Just Forensics in the Digital Age

Introduction [00:00:01] RTI International's Justice practice area presents Justice Science.

Introduction [00:00:09] Welcome to Just Science, a podcast for justice professionals and anyone interested in learning more about forensic science, innovative technology, current research and actionable strategies to improve the criminal justice system. In Episode five of our Case Studies season Just Science sat down with Justin Schorr, principal Collision reconstruction engineer, and Tim Primrose, mobile forensic analyst at E.J.S. Associates, Inc., to discuss utilizing digital evidence in real world cases. In the digital age forensic technology has broad applications for investigations from cell phones, social media accounts and car infotainment system data to three dimensional modeling for crime scene reconstruction, technology is becoming a staple in forensics. Listen, as long as Dr. Schorr and Tim describe what kinds of digital evidence is applicable to investigations, the limitations and court considerations for forensic technology in case examples on how mobile forensics and reconstruction simulations were effectively used to further investigations. This episode is funded by the National Institute of Justice's Forensic Technology Center of Excellence. Some content in this podcast may be considered sensitive and emotional responses or may not be appropriate for younger audiences. Here's your host, Jaclynn Mckay.

Jaclynn McKay [00:01:19] Hello and welcome to Just Science. I'm your host, Jaclynn Mckay, with the Forensic Technology Center of Excellence, a program of the National Institute of Justice. On today's episode, we will discuss the utilization of digital evidence and forensic technology in real world cases. Here to guide us in our discussion is collision reconstruction engineer Dr. Justin Schorr and mobile forensic analyst Tim Primrose. Welcome, Justin and Tim, thank you for talking with us today.

Tim Primrose [00:01:48] Thank you for having us.

Introduction [00:01:49] You both work outside of traditional forensic laboratory and have very unique positions and backgrounds. I'd like to start with letting you both give the audience a brief overview of your backgrounds and expertise. Justin, would you like to go first?

Justin Schorr [00:02:02] So in terms of my background, I have bachelor's and master's and a Ph.D. all in civil engineering focused in transportation with the expressed intent the entire time of going into the field of being an expert witness. And essentially what I do is if a lawyer, an insurance company, sometimes a public defender, sometimes prosecutor has a collision where there's uncertainty about who was at fault or something with regard to the injuries. I get hired as the expert witness to reconstruct the crash, then go to court and testify as to how it happened.

Jaclynn McKay [00:02:36] Tim, could you give us a little bit about your background?

Tim Primrose [00:02:38] Sure. So I only have one degree. I do have a minor, though, so I have a bachelor's degree in digital forensics and a minor in information and technology management. However, I do have an abundance of certifications that I've got, thanks to D.J.S and Justin here, and I use those to collect data from cell phones as well as laptops, computers, GPS devices, all sorts of digital devices.

Justin Schorr [00:03:03] And, you know, I'm not saying about our country's education system at the moment, but I will say it is pretty cool that Tim was able to get a degree specialized in mobile forensics. I think that, you know, more trade school esque is probably the way to go. And certainly being able to get a degree in something so specific, it was really a no brainer that we wanted to bring him on board.

Jaclynn McKay [00:03:24] Yeah, for sure. Those types of programs are very rare. What school did you go to?

Tim Primrose [00:03:28] I went to Bloomsburg University. It's located in Pennsylvania.

Jaclynn McKay [00:03:31] You both have very unique backgrounds and you touched on this a little bit. But Justin, would you mind giving us a brief overview of how forensic technology is used in investigations?

Justin Schorr [00:03:40] Yeah, we're a little bit of a fish out of water at this conference. As I started our presentation yesterday, I mentioned to the audience that what we do doesn't fit directly into, I think what everybody else here does. There's definitely some crossover and definitely a lot of commonality. But our use of forensic technology is, first of all, more for the civil lawsuits rather than the criminal cases. I would say probably about 10% of my personal caseload is criminal cases. That represents about all well, besides the ones that Tim gets, that represents about all the criminal cases that come into our office. But our use of forensic technology began primarily with a wheel and ruler. And my grandfather out in the middle of the roadway that evolved into using survey equipment, total station, and then into laser scanners and now into drones. And primarily what we're doing is we're collecting physical evidence. Now that really doesn't make a difference if we're doing civil or criminal matters. Physical evidence is the lifeblood of what I do as an engineer. Collision reconstruction can be accurately defined as application of the laws of physics to the physical evidence. So without that foundation of the physical evidence is really nothing for us to do. And that becomes an issue in cases that are, you know, we get them three years after the crash happened and there's no photographs and the police didn't document anything at the scene because it was just a fender bender. But now somebody is claiming that, you know, they can't walk for the last six months and. All sorts of things that people can come up with. Sometimes accurately, a lot of times not accurately about, you know, what injuries they were getting from a crash. But these things that happened a while ago when there's no physical evidence, very difficult to reconstruct. So our use of forensic technology is always to collect and preserve the physical evidence. I mentioned scene evidence. We also do vehicle physical evidence. A lot of times that's the event data from a vehicle, whether it be the traditional quote unquote, black box data. Your airbag control module is where you get that data from, from tractor trailers, from the engine control module, from Bendix, data from telematics, and then now from infotainment systems, which if you have a touchscreen in your vehicle and you've paired your phone with that touchscreen, essentially everything you've ever done on your phone is now somewhere in your car. And guys like myself and Tim can go ahead and access that. Anything to add there, Tim?

Tim Primrose [00:06:02] Well, we do collect a lot of data from infotainment systems and there's just an abundance of cell phone data that's there, whether it's call logs, text messages, even the contact list. And essentially anything that you're doing on your phone while you're in the car driving.

Justin Schorr [00:06:16] How about from cell phones themselves?

Tim Primrose [00:06:17] Cell phones have way too much information. Pretty much everything that you do on a daily basis is tracked and logged, whether it's just a text that you're sending, a photo that you're taking, the location of where you are, or even the steps and distances that you're traveling.

Justin Schorr [00:06:30] One of the barricades actually, to getting that cell phone data, as we're learning, is the cost of the software that you need to actually download the data from the cell phone. One of the things that I've been thinking at this conference is that there needs to be some easier avenue to partnerships between ourselves and law enforcement so that we can kind of combined forces to get this software to download cell phones.

Jaclynn McKay [00:06:53] You guys are blowing my mind right now. Like, I don't even want to use my cell phone anymore.

Justin Schorr [00:06:57] Or when we do our presentation, one of the first things that people come to the conclusion is that if you're pair your phone with a rental vehicle.

Jaclynn McKay [00:07:04] I was just going to bring that.

Justin Schorr [00:07:06] Literally insane. I mean, unless this thing is involved in a fire. What we did when we wanted to practice doing the infotainment system downloads is that we went on eBay and we bought a bunch of infotainment systems that were in rental vehicles that were either retired or had been in the crash. And then the junkyards after junk in the vehicle sold the infotainment system on the Internet. So we went and bought these infotainment systems and we were getting ten or 15 different people, cell phones, tons of information from their cell phone downloaded just from that infotainment system. So always make the joke, you know, six degrees of Kevin Bacon while we had this contact card for this gentleman named Chad. And it's got his picture, it's got all of this information and this contact card was not even on Chad's phone that was paired with the vehicles on somebody else's phone that he knew. So Chad's contact card is in their phone. They pair their cell phone with the rental vehicle, the rental vehicles involved in a crash. The junkyard sells the rental vehicle, sells the infotainment system. We buy the infotainment system. We do the download. We have Chad's contact card and picture on our computer.

Jaclynn McKay [00:08:06] Wow. Yeah. So when you say pair a cell phone with a vehicle, are we talking like Apple CarPlay or are we just talking Bluetooth connection?

Justin Schorr [00:08:15] Well, the fastest way is if you use that plug, that USB.

Jaclynn McKay [00:08:19] Yeah.

Justin Schorr [00:08:19] That's asking for trouble right there. But Bluetooth and Apple CarPlay. Well, both the vehicle when it's asking you for all those permissions it does download of all that information on to the vehicle like one of the permissions is like your calendar in most vehicles and say why does it need your calendar access but it's just downloading everywhere, all your appointments, everything that's on your calendar, it's downloading it straight to the vehicle storage.

Jaclynn McKay [00:08:41] That's pretty scary.

Justin Schorr [00:08:42] Yeah, it's terrifying.

Tim Primrose [00:08:45] And I did something similar when I first started. I'd just gotten a few certifications, just had my degree, and I wanted to get some practice downloading phones. So we went on eBay, ordered, I think like 100 phones for 40 bucks. They were all broken or used for parts and I was able to repair some, get data from some. And there was so much information in people's Social Security numbers, all their contacts, all their pictures, deleted pictures, videos, even some phones that they thought were locked and they were maybe trying to sell to make a couple extra bucks, we were able to get all their information, all their data, everything they've done, their browsing history, you know, their Internet history, what they were searching.

Jaclynn McKay [00:09:18] How can we completely wipe phones? Like, does the factory reset actually work?

Tim Primrose [00:09:24] So when data is deleted, sent to what's called unallocated space, and this is a certain area within the hexadecimal data of the phone where a deleted data is stored.

Justin Schorr [00:09:34] So real quick, I think the easiest way to think about unallocated space is that when you click on a file on your computer, if you're using a Windows computer, you have that file path. What that's essentially doing is it's telling the computer how to get to this file. When you delete something, all it really does is it deletes that path and the computer forgets how to find that file. So it just goes into this this nothingness that we call unallocated space.

Tim Primrose [00:09:58] And so essentially the data just resides there, depending on the type of phone and depending on the type of data for sometimes an unlimited amount of time or just until you know, more data. Is deleted and there has to be more room created within unallocated space for that newly deleted data. Because even though it's unallocated, there's still an allocated amount of space for incoming deleted data.

Justin Schorr [00:10:20] So the only way to get rid of something on a device.

Jaclynn McKay [00:10:24] Was just smash it with a sledgehammer.

Justin Schorr [00:10:26] There's two ways. One is fire. The other way to get rid of data is what's called a secure wipe. So this is something that actually hackers tend to do when they ransomware people where they'll download all of your data and then they'll secure wipe your drive. So what that does is it essentially just sends every single one and zero resets them all to zero. Essentially gets rid of all the ones that are defining what the files are. I'm not sure how you actually secure wipe a device.

Tim Primrose [00:10:56] I mean, there's there's ways to check that. And that's where we get into some of the spoliation scenarios where we see that something has been deleted or I get a cell phone and I know that the person has had the cell phone since 2021, and I'm downloading their phone now and 2023, and there's like seven phone calls and a handful of pictures from the last two months. There's something fishy there. So that's where we want to look and see if there's any evidence, any breadcrumbs left over that this phone was factory reset or deleted. We might not get that data back. There are times that we can. That's typically through like a back up or we access the cloud and we can still try to find other avenues to find that data.

Justin Schorr [00:11:33] Sometimes there's fragments. If you've paired your phone with a vehicle, that is a way that we can actually access data that you've deleted from your phone because sometimes that will still be on the vehicle. And people think that if they delete their device from the device list of a rental vehicle, that that gets rid it doesn't get rid of anything other than the pairing of your your phone in the vehicle.

Jaclynn McKay [00:11:53] So I think that's a really good point, because that's valid for law enforcement to know, too, because if they can't find an individual's phone, okay, well, maybe we could get a search warrant for the car and see if any of that data is still there. And that's another option.

Justin Schorr [00:12:07] Absolutely. And the only hindrance to that is that the acquisition of infotainment data is a new field. So it's literally daily, weekly that we're getting updates that say, you know, we can now get this data from these vehicles or, you know, these vehicles are now added to the list that you can download from all the data is there. It's just a question of accessing rental vehicles. The great example for this, because the person that has to sign consent for you to do a download of the vehicle is the owner of the vehicle. If it's a rental vehicle, you don't own the vehicle. So your data is now on a vehicle that you don't own, that somebody else has the gatekeeper control over whether or not, you know, the data is accessible, should it be in a crash or something along those lines.

Jaclynn McKay [00:12:50] So you said that downloading this infotainment data is kind of new and upcoming. Can you talk to me a little bit more about what you need in order to do this and who all is allowed to do it and.

Justin Schorr [00:13:02] Why you need to pay this company, Burleigh, to go down to their training and then buy their kit and then buy their software. And to be fair to them, they're the ones that, you know, have spent the time to, quote unquote, hack into the cars and figure out how the data stored and how to access it.

Tim Primrose [00:13:17] Do you use social media that's tracking everything that you're doing on any platform and it's stored indefinitely. You can go on and request your own data file as well, and you can see what other people will be able to get if they were to submit a subpoena or even hack your account. And you can get all this information extremely quickly. If you were to go in through your settings, go on Facebook, Instagram, TikTok, even Spotify, you can go in and request all of your information. And I'm not even kidding. Within 30 seconds you will get an email with a data file of every single thing you've ever done. Between every like that, you've made every comment from requests, denied requests. Every time you've logged in, what type of phone you logged in with, or device, even like a computer. Sometimes where you are, your IP address, all of your information, everything you've commented on, everything you've posted, everything you've been tagged. And when it comes to tik tok, it'll show you every post that you've watched and for how long.

Justin Schorr [00:14:14] And there's a scarier element to this that I don't think that people pick up on immediately. And that's that there's so much more information on each one of these data entries than you realize. So it's not just the fact that you watch this post for this long, but all of the metadata where you were, the device, like Tim said that you used to log in, that information is also stored with those entries. So you're not only getting kind of your activity, but there's a little bit of a story behind your activity that you're getting with that as well.

Jaclynn McKay [00:14:48] And so even if you quote unquote, delete your account or deactivate your account, all that information is still there.

Tim Primrose [00:14:56] Yeah, they have servers with all of your data. And I mean, they can say that they get rid of it. Do we really know that?

Jaclynn McKay [00:15:01] So while we're on the topic of getting information from phones and social media, when you do a quote unquote phone dumb. What type of information are you getting from it in a forensic standpoint.

Tim Primrose [00:15:14] From the physical phone itself? There's a few ways that we can collect data, and that sometimes affects what information we're going to collect. So there's what's called a logical acquisition, and that's going to allow us to collect all of the data that you would be able to see if you were to go through your phone, look at your text messages, look your photos, all those kinds of things, but you're going to get a little bit more information. So we'll be able to see, for instance, the time that you actually read a text message versus when you received it. So let's say there's a situation where police picked up someone's phone and they're physically going through their phone. We call that thumb forensics and they're potentially opening messages, maybe accidentally deleting things. We can see when they actually open that message so that if we know if there was a car crash, we want to see if someone opened a message and was maybe texting while they were driving, we can say, well, this message was opened after the crash. They received it maybe leading up to it. We know there's notification that came in that may have distracted them, but they didn't actually open the text message, actively use the application. And that's some of the information that we get when we're physically downloading the phone. There's a few more steps that we can take when collecting data. There's a file system acquisition that allows us to see some of the application usage when apps are actually open. Even things like a flashlight app. And then we move up to a physical acquisition. And this is what allows us to reach that unallocated space that we talked about before getting some of that deleted data. And there's just so much that's available in terms of the cloud. You know, we can do that essentially anywhere. We just need their log in information. And from there, there's usually like a two factor authentication. They'll send them a code. We always need their consent unless there's a subpoena involved, but we need their cooperation. And once they're able to revise that code, we can collect all their back ups, whether it's from their phone or their computer, and we can access all that information. And we're going to see a lot of the same information that we would see from the phone. And that's where it's nice. If the phone is damaged, someone sets it on fire. We can still get that information and other methods.

Jaclynn McKay [00:17:11] So you guys have already talked about all the ways people use their devices. And with the age of social media, how long does this take to actually get all this information from the phone and get something useful out of what the data is telling you? Like, this seems like it's just takes days.

Tim Primrose [00:17:28] Well, as I mentioned with social media, it takes seconds to get that data file. And I mean, that's a lot of just text based files. So they're small. It is easy to provide that information. But when we're collecting data from a phone, it really depends on how much data is on the phone and typically how many pictures are on the phone. And in today's digital age, people have thousands, tens of thousands of photos. It's not just a disposable camera and it takes a long time to collect all that information. And unfortunately, in a lot of cases, when we're collecting data from a phone, we want to collect as much as we can. And in order to do that, we're going to collect all of the data from the

phone. From there we're going to filter it down and look at what's relevant or redact personal information if it's not relevant, just always worrying about the user's privacy.

Justin Schorr [00:18:08] And so when Tim does a cell phone download, there are some kind of barriers that we should put on what he's actually doing. So that the first thing to know is that if it comes across Tim's desk, when Tim gets his directive, which most of the time it's going to be subpoena based. And in this subpoena, it's going to define the time period over which the download is permitted. So what Tim has to acquire all of the data, there's only a select time period that he's quote unquote allowed to be looking at or to analyze. And I think a good question, Tim, is how long does it take to parse that data? So I know that acquiring the photographs, especially from some from somebody's phone, it can take a while to do the download. But let's say you got everything downloaded. How long does it take for you to parse you know, a day's worth of data on somebody's phone.

Tim Primrose [00:18:58] So once I've acquired the data, it does take some time to parse that information, all that data. And once I can get into the data file and start digging and doing my analysis, there are a lot of filters and functions within the software that we use that make it easy to narrow in on what we're looking for. So now I have to validate all the information that the software is telling me. You know, they'll say this is the time that this photo was taken. And for example, there was a phone that I downloaded. It was my own phone from when I was in sixth grade. And there's a picture of me at the orthodontist with my braces on, and there's a timestamp on there that says it's taken at 116 in the morning and in sixth grade, that's past my bedtime. I know that I'm out of the orthodontist, that one in the morning. So that's like the next step is validating that timestamp. So now I see that the time zone is incorrect for the East Coast. It's UTC minus five during that month time frame because of daylight savings. And so it changes it to 8:16 p.m. and that's still a little late to be at the orthodontist. That's where I now dig a little bit deeper, look at the hexadecimal data and I see that the true timestamp is 1500 hours, which is military time for 3 p.m. and from there. I now have to say, okay, well, where did this other timestamp come from of 816? And that's when that photo was sent as an attachment and a text message. So there is someone else out there that has some blackmail on me.

Jaclynn McKay [00:20:18] Is this a good time to bring up spoliation?

Justin Schorr [00:20:21] So spoliation is essentially when somebody destroys evidence, does something that that essentially they're trying to hide some information from the other side. Spoliation might actually only be a term of art for civil cases. I'm sure there's there's a criminal word that means the same thing in the tampering or something along those lines. But spoliation is like, say, a trucking company has a tractor that's involved in a crash and they know it was their fault and they had dashcam and they go and they destroy the dashcam video so that the other side can't get it. Well, then they're going to have serious spoliation issues when the other side says, Hey, where the hell is dash cam? We know you destroyed it. And obviously that's not going to look very good in front of a jury.

Jaclynn McKay [00:21:04] Tim, you did a great job telling us about your workflow. Can you maybe talk about a case example in which you utilize these methods?

Tim Primrose [00:21:11] It was actually my first case, and unfortunately it was child pornography based. I'd just finished all my training and I've been just for a few months. I was all excited to jump in on my first case, download a phone, collect some data and do my job. And the first call I got was from an attorney who had received phone downloads from a ten year old girl and an adult male, and they wanted to see if this guy was one of, I

think, about five different adult males that were messaging this ten year old girl. She had been sending photos and videos to them at their request. There was a lot of messages that I can't unread things that these adults were saying to this child who didn't know what she was doing. And luckily the mother had found her phone and found everything that she was doing and turned it over to police for them to conduct their investigation. And they had made an arrest on this guy. He was then released and he sued the state for wrongful imprisonment. And that's where they wanted me to investigate what the police had done and see if there was a basis for their conclusions. So they handed me 2000 plus page reports and they were like, there's just so much information here. We can't get through everything. It's full phone dumps from from both the ten year old's phone and this guy's phone. Can you condense this down to like four or five pages and give us something that we can actually look at and make a basis on? So I started digging through. I was able to cut out a lot. Initially there was stuff that was outside of the timeframe, but ultimately the most important thing was that the guy had so much information on his phone of affairs that he was having with his wife. I think he had over 20 different women that he was meeting with casually, and that really didn't help his case. He was using all sorts of dating profiles, online dating chat rooms, and he was always communicating with different women. Now, through my analysis of what I was finding, most of these women were in their forties, some of them in their thirties, but there weren't any that were even in their twenties. There was no one that was young and this guy was in his early thirties. The one thing that I found on the ten year old's phone was a contact for this guy that had his phone number. It had his first name, not his last name. And the one thing we still weren't able to determine was how she got his phone number and when she saved it in her phone. It was shortly after that that she called him. She made a face time call. And that was the only record of communication that we could find at first. As I said, this was 16,000 pages worth of information and at one point pretty much done my report. I pretty much had everything that I thought I could find in terms of his online Internet activity, people he was messaging and that he really had messaged her. There was just this one FaceTime call that lasted for three and a half minutes when I came across a couple of screenshots that the ten year old took and it was a FaceTime call. And in the first image you could see the adult male that I had his phone. You could clearly see his face and in the face time window, it was just a little black little square so you couldn't see anything. And in the next image you could see the ten year old's face in the face time window. You could clearly see that she's underage and the adult male was exposing himself. And that was pretty much all that we needed to see. That's okay. You know, he was involved. He wasn't one set of big fish that they were looking for. There were people that were messaging her on her phone that were really requesting a lot of things and saying a lot of things, and that she was sending things, too. But this guy, his story was that he was messaging some girl on a platform that he had met with prior and spoken with prior and thought that that's who was FaceTiming him. And so, I mean, the attorneys took it from there, and that was their job to determine those next steps. But I was able to find those screenshots of the face time, cause.

Jaclynn McKay [00:25:01] I'm sure that felt like finding a needle in a haystack.

Tim Primrose [00:25:04] It did. And luckily, I mean, because I had her phone, there were a lot of photos. Videos that were of her. But thankfully, since the police had already done the initial investigation, they redacted all those photos. They just missed the one of the guy. So was this traumatizing as they would have been?

Jaclynn McKay [00:25:19] Yeah, that's good. Justin, you brought up the fact that you reconstruct traffic accidents. Can you talk to us a little bit about that?

Justin Schorr [00:25:26] Absolutely. This is my favorite thing in the world to talk about. So collision reconstruction is the application of the laws of physics to the physical evidence. And what you're trying to do by applying the laws of physics is you're trying to establish what the dynamic elements of a crash were. So anything that involves any sort of movement, how the vehicles move from impact to rest, how they got to the point of impact, the angle of impact, the speeds at the point of impact, all of those elements you're attempting to, based on the physical evidence, come up with a reasonable range of values for. So one of the places that people go awry in my field is that they try to be way too specific with what they're doing. So you have to keep in mind, I know this is something that anybody listening will remember from chemistry class in 10th grade, but significant figure. So when you had to deal with your sig figs, when you had you had one measurement that was only to one decimal point, all of your other answers could only then be to one decimal point. Well, we're dealing in a world that is not to a decimal point. And really, if you're you're talking about how accurate we can be with with what we're doing, it's probably two a mile an hour or two miles an hour or maybe even five miles an hour. And you have to be reasonable within what you're saying, because certainly if you're too specific, somebody like me is going to go in and they're going to pick apart everything that you did and show how, you know, you're not even close to a good answer there because you really tried to get too cute with what you do. But after we've defined all of those dynamic elements, that point of impact, the angle of impact, how the vehicles got there, the key for us in our field is not really knowing the nuts and bolts science behind that because that that science is already done. It's how do we display this? How do we show this to, again, a jury or to our client or to whomever the consumer is for who we're doing the reconstruction for? So one of the ways that that we like to do that is through 3D animations. And this has been a staple in what we do at DJS for close to 20 years now. My father was very, very good, although he didn't always use technology the best, he was certainly good about equipping his people with the best technology and kind of trying to be on the forefront of all of these things. So we were the first company in Pennsylvania. It was us in PennDOT that had the laser scanner for the longest time. Then we moved to the drone before anybody else moved to the drone. One of the things that we got real good at first was our animations. And while it shouldn't make a difference to a jury the quality of what they're looking at and you got an animation that looks like real life like ours do, it's going to make a tremendous impact on a jury. And so we've actually had situations where one company will do the reconstruction and they'll hire somebody to do their animation. But because it's not their engineers that are doing the animation, the animation doesn't accurately reflect what's in this person's report. And you have serious problems if you're going to turn something in to a court that the visual is different than what's written there, especially when it's different than the actual engineering. Because one of the major issues with taking things to court and with animations in court and with technology in court is actually the judge is the gatekeeper deciding what's being allowed to be shown to the jury. So your animations, we call them engineering animations, have to be accurate based on the laws of physics. So when you have two different people, one company doing the reconstruction, one doing the animation, we've seen recently a situation where that animation is not reflecting that underlying reconstruction and becomes completely useless.

Jaclynn McKay [00:29:14] When I testify, they always ask me, does a photo fairly and accurately represent a scene? Does that ever come up with the animations that you guys are bringing in the court? I know you said you do majority civil cases, but does that apply to your animations as well?

Justin Schorr [00:29:31] Absolutely. And a lot of times that's something that gets adjudicated before we ever stepped foot in the courtroom recently, we've had to go to to

that adjudication where the judge was deciding whether or not to grant in this case plaintiff's motion to exclude our animation based on the fact that in this case it was because the environment had changed. So this settled. So I can talk about it. So this was one where an individual is crossing and there's a bus terminal to his right, and it's a very odd intersection. It's in a city. So there's there's this brick walkway between. Two sides of the road. And I mean, it's a brick roadway, but anybody that seen brick instead of traditional asphalt, that is almost universally for a pedestrian crossing. So it's not unreasonable that a pedestrian be crossing here, but it's also at the exit of a bus facility. So as the bus drivers coming out, the question was, could she see him to his right? And it was one of those freak cases where it just so happened that this guy was hidden by the window pane of the bus the entire time. And we had video from multiple angles. And one of the main things that we do now is video tracking so we can accurately track the motion of an object through essentially any video as long as we're able to go out and capture the 3D data that represents the environment. And to get to your question. Here was a case where the 3D data of the environment was substantially similar in the sense that we could use it to do our analysis. But they had put up some bollards. They put up a chain that they'd taken subsequent remedial actions to prevent pedestrians from walking across this roadway at this location. They want them to go to the corners, which this guy should have done to begin with. But, you know, obviously nobody was going to blame him given the fact that there was nothing preventing him from walking across when he did. But I can't really think of a time where we haven't gotten it accepted because what we're able to show is that all of the relevant parts of the environment were still the exact same as they had been at the time of the crash. But the place where you might run into that is lighting sometimes with nighttime crashes because it's very, very difficult to accurately recreate the lighting at the time of any nighttime crash. The way that that's going to be kind of sussed out is through virtual reality. And that's something that we're starting to get into where we've done a few exhibits. We were about to be the first ones to get it accepted in a court in Pennsylvania, and the case settled two days before trial that that crushed me. But we have another case that's coming down the pipeline right now where we've done it again, and hopefully this one will actually go to trial because it will be a momentous occasion to get virtual reality accepted. Because if you want an accurate representation of the environment, that's the only way you're truly going to get it, is to put on the goggles and be there yourself.

Jaclynn McKay [00:32:19] So we're going to link one of your animations on our FTCOE landing page for this podcast episode. But can you provide us with a little bit of background of what that case was about?

Justin Schorr [00:32:31] Yeah, that that case is up in Ulster County, New York, for a plaintiff's attorney named Joe O'Connor, where we were hired by Mr. O'Connor to go up there and collect data from the environment. We had video from a ATM that showed the crash and we did a full analysis on this video. So one of the things that you find out when you're doing a lot of video analysis is that every camera has a fisheye to it, whether it be severe or kind of almost unnoticeable. So the first thing that our guy Lawrence does, who does our video analysis and what the ATM video like kind of boils down to is it's just like a little sliver. And in the sliver, you can see the motorcycle coming from the left and you can see the bus making the turn. Now, this motorcycle was going at a very, very high rate of speed. We also had video from another bus that this motorcycle had passed as it approached the area of the crash. And it was doing upwards of 100 miles an hour. When it passes this other bus, by the time it gets down to the the area where the crash occurs, the motorcycle is still going at a very high rate of speed and the bus pulls out and the crash occurs. Now, what we noticed in the video is that right before the bus pulls out, there are

two red vehicles that are going the opposite direction of the motorcycle that the bus seems to follow. So our theory was that the bus driver does not look to his left at any point relevant, but that he's following these two red vehicles. Once the red vehicles pass from his right, he he had looked to his left prior and he says, oh, I can just go and pulls right out. Luckily, that is what he testified to during his deposition, because without that testimony, you know, we would have still had that theory and I think we still would have been successful, but it would have certainly been a tougher sled for the gentleman that was was on the motorcycle, the motorcycle operator, even though he was exceeding the speed limit. It just so happened that at the moment the bus pulled out, which it did, again, irrespective of where that guy was, because the guy wasn't looking to his left, it just so happened that where the motorcycle was at the moment the bus pulled out, even if the motorcycle been going speed limit, the crash would have still occurred. Now, this is not to say that the motorcycle operator was driving his motorcycle in a safe way, you know, going at that high rate of speed. But at the end of the day, my job is not to make that sort of an evaluation. My job is to objectively do my analysis so that I can provide an objective answer to any question that somebody wants to ask about the crash.

Jaclynn McKay [00:35:02] Yeah, that's the same with crime scene reconstruction and bloodstain pattern analysis. It's you give us a question and we objectively provide you with an answer. So we've talked about video and we've talked about cell phones. So can you guys give us some tips and tricks on how to properly collect these things?

Justin Schorr [00:35:19] Look for every avenue that you can to acquire data. This is everything from, you know, finding every electronic device to going out and asking, you know, every gas station that's along someones path of travel. Hey, do you have video of this day and time.

Jaclynn McKay [00:35:34] And specifically with video? Right. You want to try to get that as soon as possible because a lot of places wipe the video after so many hours.

Justin Schorr [00:35:43] You know, it might be on a 30 day loop. It might be on a 24 hour loop. It might be on an hourly. You know, you never know.

Tim Primrose [00:35:49] And another great way to when you're starting off with a device that you've never looked at before. I mean, research is really important. You want to make sure that, you know, for me as an expert, I'm an expert in not only collecting data and analyzing data, but also doing it in a forensically sound manner and also knowing and understanding where to look for the right resources in terms of getting a manual or, you know, there's there's different kinds of devices that I'm not doing every day. You know, I'm mostly doing cell phones or GPS devices, but there's times where we get some type of wearable device that's different than like an Apple Watch or a Fitbit, something that I'm used to collecting data from when it's linked to a phone. You know, there's times where we have a bicyclist who has some type of bike computer, and that's not something that is an average daily use item that we're collecting data from. It's only if a bicyclist is hit by a bus or a truck or something along those lines. And so trying to figure out how to collect data from that bike computer is not something that I necessarily went to school for. But my knowledge and understanding of different digital devices has allowed me to know how to properly research the best method to collect data from that device, whether it's linking it to, you know, a cell phone and collecting data that way, or maybe doing a chip off and collecting data from the chip. There's different methods and it's just having that understanding of what you're dealing with and how to deal with it without, you know, deleting any information or changing any data as well.

Jaclynn McKay [00:37:12] Yeah, that makes a lot of sense.

Justin Schorr [00:37:13] How to get the data with doing the chip off is the very last option.

Tim Primrose [00:37:17] Yeah, that's that's the last thing we want to do. We want to try to repair the phone if we can, because chip off is destructive. You're removing the data chip that the information stored on. And we've had cases where someone, you know, stepped on a thumb drive and they thought that they'd got rid of the information, that it's not accessible. And now we can communicate with that board, the logic board that the chip stored on. We can do some soldering wire it to another USB cable to plug it into a computer to collect data from it. And if we're not able to do that for whatever reason, that's when we're going to go to that chip off. There's few things we want to try before doing that.

Jaclynn McKay [00:37:48] Well, Tim and Justin, thank you both for your time. It has been a pleasure discussing this topic with you today.

Justin Schorr [00:37:53] Thank you.

Tim Primrose [00:37:54] Thanks for having us.

Jaclynn McKay [00:37:55] If you enjoyed today's episode, be sure to like and follow just science on your platform of choice. For more information on today's topic and resources in the forensics field, visit Forensic COE dot org. I'm Jaclynn Mckay and this has been another episode of Just Science.

Introduction [00:38:13] Next week, Just Science sits down with Dr. Richard Goyder Bhajji to discuss using facial recognition technology and two high profile investigations. Opinions are points of views expressed in this podcast represent a consensus of the authors and do not necessarily represent the official position or policies of its funding.