PD-1269-16
COURT OF CRIMINAL APPEALS
AUSTIN, TEXAS
Transmitted 7/24/2017 11:57 AM
Accepted 7/24/2017 2:37 PM
DEANA WILLIAMSON
CLERK

No. PD-1269-16

FILED
COURT OF CRIMINAL APPEALS
7/24/2017
DEANA WILLIAMSON, CLERK

IN THE TEXAS COURT OF CRIMINAL APPEALS

CHRISTOPHER JAMES HOLDER,
Appellant

v.

THE STATE OF TEXAS,
Appellee

On Appeal From
THE FIFTH COURT OF APPEALS, DALLAS, TEXAS
No. 05-15-00818-CR

and

THE 416TH JUDICIAL DISTRICT COURT, COLLIN COUNTY, TEXAS
No. 416-80782-2013

APPELLANT'S BRIEF ON THE MERITS

STEVEN R. MIEARS
COUNSEL FOR APPELLANT
Texas State Bar No. 14025600
206 East College, Suite 200
Grapevine, Texas 76051
SteveMiears@msn.com
Telephone: 817-915-4006
Facsimile: 817-410-4783

ORAL ARGUMENT REQUESTED

IDENTITY OF PARTIES AND COUNSEL

Under Rule 68.4(a), Texas Rules of Appellate Procedure, the following is a complete list of the names and addresses of all parties to the trial court's final judgment, and their counsel in the trial court, as well as appellate counsel, so that the members of the court may at once determine whether they are disqualified to serve or should recuse themselves from participating in the decision and so the Clerk of the Court may properly notify the parties or their counsel of the final judgment and all orders of the Texas Court of Criminal Appeals.

1. **Trial Court:** The 416th Judicial District Court, Collin County, Texas, 2100 Bloomdale Road, McKinney, Texas 75071; The Honorable Judge Chris Oldner presided.

2. **Appellant**: Christopher James Holder, TDC Inmate No. 02006517, Eastham Unit, 2665 Prison Road #1, Lovelady, Texas 75851.

3. **Counsel for Appellant at Trial and on Appeal:** Mr. Steven R. Miears, Texas State Bar No. 14025600, 206 East College, Suite 200, Grapevine, Texas 76051.

4. **Counsel for the State of Texas at Trial:** Mr. Gregg Willis, Criminal District Attorney, Collin County, Texas; Ms. Cynthia Walker and Mr. Wes

Wynne, Assistant District Attorneys, Collin County, Texas, 2100 Bloomdale Road, Suite 200, McKinney, Texas 75071.

5. **Counsel for the State of Texas on Appeal:** Ms. Libby Lange, Assistant Criminal District Attorney, Collin County, Texas; Mr. John R. Rolater, Jr., Assistant Criminal District Attorney, Chief of the Appellate Division, Collin County, Texas, 2100 Bloomdale Road, Suite 200, McKinney, Texas 75071.

TABLE OF CONTENTS

INDEX OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Materials

TO THE HONORABLE COURT OF CRIMINAL APPEALS:

Appellant submits this brief on ground three of his Petition for Discretionary Review.

STATEMENT REGARDING ORAL ARGUMENT

Permission to present oral argument was requested in the Petition for Discretionary Review and granted by this Court.

STATEMENT OF THE CASE

Appellant was convicted of capital murder. The State did not seek the death penalty. There was an automatic life sentence. The opinion of the Court of Appeals issued August 19, 2016. It affirmed the conviction. *Holder v. State,* 2016 WL 4421362 (Tex. App. – Dallas 2016). This Court granted review of ground three of Appellant's Petition for Discretionary Review on June 7, 2017, in PD-1269-16.

ISSUE PRESENTED

Did the Court of Appeals err in holding the State's petition to obtain the Appellant's cell phone records set forth the "specific and articulable facts" required by federal law under 18 U.S.C. section 2703(d)?

STATEMENT OF FACTS

On November 12, 2012, Plano detective Jeff Rich brought a petition to the home of the Honorable Judge Mark Rusch. The petition requested an Order authorizing AT&T to release the historical cell phone records including historical cell-site location information (CSLI) associated with Appellant's cell phone number for October 20, 2012, through November 12, 2012. 6 RR 108-09.

The request was not for content-based information. What was said in the phone calls was not obtained. A live "wiretap" is the usual method to record the content of phone conversations. And the contents of text messages are usually not obtained using this method. An extraction or download of the phone by attaching it to specialized equipment is typically the method used to acquire the contents of text messages. It was also not a request for a live "pinging" of the cell phone which establishes the current whereabouts of a phone.

The CSLI and historical records information requested would include records on when calls, texts, and data were made and received by the phone, and for how long those communications lasted. The records would show the other phone numbers associated with those communications. And the records would show when data was transmitted and received by the phone.

Importantly for this case, the CSLI records identify the locations of the cell towers that the phone signals were hitting. It is generally accepted that a cell phone's signal will connect with the cell tower which provides the strongest signal. That cell tower is usually the one located closest to the phone. The range and direction of coverage for a cell tower depends upon several factors, but it is limited to a particular geographical area. Testimony establishing the probable range for a cell tower is used to prove the probable presence of a phone within that area at a particular time.

Judge Rusch signed the Order authorizing AT&T to release the records. Rich forwarded the Order to AT&T, but it was rejected. AT&T notified Rich he had to recite in the petition his need for the records was based upon "probable cause." 2 RR 115. Rich testified at the motion to suppress hearing that, "[i]t was simpler for me to just change the wording and have it re-signed and bother the judge one more time, as opposed to waiting until later in the day, after their counsel had time to look at it and make an assessment." 2 RR 118. After changing only the phrase "reasonable suspicion" to "probable cause," Rich took the petition back to Judge Rusch. He signed that Order too. 13 RR 132-36; State's Exhibits 7A and 7B. AT&T then emailed the records to Rich. 13 RR 131-32.

In support of the request for the records the petition stated:

> Petitioner has probable cause that the above records or information are relevant to a current, on-going police investigation of the following offense or incident: Death Investigation - Texas PC 19.03
>
> The cellular telephone was used by a possible suspect to communicate with unknown persons and obtaining the locations of the handset will allow investigators to identify if this suspect was in the area at the time of the offense and will provide investigators leads in this case.
>
> State's Petition for Court Order to Obtain Electronic Communication Records, 13 RR 134; State's Exhibit 7B.

Judge Rusch was not provided with any additional information about the investigation. Rich's petition was unsworn. No affidavits or offense reports were presented to the judge. No record of the *ex parte* meeting between detective Rich and Judge Rusch was made. 2 RR 120-27.

Appellant's cell phone records and CSLI were used by the State to prove he was in Plano on the date of the homicide; more specifically, that he was in the vicinity of the victim's residence at a time when the victim could have been killed. Based upon this evidence, the Court of Appeals found the evidence sufficient to prove Appellant to be the perpetrator. Appellant moved to suppress this evidence. He argued the petition was insufficient under the federal Electronic Communications Privacy Act, and the records were thus inadmissible under Article 38.23. The trial court denied the motion. 6 RR 108-40; 2 RR 109-40; 3 RR 8-12; CR 47-56; CR 113-27 (Trial Brief in Support); CR 399 (Trial Court's Ruling).

SUMMARY OF THE ARGUMENT

The Federal Electronic Communications Privacy Act, 18 U.S.C. § 2703,[1] sets forth how the police may obtain cell phone records and CSLI from a provider of cellular phone service. 18 U.S.C. § 2703(d). These methods include use of a warrant, obtaining a court order, issuance of a subpoena, or making a request based upon exigent circumstances. Law enforcement chose to seek Appellant's records by applying for a court order. The statute states that a court may not issue the order unless the officer "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

Article 38.23(a) of the Texas Code of Criminal Procedure codifies an exclusionary rule of evidence which is broader than its federal counterpart. Under that statute, evidence obtained in violation of the laws of the United States of America is inadmissible. Notwithstanding the lack of an expectation of privacy in the records protected by the Fourth Amendment, Appellant has standing under

[1] The Electronic Communications Privacy Act is sometimes referred to as the SCA, or "Stored Communications Act". The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but the ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute. See Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the SCA here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

38.23(a) to object to the admissibility of the evidence procured in violation of 18 U.S.C. § 2703(d) by the government.

The federal law was enacted to protect confidential records held by third parties from being obtained by the government to use in a criminal prosecution. Under that law, a showing of reasonable suspicion that the records sought relate to an investigation must be made. Article 38.23(a) requires suppression of evidence obtained by violating a federal law which regulates how evidence is gathered in a criminal prosecution.

The petition failed to articulate specific underlying facts showing reasonable grounds to believe the records were relevant and material to an ongoing criminal investigation. The Court of Appeals erred in holding the petition was sufficient. Appellant's motion to suppress the cell phone records and CSLI should have been granted. The records were crucial to the State's proof of the identity of Apellant as the murderer. The holding of the Court of Appeals must be reversed. Remand for a new trial is required.

ARGUMENT

Standing

In its brief to the Court of Appeals, the State did not complain that Appellant lacked standing to complain about the State's acquisition of his records. the Court

of Appeals did not question Appellant's standing to seek exclusion of the evidence. The Court of Appeals rejected Appellant's arguments by finding the petition was sufficient under the federal law. However, at oral argument in the Court of Appeals, the State raised standing. It is anticipated the State will raise it for the first time on appeal in its brief which is apparently permissible. *See Kothe v. State,* 152 S.W.3d 54, 59 (Tex. Crim. App. 2004).

This Court holds that the government's warrantless acquisition of CSLI records from a cell phone service provider violates neither the Fourth Amendment to the U.S. Constitution, nor Article I § 9 of the Texas Constitution. *See Ford v. State,* 477 S.W.3d 321, 322 (Tex. Crim. App. 2015); *see also Hankston v. State,* 517 S.W.3d 112 (Tex. Crim. App. 2017). In doing so, the Court has joined those jurisdictions which hold a customer has no expectation of privacy in the data stored by the phone company detailing use of a cell phone.[2] The principle that records or information voluntarily shared with third parties deserve no Fourth Amendment protection is called the "third-party doctrine." Cell phone data, once received or transmitted, is like trash left for the garbage man. The government may acquire information abandoned. Standing to complain under the Fourth Amendment ceases

[2] The U.S. Supreme Court recently granted review in *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2015); *cert granted* 2017 WL 2407484 (June 5, 2017). The question for review is: Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment. This decision may shed light on the continued viability of the third-party doctrine in the context of confidential records protected under federal law.

to exist. Appellant's right to object, therefore, must exist under some law other than a right to privacy grounded in the Constitution.

In *State v. Huse,* this Court recognized, perhaps in judicial dictum, that use of a defective subpoena to acquire blood test results could cause suppression of those records. As medical records, the blood test results were protected from disclosure under a federal law, HIPAA, 45 C.F.R. § 164.512. Had the subpoena for the records been defective, the Court said they might have been suppressed under Article 38.23. *Huse,* 491 S.W.3d 833, 841-43 (Tex. Crim. App. 2016).

Besides HIPAA, other federal laws prescribe a judicial process to be followed prior to release to the government of records held by third parties. For example, government access to financial records is regulated by The Federal Financial Records Privacy Act, 12 U.S.C. § 3403. These statutes protect a privacy interest in records utilized and held by third parties that provide a service to individuals related to confidential matters. The statutes create an expectation the information will remain confidential unless certain procedures are followed—procedural protections guarded by a lower threshold showing of need than constitutionally mandated probable cause.

The federal statute at issue here is the Federal Electronic Communications Privacy Act, 18 U.S.C. § 2703, also known as the Stored Communications Act (SCA). This law establishes procedures for federal and state authorities to follow

to acquire CSLI from third-party providers. However, the act states that "the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. The exclusion of evidence obtained in violation of this law is not a remedy in federal court. *See, e.g,. United States v. Guerrero,* 768 F.3d 351, 353 (5th Cir. 2014).

Exclusion of evidence under federal law is usually limited to evidence obtained through certain violations of the Fourth Amendment. Seldom does suppression result for statutory violations. As explained by the U.S. Supreme Court, "[i]n those cases, the excluded evidence arose directly out of statutory violations that implicated important Fourth and Fifth Amendment interests." *Sanchez-Llamas v. Oregon,* 548 U.S. 331, 348, 126 S. Ct. 2669, 2681 (2006).

No federal laws, however, prevent states from choosing the remedy of suppression to deter statutory violations of federal law. By legislation, Texas has done that. The Texas exclusionary rule operates to suppress not only evidence obtained in violation of the U.S. and Texas constitutions, but also embraces federal laws and Texas laws. *See State v. Rodriguez,* 2015 WL 5714548 (Tex. App.—Eastland 2015) (not designated for publication), *judgment aff'd* 2017 WL 2457441 (Tex. Crim. App. 2017) (not designated for publication); *see also Milligan v. State,* 2014 WL 7499050 (Tex. App. – Dallas 2014, pet. ref'd).

The Texas Legislature intended Article 38.23 to be more expansive than the federal exclusionary rule. *See Miles v. State*, 241 S.W.3d 28, 35 (Tex. Crim. App. 2007); s*ee generally* George E. Dix and Robert O. Dawson, Texas Practice: Criminal Practice and Procedure §§ 4.11–4.35 (2d ed. 2001) (discussing the distinctions between the federal constitutional exclusionary law and the Texas statutory exclusionary rule; noting that, "Article 38.23 of the Code of Criminal Procedure imposes what is probably the broadest state exclusionary requirement of any American jurisdiction.").

On its face, the statute would seem to embrace all state and federal laws. However, this Court has held otherwise. As the Court said in *Wilson v. State,* "[t]he primary purpose of article 38.23(a) is to deter unlawful actions which violate the rights of criminal suspects in the acquisition of evidence for prosecution. Article 38.23(a) may not be invoked for statutory violations unrelated to the purpose of the exclusionary rule or to the prevention of the illegal procurement of evidence of crime." *Wilson*, 311 S.W.3d 452, 459 (Tex. Crim. App. 2010). A nexus, therefore, between the statute's purpose and the procurement of the evidence for prosecution should exist.

Under 38.23, standing does not necessarily depend upon whether the individual has a constitutionally protected privacy interest in the evidence itself. Suppression may result for violating a statute intended to regulate the procedure

used in "gathering, creating, or destroying evidence." *Id* at 458. In *Wilson*, a detective violated Texas Penal Code § 37.09. He fabricated a lab report and then used it to obtain a suspect's confession to murder. The confession was otherwise voluntary under federal constitutional law. The majority rejected arguments that the defendant did not have standing to complain under Article 38.23. It held that violating a penal statute governing evidence tampering barred admission of other evidence obtained through that violation. The Court said the legislative intent was to ensure that citizens and members of the legal community could rely upon the integrity of government-generated documents and other evidence. The statutory exclusionary rule pre-empted the voluntariness of the defendant's confession. *Id.* at 459-61. And, in *Wilson*, it was irrelevant that the defendant lacked a privacy interest in the fabricated report. *Id.*

Noteworthy is that the Texas legislature has periodically changed the law on whether 38.23 encompasses federal laws. That legislative history may reflect changes in policy which responded to the needs of the day. The original exclusionary statute was all encompassing. It was altered in response to the passage of state-wide prohibition laws. In the Court's 1951 opinion in *Schwartz v. State,* the Court observed:

> Prior to 1929, the statute, now Article 727a, Vernon's Code of Criminal Procedure, read, "No evidence obtained by an officer or other person in violation of any provisions of the Constitution or laws

> of the State of Texas, or of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case." It now reads, "No evidence obtained by an officer or other person in violation of any provisions of the Constitution or laws of the State of Texas, or of the Constitution of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case." In 1930, we said in Montalbano v. State, 116 Tex. Cr. R. 242, 34 S.W. (2d) 1100: "* * * Article 727a, C.C.P., was amended so as to no longer require rejection of evidence obtained in violation of laws of the United States."
>
> *Schwartz v. State,* 246 S.W.2d 174, 177 (1951), *judgment aff'd*, 344 U.S. 199 (1952).

The 1929 reenactment modified the law by excluding reference to the "laws" of the United States. That modified language led to courts holding there was no right to exclusion of evidence obtained in violation of federal statutes. *Id.* Noteworthy, perhaps in the context of this case, is that *Schwartz* held admissible wiretap evidence obtained in violation of the Federal Communications Act.

The 1953 Legislature responded to *Schwartz* and addressed this issue. The legislature recognized the language from the modified 1929 version eviscerated a primary purpose of the statute. It responded by enacting the present language that clarifies that suppression is necessary if the evidence was obtained in violation of the "laws" of the United States. *See Gillett v. State*, 588 S.W.2d 361, 369 (Tex. Crim. App. 1979); Acts 1953, 53rd Leg., 669, ch. 253, § 1.

More recently, in *State v. Harrison,* the Second Court of Appeals addressed standing under Article 38.23 *vis a vis* 18 U.S.C. § 2703. *Harrison,* 2014 WL 2466369 (Tex. App. – Fort Worth 2014) (mem. op., not designated for publication). The Court held that although the federal law does not exclude evidence as a remedy for its violation, Article 38.23 does. *Id.* at *3. The Court observed that *Wilson* provides the framework for analyzing whether Article 38.23 applies to exclude evidence obtained in violation of a federal or state law. *Id.* at *6.

Appellant has standing under Article 38.23 to seek suppression of evidence obtained in violation of the SCA because the SCA was enacted to regulate governmental gathering of evidence for a criminal prosecution. As in *Wilson,* the unlawful garnering of evidence pre-empts Appellant's lack of a constitutionally protected privacy interest in the records.

Once a defendant moves for suppression under 38.23 produces evidence of a statutory violation, the burden shifts to the State to prove compliance. *White v. State,* 2017 WL 908787, at *6 (Tex. App.—Dallas Mar. 8, 2017) (pet. filed June 13, 2017) (mem. op., not designated for publication). Appellant moved for suppression here, and produced evidence the federal law was violated. It was the State's burden to prove the petition would comply with the SCA.

The Petition

The SCA authorizes "a provider of electronic communication service" to release to a government entity "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or (B) obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703. If attaining a court order is the method chosen, then subsection (d) requires the government entity seeking such disclosure "offer" to a court "specific and articulable facts showing there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

Proof required to show "specific and articulable facts" under this law has been described as a level of proof higher than necessary for a subpoena, but lower than probable cause. The Tenth Circuit suggested that the "specific and articulable facts" language of 2703(d) "derives from the Supreme Court's decision in *Terry v. Ohio,* 392 U.S. 1 (1968)." *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008). Another court said that law enforcement is not allowed merely to certify that it has specific and articulable facts that would satisfy the standard.

Rather, as the statute states, the government must offer those facts to the court in the application. *See United States v. Kennedy,* 81 F. Supp. 2d 1103, 1109-10 (D. Kan. 2000). The *Kennedy* Court held that a conclusory application for a 2703(d) order "did not meet the requirements of the statute".

The *Terry* standard of reasonable suspicion for a warrantless "stop and frisk" has a history of case-by-case development which may provide a framework to analyze petitions requesting CSLI. This Court discussed the *Terry* standard in *Wade v. State*:

> A police officer has reasonable suspicion for a detention if he has specific, articulable facts that, when combined with rational inferences from those facts, would lead him to reasonably conclude that the person detained is, has been, or soon will be engaged in criminal activity. This is an objective standard that disregards the actual subjective intent of the arresting officer and looks, instead, to whether there was an objectively justifiable basis for the detention.
>
> ....
>
> The standard also looks to the totality of the circumstances; individual circumstances may seem innocent enough in isolation, but if they combine to reasonably suggest the imminence of criminal conduct, an investigative detention is justified.
>
> ....
>
> It is enough to satisfy the lesser standard of reasonable suspicion that the information is sufficiently detailed and reliable—i.e., it supports more than an inarticulate hunch or intuition—to suggest that something of an apparently criminal nature is brewing.
>
> ....
>
> As with the question of whether a consensual encounter has become a Fourth Amendment detention, the question of whether a certain set of historical facts gives rise to reasonable suspicion is reviewed de novo.

Wade v. State, 422 S.W.3d 661, 668-69 (Tex. Crim. App. 2013).

The legislative history behind section 2703(d) provides insight into the level of proof necessary. The House Report stated that, "[t]his section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation." H.R. Rep. No. 102-827, at 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511-12 (quoted in full in *Kennedy,* 81 F. Supp. 2d at 1109 n.8).

In *Ford v. State,* this Court signposted *via* footnote that the facts stated in the petition must be more than conclusory. *Ford,* 477 S.W.3d 321 (Tex. Crim. App. 2015). This Court held a warrant was not required in *Ford*. So while *perhaps* not dispositive to the court's holding in *Ford* that a warrant was unnecessary, this Court believed it "worth noting" that:

> the application [for the records] does contain three pages of exhaustive detail to establish the "reasonable belief that the information sought is relevant to a legitimate law enforcement inquiry" that is *necessary* for an order under Tex. Code Crim. Proc.

> art. 18.21, Sec. 5(a), as well as the "specific and articulable facts" showing *required* for a Stored Communications Act order.
>
> *Id.* at 9 n.4 (emphasis added).

According to the Appellee's Brief filed in this Court in *Ford*, the application stated:

> [T]he complainant had been found dead in her condominium, with no sign of forced entry and nothing missing except her dog; her death had been ruled a homicide; she had been at a New Year's Eve party the night before with others including Jon Thomas Ford; Ford had left the party before the others; two witnesses drove by Ford's house a few blocks from the victim's condo and did not see his car parked there; Ford told the detective he had been home asleep before midnight; a surveillance video showed a vehicle matching Ford's white Tahoe entering and exiting the condo complex twice; it also showed a person dressed similarly to the way Ford had been that night entering the complex on foot; an hour later the same person left the complex; five minutes later the car resembling Ford's drove past; the detective had obtained Ford's cell phone records with a subpoena, which showed he had checked his voicemail at 2:30 a.m., about twenty minutes after the white Tahoe had driven away from the victim's complex, and also a time when Ford had claimed to be asleep.
>
> Appellee's Brief at 12-13 citing Supp. CR 180-83, 477 S.W.3d 321 (Tex. Crim. App. 2015).

In stark contrast, the State's petition in Appellant's case comprises but a few conclusory statements:

> The cellular telephone was used by a possible suspect to communicate with unknown persons and obtaining the locations of the handset will

> allow investigators to identify if this suspect was in the area at the time of the offense and will provide investigators leads in this case.

No information was given about how the "possible suspect" was connected to the crime. No information was given about the crime itself. Nothing is given about why the person was a "possible" suspect. No facts were given why it was believed the "possible suspect" communicated with "unknown persons." Nor is it described how those potential communications related to the investigation.

Further, there was no support in the request for "tower information" for the period of October 20, 2012 through November 12, 2012. The petition does not set forth the date when a person was reported missing or a victim was discovered, much less why information for twenty-four days relates to the investigation. At best, the petition communicated that: a) there was a murder of an unknown person at an unknown time and unknown place; b) a cell phone was possibly used by an unidentified someone, to possibly communicate with an unidentified someone else; and, c) the police want to know whether that cell phone was possibly in some unidentified area. Based upon the lack of specifics described in this petition, the cell phone numbers of one and all could have been swapped for Appellant's.

The particulars in this petition are akin to the insufficiencies found in *In re Applications of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d).* The court concluded the government's effort to comply with the "specific

and articulable facts" standard fell short. The applications failed to include: factual information about the alleged perpetrators, the basis for the government's belief those individuals were responsible for the crime, or any causal nexus between the investigation and the information the government sought. *In re Applications,* 206 F.Supp.3d 454 (D.D.C. 2016).

The court also took issue with the ambiguous and equivocal language in the applications. The applications stated the alleged perpetrators "used or purported to use [the email accounts]" and that the information sought "will help investigators learn whether and how the perpetrators of the attack communicated with each other and other co-conspirators." *Id.* at 457. The court observed that "the government is incorrect if it believes that section 2703(d) permits the disclosure of more electronic information in cases where the government knows the least." *Id*. The court further stated that based upon the language of the applications, "[t]he government does not appear to have any idea at this point whether the records it seeks will advance its investigation." *Id.*

As in *Kennedy,* the court found it wanting for the government's application to convey that, "it is believed that this information will assist in the investigation relating to the aforementioned offenses." *Id.* discussing *Kennedy*, 81 F. Supp.2d 1103. An application which speculates on how the records might assist an investigation articulates only a hunch or guess. "[B]ecause of the intermediate

evidentiary burden it imposes on the government, an application seeking records pursuant to section 2703(d) is unlikely to be the first step in a criminal investigation." *Id.*

The petition here suffers the same shortcomings. In wanting the records to see "if this suspect was in the area at the time of the offense" it is evident the request was used as the starting gate for the inquiry. If more facts were known they were not included in the petition. Either way only a hunch was imparted; not reasonable suspicion.

As in *In re Applications*, there is an absence of factual information about the alleged perpetrator. The State does not appear to be sure the requested records are attributable to the perpetrator of the crime. Nor does the application include any basis for the belief that that individual is responsible for the crime. Also, like in *In re Applications* and *Kennedy*, the State offered nothing beyond speculation that the information being sought might "provide leads." This is exactly the "fishing expedition" the law intended to guard against.

Courts have additionally found applications deficient under § 2703(d) where the information sought is "largely untethered from temporal aspects of the crime being investigated." *See Matter of Application of United States for an Order Authorizing Disclosure of Historical Cell Site Information for [Telephone Numbers (Redacted)]*, 20 F.Supp.3d 67 (D.D.C. 2013). There the court found the

applications failed to justify the time span for the CSLI requested, instead of being limited to a timeframe related to the crime itself. *Id.* at 73 "[I]f the government is simply trying to tie the suspects to the scenes of the crimes, all that must be done is to ask for CSLI that is contemporaneous to the crimes." The court said, "it is the government's burden to provide "specific and articulable facts" explaining why it is entitled to these records; the Court cannot simply infer what the purpose may be." *Id.*

The court held the timeframe for the CSLI requested must have a temporal connection to the crime. The facts supporting the timeframe requested must be offered. "[A]llegations that an individual may have been involved in a specific crime on a specific date and at a specific time are insufficient to allow the 120 days—or even seven days—of CSLI sought in these Applications." *Id.* The court established that where these facts are not tendered, the court has no ability to determine whether the information being sought is relevant and material to the investigation. *Id.*

Similarly, the State's petition here included no facts justifying the request for "tower information" for the period of October 20, 2012 through November 12, 2012. The reasoning of the Fifth Court of Appeals regarding the time frame requested is suspect. The Court writes:

> Although the petition did not set out an offense date, when Detective Rich executed the petition, the morning after Tanner's body was found, the police did not yet have a time frame for when the offense occurred. Moreover, the petition's request for historical cell data was limited to twenty days, suggesting the offense was committed within that time span.
>
> *Holder v. State,* 2016 WL 4421362, at *11 (Tex. App. – Dallas 2016).

Indeed, if the petition had supplied those facts, it may have started to articulate a reason for the time span requested. Instead, the Court of Appeals re-writes the petition for the officer. It supplies missing facts, makes assumptions from those facts, and thereby proves the point: nothing was articulated in the petition showing the relevance of the records to an ongoing investigation. Instead of analyzing the sufficiency of the facts, as stated in the petition, the Court of Appeals ratifies the petition in hind sight. As the State's petition proffers no facts about the date and time of the crime, it is impossible to determine from its face whether the timeframe for the records sought relates to any aspects of the crime being investigated.

In summary, there were no specific facts offered as required. Nothing was articulated. Nothing was given to establish reasonable grounds to determine whether the records were "relevant and material to an ongoing criminal

investigation." Judge Rusch erred in signing the order. This petition is an exemplar of the governmental overreach the federal and Texas legislative bodies sought to prevent when enacting the SCA and Article 38.23.

The initial burden to determine whether the information provided in a petition is adequate falls upon an issuing judge. This case could provide those "front-line" judges with guidance on what to look for in a petition when an officer comes knocking. More importantly, it may supply law enforcement with the impetus to write a petition which includes more than a recitation of boiler plate phrases desired by the legal department of a cell phone provider.

These petitions for orders are presented *ex parte*. They need not be sworn to by the officer. After records are obtained, nothing akin to an inventory is returned to the issuing judge. No judicial review occurs to determine whether the records obtained exceeded the scope of the order. Nothing prevents the government from storing the records indefinitely, or sharing them with other agencies. A person may never discover their cell records were even acquired and perused by the government. That revelation depends upon whether criminal charges are later filed. Absent charges being filed, the government is under no obligation to inform the individual the records were obtained.

Cell phone records and CSLI can now accurately nail down to within a small area where a person's phone was on a specific date and at a precise time. They tell

how long it was there and where it travelled. The records track similar data for the other phones or computers with which it exchanged speech and data. Even DNA can't supply this information. This impressive tool should not be beyond the reach of legitimate law enforcement.

The requirement of a threshold showing of "specific and articulable facts" assures the inquiry will be legitimate. It balances government's legitimate need to know against an individual's imperfect right to confidentiality in information held by a third party. It is a threshold showing that judges, law enforcement, and the bar have become familiar with through a history of cases analyzing exceptions to the requirement of a warrant. When, as here, that showing has not been made, Article 38.23 requires exclusion of the records from evidence.

PRAYER

Appellant respectfully requests this Honorable Court reverse the opinion of the Court of Appeals, and remand this case to the trial court for a new trial.

RESPECTFULLY SUBMITTED,

/S/ STEVE MIEARS

STEVEN R. MIEARS
COUNSEL FOR APPELLANT
Texas State Bar No. 14025600
206 East College, Suite 200
Grapevine, Texas 76051
SteveMiears@msn.com

Telephone: 817-915-4006
Facsimile: 817-410-4783

CERTIFICATE OF SERVICE

This is to certify that a true and correct copy of the above and foregoing Appellant's Brief on the Merits was delivered by electronic e-filing to the Collin County District Attorney; and to the State Prosecuting Attorney, and that a copy was mailed to the Appellant, Christopher James Holder on the 24th day of July, 2017.

/S/ STEVE MIEARS

STEVEN R. MIEARS

CERTIFICATE OF WORD COUNT

Counsel for the Appellant certifies that in accordance with Rule 9.4 of the Texas Rules of Appellate Procedure the word count of this brief is less than 7,934 words and within the allowable word limit.

/S/ STEVE MIEARS

STEVEN R. MIEARS

APPENDIX

THE STATE OF TEXAS }
COUNTY OF COLLIN }

PETITION FOR COURT ORDER TO OBTAIN ELECTRONIC COMMUNICATION RECORDS

Now comes Petitioner, the City of Plano, Texas, acting by and through the undersigned peace officer of the Plano Police Department, Plano, Collin County, Texas Pursuant to the authority of article 18 21, Section 5, Texas Code of Criminal Procedure, Petitioner hereby makes written application for a Court Order to obtain the below-listed records or information pertaining to a subscriber or customer of the below-listed electronic communication service

The following records or information are sought
Any and all records regarding the identification of a ***AT&T Wireless*** *user with the assigned telephone number of* **469-286-7425**, *to include subscriber's name, address, date of birth, status of account, account history, call detail records,* ***including tower information*** *for calls made or received, for the period of October 20, 2012 through November 12, 2012, service address and billing address, ANI, method of payment and information on any and all other numbers assigned to this account or this user in the past or present Affiant also requests that this order allow for the precision location/GPS location of the cellular handset to be provided for a period of 20 days beginning November 12, 2012*

The name of the company believed to be in possession of this information is
AT&T Wireless
POB 24679
West Palm Beach, Florida 33416
(888) 938-4715

Petitioner has specific and articulatable facts, along with reason to believe that the above records or information are relevant to a current, on-going police investigation of the following offense or incident

Death Investigation – Texas PC 19.03

The cellular telephone was used by a possible suspect to communicate with unknown persons and obtaining the locations of the handset will allow investigators to identify if this suspect was in the area at the time of the offense and will provide investigators leads in this case

Wherefore, Petitioner prays the Court to issue its Order for Disclosure of the above-described records or information

Signed at McKinney, Collin County Texas, this 12 day of November, 2012

Petitioner – Peace Officer

THE STATE OF TEXAS }
COUNTY OF COLLIN }

RE Petition For Court Order To Obtain Electronic Communication Records } IN THE CRIMINAL DISTRICT COURT } MCKINNEY, COLLIN COUNTY, TEXAS

ORDER FOR DISCLOSURE OF ELECTRONIC COMMUNICATION RECORDS

On this date came on to be considered the above Petition for a Court Order to obtain Electronic Communication records, said Petition appearing within this document and being hereby incorporated by reference It appears to the Court that adequate cause is shown for the issuance of an Order, and that the described records or information are reasonably believed to be relevant to a legitimate law enforcement inquiry

IT IS ORDERED, pursuant to the authority of Texas Code of Criminal Procedure Article 18 21 Section 5, that the electronic communication service or telephone company listed in said Petition (*AT&T Wireless*) shall forthwith deliver or disclose to the Petitioner or its Agent the subscriber records or information as described in the Petition by furnishing the records to

Detective Jeff Rich
Plano Police Department
909 14th Street
Plano, Texas 75074
Phone - (972) 941-2631
Email – jeffr@plano gov

You are not to disclose the existence of this request as any disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law

ENTERED THIS 12 DAY OF November, 2012, at 1200 AM

JUDGE
401st DISTRICT COURT COLLIN COUNTY, TEXAS

Vernon's Ann.Texas C.C.P. Art. 38.23
Art. 38.23. [727a] Evidence not to be used

Art. 38.23. EVIDENCE NOT TO BE USED. (a) No evidence obtained by an officer or other person in violation of any provisions of the Constitution or laws of the State of Texas, or of the Constitution or laws of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case.

In any case where the legal evidence raises an issue hereunder, the jury shall be instructed that if it believes, or has a reasonable doubt, that the evidence was obtained in violation of the provisions of this Article, then and in such event, the jury shall disregard any such evidence so obtained.

(b) It is an exception to the provisions of Subsection (a) of this Article that the evidence was obtained by a law enforcement officer acting in objective good faith reliance upon a warrant issued by a neutral magistrate based on probable cause.

Acts 1965, 59th Leg., vol. 2, p. 317, ch. 722.

Amended by Acts 1987, 70th Leg., ch. 546, Sec. 1, eff. Sept. 1, 1987.

18 U.S.C.A. § 2703

§ 2703. Required disclosure of customer communications or records

Effective: October 19, 2009

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber

to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection

records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or

compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.