IN THE

SUPREME COURT OF THE UNITED STATES

No. 23-6241

Mark Emmanuel Martinez,

Petitioner,

v. Erik A. Hooks, Secretary, North Carolina Department of Public Safety,

Respondent

PETITION FOR REHEARING OF ORDER DENYING CERTIORARI

Mark Martinez

Petitioner, pro se

1255 ~~prison~~ Camp Road

Whiteville, North Carolina, 28472

Thursday, March 14th, 2024

QUESTION PRESENTED

1. CAN THIS COURT RESOLVE A CIRCUIT SPLIT AND OVERALL UNCERTAINTY BETWEEN FEDERAL AND STATE COURTS REGARDING WHETHER OR NOT LAW ENFORCEMENT CELLULAR PHONE FORENSIC EXTRACTIONS REQUIRE EXPERT TESTIMONY UNDER FEDERAL RULE OF EVIDENCE 702 IN ORDER TO PROPERLY ADMIT THEM AS EVIDENCE?

ADDITIONAL CONSTITUTIONAL PROVISION INVOLVED

Federal Rule Of Evidence 702 reads as follows:

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if the proponent demonstrates to the court that it is more likely than not that:

(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert's opinion reflects a reliable application of the principles and methods to the facts of the case.

STATEMENT OF THE CASE

Petitioner was convicted in State Court based on two and only two pieces of evidence: A victim accusation which has since been recanted, and an allegedly accurate Forensic extraction performed on the victim's cellular phone using Cellebrite software. Petitioner challenged this forensic extraction prior to trial, due to Petitioner possessing irrefutable evidence that proves that the forensic extraction has been tampered with by law enforcement.

The State court excluded Petitioner's evidence without conducting any investigation. Petitioner has challenged this forensic extraction on appeal and in Habeas review. At every step of the way, the courts fail to resolve this problem. In fact, the courts don't even aknowledge that Petitioner is making the argument that the evidence under which he is in prison may be a fabrication.

As far as Cellebrite forensic extractions not being infallible, Petitioner is not the first to make the allegation that tampering has occurred. Petitioner does happen to be the first who can prove it.

PETITION FOR REHEARING

Cellebrite is a tool used by law enforcement to extract the contents of electronic devices. It is the most popular software used by law enforcement. The software takes an electronic device seized during an investigation and retrieves text messages, phone calls, application data, photographs, cellular tower location information, and more.

Since the beginning of its use in criminal investigations, courts have enjoyed the ease with which these extractions reveal every detail of a person's personal life, and the relative difficulty an opponent faces in crafting a defense to these extractions. Two major challenges have become the battleground in the courts:

(a) That the extractions require expert testimony under rule 702 of the Federal Rules of Evidence; and

(b) That the extraction has been altered, tampered with, manipulated, fabricated, etc.

Under Rule 702, a trial judge serves as a gatekeeper of whether or not a law enforcement agent can testify regarding these cell phone extractions, and the limitations imposed on said testimony. The end result is either the admission of the forensic extraction or its exclusion.

Circuit courts and State courts are divided on whether or not expert testimony is actually required in order to introduce these extractions, as the process is considered "rote" (United States v. Rubio, 2022 WL 17246937 (5th Cir. 2022), with "minimal prompts," (id), "the software does all the work." (id). Other courts have stated that due to "training, and therefore specialized knowledge beyond the common knowledge of the jury was required to operate, obtain, and interpret data using the program," expert testimony is required (United States v. Daniels, 625 F. Supp. 3d 1191 (U.S. Dist. Court, S.D. California, 2023) The courts are split as follows:

(a) Rule that Cellular forensic extractions (CFE's) do implicate Rule 702:

1. United States v. Daniels, 625 F. Supp. 3d 1191 (U.S. Dist. Court S.D California, 2023)
2. United States v. Wehrle, 985 F.3d 549 (7th Cir. 2021)
3. United States v. Smith, 2022 WL 17791100 (U.S. Dist. Court. S.D. Illinois, 12-16-2022)
4. United States v. McLeod, 2023 WL 4750123 (U.S. Dist. Court, S.D. California)

(b) Rule that CFE's do not implicate Rule 702:

1. United States v. Williams, 83 F. 4th 994 (5th Cir. 2023)
2. People v. Price, 193 N.E.3d 320, 2021 IL App (4th) 190043
3. United States v. Chavez-Lopez, 2019 WL 1562352 (4th Cir. 2019)

A Westlaw survey of Rule 702 in Cellebrite cases reveals that although the circuit split heavily favors the ruling that CFE's do not implicate Rule 702,

none of the cases want to answer whether Cellebrite is reliable software or not, nor do they seek testimony from the law enforcement agent regarding Cellebrite's reliability. This allows the proponent of the extraction to circumvent Rule 702. The list of cases that do not wish to "opine" on the reliability of the software is extensive, and falls on both sides of the argument:

1. United States v. Smith, 2022 WL 17741100 - court did not offer opinion of Cellebrite's reliability.
2. United States v. Wehrle, 985 F.3d 549 (7th Cir. 2021) - stated that although CFE did implicate Rule 702, the court was making no findings as to the "reliability or efficacy" of Cellebrite
3. United States v. Chavez-Lopez, 2019 WL 1562352 (4th Cir. 2019) - does not implicate Rule 702 because no testimony is being offered about "effectiveness or reliability"
4. In re D.H., 2015 WL 514336 - state that reliability findings apply to "unproven techniques or procedures that are presented as infallible" due to it giving juries a "misleading aura of certainty."
5. United States v. Ovies (9th, Cir. 2019) 783 Fed Appx. 704 - allowed Cellebrite testimony because witness did not testify to "reliability or other specialized knowledge." and stated that "without additional evidence of how Cellebrite works, we decline to reach the question of whether the introduction of Cellebrite evidence requires expert testimony".
6. United States v. Daniels, 652 F. Supp. 3d 1191 (U.S. Dist. Court, S.D. California, 2023) - the court noted that due to the absence of a duly noted expert to testify about the reliability of Cellebrite, and law enforcement's limited ability to testify as a lay witness, the Government would not be allowed to introduce any evidence obtained from the extraction.

The court also declined to opine on the reliability of Cellebrite despite its ruling.

By allowing law enforcement to testify that they followed software prompts and yielded a report, juries are given the assumption that nothing could have gone wrong. In United States v. McLeod, the dissenting judge stated that "just because a user can follow prompts from the program does not mean that expert testimony is not required or that the underlying technology is reliable."

To resolve this circuit split, one has to look at the second challenge to Cellebrite reports, and the supporting facts that show that Cellebrite reports are subject to an assortment of manipulations.

In April of 2021, the creator of an encryption application called Signal released news to the public that he and his team had found "vulnerabilities" that would allow manipulation "of the cellebrite report". To quote, in one single exploitation, one can modify "not just the Cellebrite report being created in that scan, but also all previous and future generated Cellebrite reports from all previously scanned devices and all future scanned devices in any arbitrary way (inserting or removing text, email, photos, contacts, files, or any other data) with no detectable timestamp changes or checksum failures." (https://signal.org/blog/cellebrite-vulnerabilities/) Within days of this report, Cellebrite cut off Iphone support in its software, meaning law enforcement could not perform Iphone extractions until the problem is resolved. (https://hothardware.com/news/cellebrite-physical-analyzer-software-no-longer-supports-iphones) Signal also provided data on the sheer number of vulnerabilities in the Cellebrite software. In 2012, 54 vulnerabilities existed. In 2013, 77. In 2014, 19. In 2015, the year of Petitioner's case, 29 ways existed to sabotage Cellebrite. News outlets that cover technology reported the hack.

1. Thomas Brewster, April 22, 2021 - Cops' Iphone Hacking tools Are (Sometimes) Insecure And Buggy. (https://www.forbes.com/sites/thomasbrewster/2021/04/22/cops-iphone-hacking-tools-are-sometimes-insecure-and-buggy/?sh=7fddd6822874)

2. Lorenzo Bicchierari, Joseph Cox, April 27, 2021 - Cellebrite pushes update after Signal owner hacks Device (https://vice.com/en/article/qj8pjm/cellebrite-pushes-update-after-signal-owner-hacks-device)

3. Joe Tidy, April 22, 2021 - Signal slams Cellebrite security company over alleged security holes (https://www.bbc.com/news/technology-56816357)

4. Alex Hern, April 22, 2021 - Signal Founder: I hacked police phone-cracking tool Cellebrite (https://www.theguardian.com/technology/2021/apr/22/signal-founder-I-hacked-police-phone-cracking-tool-cellebrite)

5. Brin Barrett, April 24, 2021 - Security News This week: Signal's founder hacked a notorious phone-cracking Device (https://www.wired.com/story/signal-cellebrite-hack-app-store-scams-security-news)

6. Steve Dent, April 22, 2021 - Signal Hacked cellebrite's phone hacking software used by law enforcement (https://www.endgadget.com/signal-hacked-cellebrite's-i-phone-hacking-device-092006603.html)

Berkeley Law school's Technology Law & Public Policy Clinic as well as Stanford Law School's Center for Internet Society also did extensive coverage and assessed the legal ramifications of this problem. see Lucas Ropek, April 27, 2021 - Signal's Cellebrite hack is already causing grief for the law (https://gizmodo.com/signals-cellebrite-hack-is-already-causing-grief-for-th-1846773797) see also Rianna Pfefferkorn (https://cyberlaw.stanford.edu/blog/2021/05/I-have-lot-say about-signal%of2%80%995-cellebrite-hack).

What this means is that there is an assortment of ways to alter a Cellebrite extraction. If one were to do a survey of challenges to cellebrite reports, one would notice that the challenges are by defendants with cases prior to April 2021, when this was finally revealed to the public. This means that defendants were making observations about changes or inconsistencies in their cases' forensic extractions that may possibly be the result of

tampering. See the following:

1. United States v. Childress, 2021 WL 2972868 - court stated that defendant's allegations of tampering "lack adequate support"

2. United States v. Rubio, 2022 WL 17246937 (5th Circuit, 2022) "to the extent [Petitioner] fears any portion of the report was manipulated, the officer most closely involved was available for cross examination"

3. United States v. McLeod, 2023 WL 4688798 (U.S. Dist. Court, S.D. California) "[Petitioner] presented evidence that the cellebrite device used can produce significant errors, including not acquiring files and misreporting data"

4. United States v. McLeod, 2023 WL 4750123 (U.S. District Court, S.D. California) 2 cellebrite reports were made of the same device, yet both were not identical. Also, "[Petitioner] identified specific messages that victim authored but that the Cellebrite report attributed to Petitioner." " Government allowed Detective to offer incomplete and unreliable extraction report, making Petitioner appear guilty of conversations he did not have."

5. Christian v. United States, 2020 WL 3244008 (U.S. Dist Court, E.D. Virginia, Alexandria Division) "Christian states that the Cellebrite extraction report contained several notations of phone activity which were dated after the phone was in Gavernment custody." The court found that the allegations were "devoid of further explanation"

6. United States v. Hernandez, 2023 WL 6121981 (US Dist. Court, S.D. Florida) Forensic specialist observed that the cell phone contents had changed while in police custody.

7. State v. Wright, 2023 WL 5317754 (COA of Ohio, Second district, Miami County) Forensic Specialist testified that "various cached files and other objects were deleted from the phone when it was in the Sheriff's possession", and that "Due to a fault in the Cellebrite program that [was] used, all photos residing

in Google photos .... were incorrectly labeled as deleted."

8. United States v. Glatz, 2023 WL 4492405 (U.S. District Court, E.D. Tennessee) Defendant asserts that he "has proven that the FBI planted their own illegal images on the phone, due to the images [not being] on the cell phone when it was seized."

9. People v. Delhaye, 2021 IL App (2d) 190271 (Appellate Court of Illinois, Second District) court found Defendant's arguments with respect to purported deficiencies in the data from the Cellebrite report unpersuasive.

10. State v. Holmes, 2022 WL 16736968 (Court of Crim. Appeals of TN, at Knoxville) Investigator testified that a former KPD officer took possession of Defendant's phone to perform a data extraction. Investigator acknowledged that officer "has been indicted for falsifying records a KPD."

11. The DOJ released a news report in 2022 (DOJ 22-300, 2022 WL 3281629) that states that a Nevada woman presented the government with a PDF cellebrite report which fooled a judge and her defense counsel. Forensic analysis revealed that the report had been falsified.

Cell phone extractions also face manipulation after they are generated. Cell phone extractions are produced as .PDF files. These files can be edited completely divorced from whether or not a reliable Cellebrite extraction was performed. see US v. Jean-Claude, 2022 WL 2334509 - during cross examination, mobile phone forensics examiner testified that cell phone extraction reports are "PDF's that can be made editable ... using the right software" and that it is possible to "write over" the contents of the reports. A Westlaw survey of PDF tampering yields an incredible amount of cases where .PDF files were fabricated.

As shown, Cellebrite reports are delicate pieces of evidence, subject to tampering. It is why they must be subject to reliability determinations, instead of blindly accepted as accurate and infallible to a degree that prejudices

defendants by hindering "vigorous cross examination, presentation of contrary evidence" as described by Daubert v. Marrell Dow Pharmaceuticals, Inc. 43 F. 3d 1311, 1317 (9th Cir. 1995).

Petitioner's Appendix G in the Certiorari Petition presented to this court shows the contravening evidence to the Cellebrite report in his case. The report itself shows dates of creation of files during the time that the Detective seized the phone for forensic analysis. This is the same problem expressed in Christian v. United States.

Petitioner's Appendix G contains proof that the Detective in the case altered the Cellebrite report. The state court illegally excluded this evidence without explanation. There were no reliability determinations made to the State's evidence, nor was any explanation given for why the report on its own reveals that it was modified. This evidence proves that Petitioner is innocent.

CONCLUSION

Cellebrite reports are based on incredibly useful technology. When proffered in conjunction with other evidence such as an extraction by a different forensic program, cell phone provider records, witness testimony, photographs of the phone's contents, or the evidence in the phone itself, the report can survive evidentiary challenges. It is quite possible that the defendants in the cases named above are being truthful about their allegations against these forensic extractions. They may never get the opportunity to prove it. This problem will persist as long as the Supreme Court doesn't step in to correct this Circuit Split. For that reason, Petitioner asks that this court reconsider granting Certiorari.

Respectfully Submitted, Thursday, March the 14th, 2024.

Mark Emmanuel Martinez

1255 Prison Camp Road

Whiteville, North Carolina, 28472

3/14/24

CERTIFICATE OF SERVICE

I certify that on this day, the 14th of March, 2024, I placed the foregoing Petition For Rehearing of Order Denying Certiorari in the exclusive care of the United States Postal service. I used a first class envelope, postage prepaid, and submitted it to the prison mailroom. I simultaneously sent a copy of the foregoing motion to the following Respondent in the case:

Ms. Kristin J Uicker
NC Department of Justice
ATTN: Appellate Section
P. O. Box 629
Raleigh, NC 27602

Respectfully Submitted,
3-14-2024
Mark Emmanuel Martinez
1255 Brison Camp Road
Whiteville, NC 28472

CERTIFICATE OF PRO SE PETITIONER

I hereby certify to the Supreme Court of the United States that, pursuant to Rule 44.2 of the Rules of the Supreme Court, this petition is presented in good faith and not for the intention of delaying judgement. I also certify that it comports with and is restricted to the presentation of a Substantial Grand not previously raised.

Respectfully Submitted,

March the 14th, 2024

Mark Emmanuel Martinez

1255 Prison Camp Road

Whiteville NC 28472

Mark Martinez