companies even when you're not using the app, or if you don't even own it. Meta does this in a tor of apps, like the Weather app. They put their STKs in the Weather app.

You don't even have to have a Meta account, and they're collecting data on you. They're holding it for that future when they know they'll have you, or they can start selling it now. The companies are doing this. This information is out there. This is a direction I have not seen. Maybe one or two people in the Fed system I have seen go at this for very, very specific cases. But as our location stuff starts to disappear and Google gets better, the ad stuff is going to exist out there because they're putting it on our phones.

So there may be a path for us going forward. We need the right case going to have to start bringing Google engineers, Meta engineers into a grand jury and asking very, very specific questions. I give you the example. If I had to go back a little bit in time because it's been in the news a lot. The Idaho four case. That target, say you had him. You have him identified. He's got a phone. He's got a Google account. You go to Google. Google gives you no location data, but it shows his phone was on.

That would be the time I'd start to go to a grand jury, and I'd look for the right Google engineers, sending subpoenas, and bring them into a grand jury, asking the questions about, who did you sell the data to? What stuff do you keep for ads? Who does that ad and location data go to? It's there somewhere out there. But we need the right thing. Quick summation of all of that tech and who's using it. They're all using it. Where it's been the gray, they're using it limitedly there, or really what it is, they're just starting to use it and figuring out how to use it. They're all going to keep using this tech.

In our crime scenes, what I'd really like people to do is really just take a moment, and we have to start thinking, and we have to start forming groups, talking to each other, having some sidebar conversations of, OK, Kevin walked into Times Square, or Kevin walked into some rural section of Indiana. What did his phone collect, and who collected stuff from his phone? And the answer is going to be, there's a lot.

And even if I'm in the most rural of places in this country where there's very little collecting, well, there's probably only a couple of ingress-egresses to get in and out of that rural place. So maybe I don't take the rural place, but maybe I take the exit of the highway where I had to have gotten off, or the corner, intersection before that, where there's a store and there's information.

The information is going to be there, but we have to collect it better. We have to collect stuff that's in our crime scene. When I'm at somebody's house, I want their IP, their internet service provider. I want to know what their router information is, their router name. I like to take a picture of it. We have to start collecting this data differently. I hope I got that point across to everybody that this has to be done differently.

As many times as Pete and I, we've said it, and we laugh when we say about the Solving Crimes Emerging Technologies Conference, we're not paid. I'm not a paid spokesman. Pete's not a paid spokesman by them. We go there, and we believe in this. We've joined their committee. We present in this webinar because we believe in who goes to that event. That's where we go to learn. There's a lot of stuff we talked about here today. And again, I apologize for the speed of it.

It's important for us to keep pushing that envelope. It's important for investigators to find the time in their busy day to spend three days at a conference to get better at what we're doing, and for supervisors and bosses to send their people. Technology is not slowing down by any stretch of the imagination. And I am telling you, because I'm doing this a long time. I work with local, state, federal investigators from across the country. We're all behind. I don't care what agency you're from. We are all behind. It's just the nature of the beast.

But if we do a little bit more, if we talk to each other, collaborate more, go to these conferences, we can become better at this, and learn more and do what we're here for. Which I'll go back to one of my first slides. It's to find the truth.

Thank you, Kevin and Pete, for the excellent presentation today and sharing your insights and knowledge with us. To hear more on this topic, our presenters today will be part of our 2026 Solving Crimes Through Emerging Technologies Conference that will be held in Las Vegas, Nevada, January 13th through the 15th, 2026. Please join us at our conference to learn more. To view this conference and other current conference offerings, please visit ncjtc.org/conferences.

This concludes our webinar today. I'd like to thank Kevin and Pete once again for their time and insight on this important topic. If you are interested in additional training, please visit www.ncjtc.org for the listing of upcoming training opportunities, or view our on-demand online training. Thank you again for joining us, and we certainly hope you have a great day.