Hello Folks and welcome back to the Good Judge-Ment podcast. I am Wade Padgett.

*And I am Tain Kell. We really appreciate you listening to the Good Judge-Ment Podcast.*

Tain, everyone who listens knows that we like to mix things up on the podcast.

*That’s right. There are times when we are the ones who are mixed up, also*.

Well putting that aside for a moment, this episode will present a mixture of subtopics or areas of the law within the larger topic of 4th Amendment law. Tell the folks what we are discussing today, Tain.

*Today we are discussing 4th Amendment Issues associated with search and seizure of technology – with a little evidence law mixed in for good measure.*

Shout out to my awesome summer intern, Mr. J.B. Bryant, for his help is conducting some of the research for this episode.

Not a day goes by when courtrooms across the country deal with technology in the courtroom,

Sometimes, we are asked to read over Twitter exchanges between spouses when deciding a custody issue – or asked to sign a search warrant or consider a motion to suppress relating to electronic data

As the technology has evolved, the law has struggled to keep pace. Always interesting to see how a document such as our constitution, which was created prior to electricity, the internet, the computer and the motor vehicle applies to modern realities like Facebook, Twitter and similar social media

**SEARCHES OF CELL PHONES AND RELATED DATA**

Landmark US Supreme Court Case *Riley v. California,* 573 US 373 (2014) - Held that the government may not conduct a warrantless search of the contents of a cell phone that is seized incident to an arrest absent exigent circumstances, under the Fourth Amendment.

Landmark US Supreme Court Case *Carpenter v. United States,* 138 S. Ct. 2206 (2018)*:* Concluded that the government’s acquisition from wireless carriers of defendant’s historical CSLI (cell site tracking) data was a search under the Fourth Amendment. More specifically, the narrow holding was that accessing seven days of historical CSLI constitutes a Fourth Amendment search. Supreme Court held that a warrant is necessary to obtain CSLI in the absence of an exception such as exigent circumstances.

Many of these US Supreme Court cases, as well as cases from the Georgia appellate courts, have performed the analysis of cell phones and related data under the traditional search and seizure rules involving searches of "containers”

The idea being that a cell phone is really a container of electronic data – example: your phone may be seized pursuant to a search incident to arrest. But if LE wants to see what is inside of that container (a/k/a cell phone), that is a separate search. And that search of the contents of the cell phone requires a search warrant.

We will discuss some of the hearsay implications of seizure of cell phones in a few minutes – but consider this scenario:

Defendant arrested and even while the screen is locked, the messages he/she is receiving are displayed on the home screen of the cell phone. If the LE officer has legal possession of the phone, can the officer read the messages? Could the officer take a picture of the defendant’s cell phone which is displaying the messages on the locked home screen to use during the trial?

It is easy to get lost in a rabbit hole when considering search and seizure issues – so start with an analysis of when one search ends and another begins – particularly when looking at electronic information

Assuming the cell phone was legitimately seized pursuant to an arrest, the officer is allowed to look at the thing seized. If the defendant has set his/her cell phone settings to show incoming messages in their entirety while the phone is locked, the officer is allowed to look at those messages. (really no different that examining the exterior of a gun or a bag of drugs). And if the LE officer can look at phone, the officer can take a picture of what is seen. This is much more akin to a plain view “search” which does not require a search warrant

**AIRBAG CONTOL MODULE (“ACM”)**

Most new cars have a device that is more commonly referred to as a car’s “black box”

It records things such as the car’s speed, application of brakes, etc. just before the airbags were deployed.

More officially, these devices are referred to as ACM’s

*Mobley v. State,* 307 Ga. 59 (2019): Defendant was convicted of vehicular homicide after denial of motion to suppress data retrieved from airbag control module (ACM) in his automobile at scene of collision. Officer retrieved data from the airbag control module at the scene of the crash by entering the passenger compartment and attaching a crash data retrieval (CDR) device to the data port in the car and used the CDR to download the data from the ACM. The next day a warrant was applied to remove the ACM from the vehicle.

Court did not answer the question of whether there was a reasonable expectation of privacy in the ACM data but held that the entering of the vehicle and connecting a CDR device to retrieve the data was a physical intrusion into an “effect” of the defendant and the retrieval of the data without a warrant at the scene of the crash was a search and seizure regardless of a reasonable expectation of privacy.

Further, the Court did state the retrieval of this data might implicate the Fourth Amendment if the ACM included data shared from other on boarding devices such as GPS and cell phone information.

**TIME LAPSED TO SECURE A WARRANT**

*State v. Rosenbaum,* 305 Ga. 442 (2019): Defendants were arrested for death of foster child and alleged physical abuse of their second foster child. At the time of the arrest the police seized their I-phones, I-pad, and MacBook laptop without a warrant. Police obtained seven search warrants for the electronic devices, but the first warrants were not issued until 539 days after the devices were seized and the last warrants were issued 702 days after the seizure.

The trial court granted a motion to suppress the evidence found on the electronic devices because the delay in this case was unreasonable and violated defendants’ Fourth Amendment rights, the trial court also rejected the State’s argument that evidence obtained pursuant to the warrants was admissible under the good-faith exception recognized in *United States v. Leon*.

Court used the Eleventh Circuit’s analytical framework to work through the question of unreasonable delay in obtaining a search warrant: “Even a seizure based on probable cause is unconstitutional if the police act with unreasonable delay in securing a warrant. The reasonableness of the delay is determined in light of all the facts and circumstances, and on a case-by-case basis. The reasonableness determination will reflect a careful balancing of governmental and private interests.”

Eleventh Circuit framework for balancing governmental and private interests under the “totality of the circumstances”:

1. The significance of the interference with the person’s possessory interest;
2. The duration of the delay;
3. Whether or not the person consented to the seizure;
4. The government’s legitimate interest in holding the property as evidence.

Trial court concluded: “There was a significant interference with the Defendants’ possessory interests in their property over the course of the 539-day delay it took for the State to begin to examine it. This delay did not result from the complexities of the case nor any overriding circumstances, but from oversights that caused the State not to pursue their investigation into the contents of the devices with sufficient diligence. While the State’s interest in holding Defendants; property as evidence is very high, this Court finds that there was an unreasonable delay between the seizure of their property and the issuance of search warrants and that this delay violated Defendant’s Fourth Amendment rights.

**EVIDENCE ISSUES ASSOCIATED WITH ELECTONIC EVIDENCE**

Sorry we don’t have FOP Garon Muller here with us while we are talking evidence…

There really are two primary areas where our evidence rules impact the introduction of electronic evidence. Those are authentication and hearsay. THEY ARE SEPARATE ISSUES that may both impact introduction of electronic evidence and it would be simply wrong to conflate or confuse the two separate issues.

**AUTHENTICATION**

Shout out to Professor Milich for what follows concerning authentication of electronic evidence:

Authentication is a low evidentiary hurdle – but it is a hurdle nonetheless. See O.C.G.A. § 24-9-901 *(proof that authentication and hearsay are different issues – they have different rule numbers and are a part of different sections of the Code)*

Authentication does not remove the possibility of a forged document – or even a set up in the sending and receiving of messages. Instead, the law requires the party offering the evidence (a/k/a proponent) to sufficiently establish that the thing being offered is what it purports to be. Nothing more but also nothing less. See *Johnson v. State*, 347 Ga. App. 831, 841 (2018) (“The party proffering the evidence must present sufficient evidence to make out a prima facie case that the proffered evidence is what it purports to be. Once that prima facie case is established, the evidence is admitted and the ultimate question of authenticity is decided by the jury.”)

There are two different ways to handle authentication of electronic evidence. The complicated method and the low-tech method. In the complicated method, experts from Verizon or AT&T are called in and provide expert testimony concerning the IP address of the device, who it is registered to through the carrier, etc. This method is rarely used for obvious reasons.

In the low tech method of authenticating electronic data, external evidence is offered to prove that the communications are what they purport to be. For example, if the evidence being offered relates to Facebook, look for things such as if the photo of the Facebook page is actually the Defendant’s photo. Is the area where he/she lives as listed on Facebook actually correct. Look at the actual communications and if there is evidence that there was an ongoing dialogue between the sender and the receiver, see if there are things that can be proven to be true. For example, where the defendant says he is going to meet the person at a particular place at a particular time and he shows up at that place and time, the rest of the exchange is properly authenticated. If the messages back and forth reference family members of the defendant and he actually has those family members, the remainder of the conversation comes in.

“To authenticate the text messages, the State needed only to produce “evidence sufficient to support a finding” that the messages were actually sent and received by the defendant. OCGA § 24-9-901 (a). This could “be achieved through many means, including, but not limited to: testimony of a witness with knowledge that a matter is what it is claimed to be ... and appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.” *Johnson*, at 841, citing *Smith v. State*, 300 Ga. 538, 541 (2017).

So where you are dealing with text messages on the phone that has been established as belonging to the defendant, the fact that the contact is saved in the defendant’s phone is important. If there is an ongoing dialogue, determine if external proof can be established to “verify” the conversation as being one the defendant engaged in. Similar issues allow for the low hurdle to be crossed – but it is a hurdle and if an objection is raised, it needs to be dealt with appropriately.

**Hearsay Text Messages**

*Glispie v. State,* 300 Ga. 128 (2016): Two cell phones were seized incident to arrest in a drug case. At trial an officer testified as to the text messages extracted from the cell phones and the texts indicated the defendant used the cell phone to sell drugs. Officer read multiple incoming and outgoing text messages while testifying.

Court held that the outgoing text messages on the cell phone (although hearsay - falls under the admission by a party-opponent exception § 24-8-801(d)(2)(A)) and may be considered the Defendant’s own statements, as the facts of the case indicate the defendant sent the messages. However, the court stated the incoming text messages do not fall under the admission by a party-opponent hearsay exception. Court concluded that although the incoming messages were hearsay their admission was harmless in light of the other evidence.

In *Johnson v. State*, 347 Ga. App. 831 (2018), the trial court ruled prior to trial that the defendant’s cell phone records (which included the content of all of his inbound and outbound text messages) were admissible under the Business Records Exception (§24-8-803(6)). On appeal, the Ct of Appeals noted:

“While trial counsel for the defendant objected to the content of the text messages within the records as a “second layer” of hearsay, the trial court did not recognize the double hearsay issue, see OCGA § 24-8-805, and instead ruled that “the State has established that through the business records exception that these phone records and the corresponding text messages are admissible.”

(i) In its order denying the defendant's motion for new trial, the trial court held for the first time that the outgoing text messages were admissible as admissions by a party opponent. We agree. OCGA § 24-8-801 (d) (2) (A) provides that “[a]dmissions shall not be excluded by the hearsay rule. An admission is a statement offered against a party which is ... [t]he party's own statement.” As statements made by the defendant and offered against him, the outgoing text messages were admissible as admissions by a party opponent.”

They went on to address the incoming text messages:

“ As to the incoming texts, the trial court's conclusion in its order denying the defendant's motion for new trial is only partially accurate:

The text messages sent by defendant were offered by the State as proof of 1) defendant's identity as the owner and user of the phone, and 2) defendant's participation in the armed robbery ... The State maintained that the incoming messages were not admitted for the truth of the matter asserted, therefore non-hearsay, but merely for context to defendant's inculpatory admissions. Even assuming the incoming messages were inadmissible hearsay, however, this Court specifically finds that the incoming messages were not inculpatory of defendant and were harmless.

We agree that some of the incoming text messages may be admissible to provide context to outgoing text messages that are admissible as admissions. See *United States v. Osborne*, 677 Fed.Appx. 648, 654-655 (II) (A) (11th Cir. 2017) (third-party's incoming texts such as “yeah” and “ight bra” admissible to give context to the defendant's outgoing text messages because “they were not admitted for the truth of the matter asserted — particularly because they do not really assert anything”); see also *Jones v. State*, 339 Ga. App. 95, 101-103 (2), 791 S.E.2d 625 (2016). **However, a blanket admission of *all* the incoming text messages as “context” would be in error**. Statements by a non-defendant are admissible to give context to the defendant's alleged statements when the non-defendant's statements are *non-hearsay* because they are “(1) non-assertive statements that are incapable of being true or false or (2) statements that are indisputably false. In both cases, [the non-defendant's] out-of-court declarations [are] offered only to show their effect on the listener: [here, the defendant].” *United States v. Rivera*, 780 F.3d 1084, 1092 (III) (A) (2) (11th Cir. 2015). Thus, an incoming text message is admissible as context to the extent it is non-hearsay offered to prove its effect on the person receiving the message. Accordingly, upon retrial, the trial court should examine the text message exchanges the State wishes to introduce into evidence in light of the State's purported purpose in introducing them, and make an individualized determination as to the admissibility of the incoming texts.”

**HEARSAY INVOLVING RECORDED JAIL PHONE CALLS**

*(Jail phone calls have a special authentication statute, §24-9-923(c) when proper foundation is laid as to how the recording system works. See Smith v. State*, 300 Ga. 538 (2017).

In *Bully v. State*, 357 Ga. App. 663 (2020), defendant was talking on a recorded line from the jail during the trial. On appeal (while claiming ineffective assistance), it was noted that the wife was not called as a witness at trial. The call was played for the jury and, as you might imagine, the content of the call was not awesome for the defendant. The appellate court noted that what the defendant said was an admission and was not objectionable. However, what the prosecutor really wanted the call for was what the wife said which the defendant acknowledged. The Ct of Appeals held that the wife’s portion of the comment was hearsay and found that trial counsel was deficient for not objecting.

Thank you for listening to the Good Judge-Ment Podcast.

This episode is long and we apologize but we have been asked to address search and seizure issues (and we just couldn’t pass up a good evidence discussion)

*We always love a good evidence discussion. We are weird like that. Anyway, take these electronic evidence issues slowly and make the separate determination concerning each and every “search” of an electronic device. That analysis really helps.*

As we have noted, this episode was the product of requests made by our listeners. Please continue to help us help you by providing input and suggestions for episode topics at [goodjudgepod@gmail.com](mailto:goodjudgepod@gmail.com). You can visit our website, goodjudgepod.com for the episode notes from this and all other episodes.

*Again, thanks for listening to the Good Judge-Ment Podcast. And remember…*