No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

IN RE STEVEN WESTE,

Petitioner

PETITION FOR WRIT OF HABEAS CORPUS

Michael C. Gross
Counsel of Record
1524 North Alamo Street
San Antonio, Texas 78205
(210) 354-1919
(210) 354-1920 Fax

QUESTION PRESENTED FOR REVIEW

If the government issued pretrial a subpoena to a defendant's cell phone provider for historical cell-site location information (CSLI) in order to find a crime scene and, as a result of the subpoena, the government was able to discover the list of phone calls by the defendant, the CSLI for the defendant, and the locations of the cell towers, does this government action violate Carpenter v. United States, ___U.S.___, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018) (the government must use a warrant, in the absence of an exception such as exigent circumstances, to obtain CSLI from wireless carriers)?

LIST OF PARTIES

United States

Steven Weste

TABLE OF CONTENTS

INDEX TO APPENDICES

TABLE OF AUTHORITIES CITED

CASES — PAGE NUMBER

CONSTITUTION, STATUTES, AND RULES

No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

IN RE STEVEN WESTE,

Petitioner

PETITION FOR WRIT OF HABEAS CORPUS

The Petitioner respectfully prays this Court invoke its original habeas jurisdiction and grant him relief from his illegal detention and unconstitutional judgment of conviction for violating 18 U.S.C. § 1001(a)(2), making false statements to a federal agency; 18 U.S.C. § 1001(a)(1), concealing a material fact in a matter within the jurisdiction of a federal agency; and 18 U.S.C. § 875(c) transmitting threats to kill others, and sentence of imprisonment for 15 years.

Counsel for Petitioner, Steven Weste, asks this Court to grant relief on his claim that his conviction for violating 18 U.S.C. § 875(c) was invalid given the effect of this Court's new rule announced in *Carpenter v. United States*, ___U.S.___, 138

S.Ct. 2206, 201 L.Ed.2d 507 (2018). The Petitioner was convicted after the government issued pretrial a subpoena to the Petitioner's cell phone provider for historical cell-site location information (CSLI) in order to find a crime scene and, as a result of the subpoena, the government was able to discover the list of phone calls by the Petitioner, the CSLI for the Petitioner, and the locations of the cell towers.

OPINION BELOW

The opinion for the United States District Court for the Western District of Texas, San Antonio Division, appears at Appendix A and is unpublished. The opinion for the magistrate judge for the United States District Court for the Western District of Texas, San Antonio Division, appears at Appendix B and is unpublished.

JURISDICTION

This Court has jurisdiction under its authority to grant original habeas relief. 28 U.S.C. §§ 2241(a), 2254(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fifth Amendment to the Constitution of the United States provides, "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself,

nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

The Fourteenth Amendment to the Constitution of the United States provides in Section 1, "All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

STATEMENT OF THE CASE

An indictment was filed against the Petitioner in Cause No. SA-07-CR-323-XR, for transmitting a threat to kill another allegedly occurring on or about November/December 2006 and January/March 2007. A superseding indictment was filed against the Petitioner in the same cause for making false statements to a federal agency, concealing a material fact in a matter within the jurisdiction of a federal agency, and transmitting threats to kill others allegedly occurring on or about November/December 2006 and January/March 2007. The Petitioner pleaded not guilty, was convicted on all 15 counts, contrary to his plea, and was sentenced to imprisonment for 180 months or 15 years. A motion for new trial was not filed. A

notice of appeal was timely filed. The United States Court of Appeals for the Fifth Circuit affirmed the judgment. *United States v. Weste*, 419 Fed. Appx. 507, 2011 U.S. App. LEXIS 6034 (5th Cir. 2011). This Court denied the petition for a writ of certiorari. *Weste v. United States*, 565 U.S. 827, 132 S.Ct. 119, 181 L.Ed.2d 42 (2011).

A federal writ was timely filed and denied by the district court. *Weste v. United States*, 2013 U.S. Dist. LEXIS 82233 (W.D. Tex., June 11, 2013). The United States Court of Appeals for the Fifth Circuit affirmed the denial of relief. *United States v. Weste*, No. 13-50564 (5th Cir., January 14, 2014). This Court denied the petition for a writ of certiorari. *Weste v. United States*, 572 U.S. 1117, 134 S.Ct. 2319, 189 L.Ed.2d 178 (2014).

The Petitioner, Steven Weste, had dated the complainant, Amanda Stewart, beginning in May 2005. From February 25, 2006 until April 16, 2007, numerous people, including police officers, college students, Amanda, Amanda's family, and Steven himself, received approximately 648 threatening emails. (R - v.5 - 1261).[1] The emails appeared to be from Amanda's mother, Celia Phillips, and from Amanda's ex-boyfriend, Ricardo Ramirez. The content of the emails ranged from threatening

[1]The clerk's record from the trial will be referred to as "T and page number." The court reporter's record from the trial will be referred to as "R and volume and page number."

and violent to innocent and obscure. Investigators from Homeland Security, along with the College of William and Mary police department (Amanda was a student at William and Mary), began investigating these emails. Initially, the investigation was focused on Ricardo Ramirez, Amanda's ex-boyfriend. (R - v.5 - 1261; R - v.7 - 1718).

A majority of the threatening emails involved in this case contained the same IP address. (R - v.7 - 1726). The government's investigation suspected that the IP address belonged to a T-Mobile user. Investigators eventually believed that the IP address (208.54.95.1) could have in fact belonged to any T-Mobile "Hotspot" user located in the eastern half of the United States. (R - v.8 - 1723). T-Mobile sold "Hotspot" cards which provided customers with internet access at public locations such as Starbucks and Borders. (R - v.8 - 1723). When a customer used the "Hotspot" card to access the internet, any email sent would contain the same IP address (i.e., 208.54.95.1). Thus, all emails sent using a T-Mobile "Hotspot" card would contain the same IP address whether it was sent from a Starbucks in Dallas or a Hyatt in New York. (R - v.8 - 1723).

Because so many of the threatening emails contained the T-Mobile IP address, the government subpoenaed T-Mobile and directed them to produce data which would connect specific "Hotspot" cards to specific log-ins. In other words, the government wanted to link the purchaser of a particular card to a particular location

at a particular time. This task proved to be difficult for T-Mobile to accomplish because T-Mobile did not maintain data regarding which "Hotspot" cards were used at which locations at a given time. As a result, T-Mobile attempted to create an "experimental" program to satisfy the government's request. (2/18/09 Pretrial Hearing at 16).

A deposition was held on March 16, 2009 wherein the T-Mobile employee assigned with gathering the data for the government, Douglas Latimer, testified about the program. At the deposition, Latimer testified that he created the experimental program and that it contained "bugs" and "glitches." Deposition at 83, 84, 91. Latimer had difficulty explaining his own program, and on multiple occasions was unable to explain why a particular item was in the program. During the deposition, Latimer stated that it was not possible to link a particular card to a particular location where the card was accessed, and it was not possible to correlate a PIN card with a log-in. *Id.* at 93, 122. Latimer stated that he was making assumptions. *Id.* at 126. With respect to this, Magistrate Judge Primomo stated in his filed opinion at Appendix B that, "Instead, Calfas [trial defense counsel] asked Latimer if any of his records showed that Weste had purchased a single T-Mobile Hotspot cart. *Id.*, p. 683. Latimer replied that they did not. *Id.* On further questioning by Calfas, Latimer acknowledged that it appeared that Ramirez and Phillips had purchased the cards. *Id.*

Calfas also obtained an acknowledgment from Latimer that the evidence showed that Weste had accessed the Internet only once, on July 6, 2006, for 20 minutes." It is important to note that the government never produced any emails (neither judsonband1 nor chalcedony1 email addresses) on this date let alone any emails of a threatening nature. This establishes that the only means in which the government could link the Petitioner to any Starbucks or any other location was to use the Verizon records. The records the government should have sought, based on the government's evidence, was that of Philips and Ramirez. Without the Petitioner's name being on the Hotspot cards, it would have been even more difficult for the government to have met the burden to obtain a warrant from the court.

The government was able to tie the Hotspot cards and IP address to the particular Starbucks by issuing a subpoena to Steven's cell phone provider, Verizon. See attached subpoena. The government requested, "Any and all records, but not limited to the following information regarding cellular number (210) 834-2176, for the period of June 1, 2006 through April 30, 2007, in the name of Steven D. Weste." *Id.* As a result of the subpoena, the government was able to discover the list of phone calls by Steven, the historical cell-site location information (CSLI) for Steven, and the locations of the cell towers. No Verizon representative ever testified at trial. The CSLI was testified to at trial by Jose Arrendondo, DHS OIG, and case agent for the government. Arrendondo used the CSLI to develop a cell phone map which was used during this testimony.

The Verizon records were obtained ten months prior to the T-Mobile records, and Latimer testified in March of 2009 that it was not possible to link a particular card to a particular location. The assumption made by Latimer was that the emails had come from a specific location. The government, however, used the Verizon records to reverse engineer the T-Mobile records which, without the Verizon records, would never have allowed Latimer to conclude that the emails originated at that location. Indeed, the Verizon records provided Latimer the location and he built his computer program to assume the location. If the government had not obtained the Verizon records, the government would have continued to guess as to the location and could just as easily developed the theory that the emails originated from the hotspots in Massachussets which is where the government previously believed was the point of origin. The government needed the Verizon records to locate a crime scene rather than find the crime scene and develop the case. This type of scenario concerned Chief Justice Roberts in *Carpenter*.

REASONS FOR GRANTING THE WRIT

The Petitioner is entitled to relief because this Court announced in *Carpenter v. United States*, ___U.S.___, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018), that the government must use a warrant, in the absence of an exception such as exigent circumstances, to obtain CSLI from wireless carriers.

The Supreme Court of the United States held, on June 22, 2018, that the government must use a warrant, in the absence of an exception such as exigent circumstances, to obtain from wireless carriers a defendant's historical cell-site location information (CSLI). *Carpenter v. United States*, ___U.S.___, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018). When the government accesses CSLI from wireless carriers, such action invades a person's "reasonable expectation of privacy in the whole of his physical movements." *Id.* The government's acquisition of CSLI is "a search within the meaning of the Fourth Amendment." *Id.* Because the acquisition of CSLI is a search, the government "must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* A subpoena is insufficient. *Id.* "[T]his Court has never held that the [g]overnment may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Id.* "If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.* "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.*

In the case at bar, the government was able to tie the Hotspot cards and IP address to this particular Starbucks by issuing a subpoena to Steven's cell phone provider, Verizon, for Steven's CSLI. The government requested, "Any and all records, but not limited to the following information regarding cellular number (210) 834-2176, for the period of June 1, 2006 through April 30, 2007, in the name of Steven D. Weste." As a result of the subpoena, the government was able to discover the list of phone calls by Steven, the historical cell-site location information (CSLI) for Steven, and the locations of the cell towers. No Verizon representative ever testified at trial. The CSLI was testified to at trial by Jose Arrendondo, DHS OIG, and case agent for the government. Arrendondo used the CSLI to develop a cell phone map which was used during this testimony. Because the acquisition of Steven's CSLI was a search without exigent circumstances, the government was required to obtain a warrant supported by probable cause before acquiring these Verizon records. The subpoena was insufficient and, therefore, the obtaining of the CSLI records from Verizon by using a supboena violated the Fourth Amendment. The government may not subpoena third parties for such records because Steven had a reasonable expectation of privacy in these records.

The judgment against the Petitioner was based upon Verizon historical CSLI which was improperly subpoenaed by the government and used to place the Petitioner near a Starbucks from which threats were transmitted by a T-Mobile hot spot. This

was a violation of the Petitioner's right to due process as guaranteed by the Fifth and Fourteenth Amendments to the United States Constitution.

THIS CASE WARRANTS ORIGINAL HABEAS JURISDICTION

The case at bar presents exceptionally rare circumstances that warrant the exercise of this Court's original habeas jurisdiction. This Court's Rule 20.4(a) "delineates the standards under which" the Court will grant an original writ of habeas corpus. *Felker v. Turpin*, 518 U.S. 651, 665, 116 S.Ct. 2333, 135 L.Ed.2d 827 (1996). First, "the petitioner must show . . . that adequate relief cannot be obtained in any other form or from any other court." Sup. Ct. R. 20.4(a). Second, "the petitioner must show that exceptional circumstances warrant the exercise of the Court's discretionary powers. *Id.* (*quoting* 28 U.S.C. § 2242). The Petitioner's case satisfies both requirements, and the case at bar presents the precise circumstance in which this Court has recognized that it would be proper to exercise its original habeas jurisdiction.

The AEDPA requires that a petitioner seeking to file a successive petition for a writ of habeas corpus first request authorization in the appropriate court of appeals. 28 U.S.C. § 2244(b)(3)(A). Under § 2244(b)(3)(E), the denial of such authorization "shall not be the subject of a petition for rehearing or for a writ of certiorari." The Fifth Circuit would refuse to entertain a subsequent writ in this case given the case history and the fact that *Carpenter* has not been held to be retroactive. Such a refusal

by the Fifth Circuit would preclude this Court from reviewing the Fifth Circuit's order by writ of certiorari.

If this Court does not intervene, Mr. Weste will be forced to continue serving a sentence without having had the constitutional guarantees of a fair trial. For that reason, there is a significant risk that the Petitioner stands convicted based upon the government's illegal use of a subpoena contrary to *Carpenter*. The case at bar presents extraordinary circumstances that warrant the exercise of this Court's discretionary powers. No other state or federal forum remains to hear Mr. Weste's claims.

Under the extraordinary circumstances presented in this case, and given the new substantive constitutional law announced in *Carpenter*, this Court should not allow Mr. Weste's conviction to stand. Mr. Weste respectfully requests that the Court grant this petition for writ of habeas corpus and order the District Court below to vacate his sentence or, in the alternative, provide him with a new trial.

CONCLUSION

The petition for a writ of habeas corpus should be granted.

Respectfully submitted,

Michael C. Gross
Counsel of Record
1524 North Alamo Street
San Antonio, Texas 78205
(210) 354-1919
(210) 354-1920 Fax