

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

Defendant.

**DEFENDANT [REDACTED]'S MOTION *IN LIMINE* TO PRECLUDE THE
GOVERNMENT FROM OFFERING NON-EXPERT TESTIMONY AND
EVIDENCE OBTAINED FROM A FORENSIC EXAMINATION OF
CO-DEFENDANT [REDACTED]'S IPHONE AND ANY OTHER PHONE
PRESENTING SIMILAR ISSUES**

Respectfully submitted,

**JOSHUA J. HOROWITZ, ESQ.
HOROWITZ TECH LAW P.C.**

734 Franklin Ave., #605
Garden City, New York 11530
Tel: (212) 203-9011
joshua.horowitz@techlawny.com

**STEPHEN TURANO
TURANO LAW**

275 Madison Avenue, 35th Fl.
New York, New York 10016
Tel: (917) 594-5666
sturano@turanolaw.com

Counsel for Defendant [REDACTED]

Dated: June 30, 2025

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

I. FACTUAL AND PROCEDURAL BACKGROUND 1

 The Seizure of Ms. ██████’s Two Cell Phones..... 1

 The GrayKey File System Extraction of Ms. ██████’s Cell Phone 2

 Cellebrite Analysis of the Extracted Data from ██████’s iPhone 3

 The “Savage” Group Chat From the ██████ iPhone 4

 The Deleted Group Chat 7

 Other Memorialization of the “Savage” Group Chat in the ██████ iPhone..... 8

 The Government’s Lack of Notice for a Cell Phone Forensics Expert..... 8

 Other Cell Phone Forensic Evidence and ESI as Trial Evidence..... 10

II. ARGUMENT..... 10

 A. The Federal Rules of Evidence Preclude the Introduction Non-Expert
 Testimony and Evidence Relating to the ██████ iPhone at Trial 10

 B. If the Court Permits The Government to Offer Evidence from the ██████
 iPhone it Should Hold a *Daubert* Hearing..... 16

III. CONCLUSION..... 19

TABLE OF AUTHORITIES

Cases

<i>Daubert v. Merrell Dow Pharmaceuticals, Inc.</i> , 509 U.S. 570 (1993).....	17, 18
<i>Kumho Tire Co. v. Carmichael</i> , 526 U.S. 137 (1999).....	17
<i>United States v. Ashburn</i> , 88 F. Supp. 3d 239, 242 (E.D.N.Y. 2015)	17, 18
<i>United States v. Cuti</i> , 720 F.3d 453, 459 (2d Cir. 2013)	11, 12, 14
<i>United States v. Daskal</i> , 21-Cr-110 (NGG) (LB), 2023 WL 9424080 (E.D.N.Y. Jul. 12, 2023)	14
<i>United States v. Jimenez-Chaidez</i> , 96 F.4th 1257 (9 th Cir. 2024)	14, 15, 16
<i>United States v. Marsh</i> , 568 Fed. Appx. 15 (2d. Cir. 2014).....	12, 13
<i>United States v. Natal</i> , 849 F.3d 530, 536 (2d Cir. 2017)	11, 12
<i>United States v. Ray</i> , No. 20-CR-110 (LJL), 2022 WL 817270, at *1 (S.D.N.Y. Mar. 16, 2022)	14
<i>United States v. Rigas</i> , 490 F.3d 208, 224 (2d Cir. 2007)	11
<i>United States v. Saipov</i> , No. 17-CR-722 (VSB), 2023 WL 4199415, at *11 (S.D.N.Y. June 27, 2023)	14
<i>United States v. Wehrle</i> , 985 F.3d 549, 554 (7 th Cir. 2021)	16
<i>United States v. Yeley-Davis</i> , 632 F.3d 673, 684 (10 th Cir. 2011)	11

Other Authorities

Fed. R. Evid. 701 advisory committee's note, 2000 amend.....	11
--	----

Rules

Fed. R. Crim. P. 16	1, 9, 16
Fed. R. Evid. 701	1, 10
Fed. R. Evid. 701 (c).....	12, 14
Fed. R. Evid. 702	passim
Fed. R. of Crim. P. 16(a)(1)(G)	9
Local Criminal Rule 16.2.....	9

PRELIMINARY STATEMENT

Defendant [REDACTED] (“Mr. [REDACTED]” or “[REDACTED]”) respectfully submits this motion *in limine*, seeking to preclude the government from offering cell phone forensic evidence at trial through non-expert testimony. Specifically, Mr. [REDACTED] seeks to preclude the government from offering non-expert testimony relating to, and evidence obtained from a forensic examination of one of co-defendant [REDACTED]’s (“Ms. [REDACTED]” or “[REDACTED]”) cellular telephones and any other phone presenting similar issues.

The government has failed to provide any notice of its intent to offer expert testimony relating to the forensic extraction of cellular devices that it intends to rely upon at trial. It is apparently the government’s view that the introduction of such evidence at trial does not require expert testimony. Given the complexity of the cell phone forensic evidence at the heart of this case, Federal Rules of Evidence 701, 702 and Fed. R. Crim. P. 16 dictate otherwise, mandating preclusion of the government’s non-expert cell phone forensic testimony and evidence at trial.

I. FACTUAL AND PROCEDURAL BACKGROUND

The Seizure of Ms. [REDACTED]’s Two Cell Phones

In the late evening of December 27, 2023, NYPD officers located co-defendant [REDACTED] at her parents’ home in the Bronx and asked her to accompany them to the 107th precinct in Queens to be interviewed in connection with a homicide investigation.¹ Law enforcement officers at the 107th precinct took possession of Ms. [REDACTED]’s cellular

¹ ECF Dkt. No. 91 at pg. 6. Given the Court’s extensive familiarity with the factual background pertaining to the seizure of Ms. [REDACTED]’s cellular phones, having presided over a suppression hearing and issuing a thoroughly reasoned 27-page opinion, this memorandum contains a very brief recitation of the facts pertaining to the seizure of Ms. [REDACTED]’s cellular phones.

telephones at the conclusion of her interview at approximately 1:40 A.M. on December 28, 2023.² Less than 18 hours later, law enforcement obtained a search warrant authorizing the search of Ms. [REDACTED]'s two cell phones.³

The GrayKey File System Extraction of Ms. [REDACTED]'s Cell Phone

Forensic extractions and data obtained from each of Ms. [REDACTED]'s cell phones were produced in the government's January 9, 2025 discovery production at USAO_277453. The cell phones were further sub-labeled as "Cellphone #5 (107 pct)" and "Cellphone #6 (107 pct)." (Horowitz Decl. at ¶ 3). The cell phone identified as Cellphone #5 is an iPhone 14 Pro Max running iOS version 16.6 and named "[REDACTED]" (hereafter "the [REDACTED] iPhone" or "the Phone")⁴. (Morrissey Decl. at ¶ 13). The cell phone identified as Cellphone #6 is an iPhone XS running iOS 16.5 and named "[REDACTED]". (Morrissey Decl. at ¶ 14).

On January 2, 2024 at approximately 8:29 AM⁵, Special Agent [REDACTED] began the process of extracting the contents of the [REDACTED] iPhone utilizing a tool available only to law enforcement called "GrayKey" developed by a company called GrayShift. (Morrissey Decl. at ¶ 15). Although its precise inner-workings are a closely guarded

² *Id.* at pg. 12.

³ *Id.*

⁴ For purposes of this motion, data recovered from Cellphone #5 ("[REDACTED]'s iPhone" or "the Phone") is the operative data being discussed because a forensic extraction and examination of the Phone's data resulted in the recovery of the government's core evidence against Mr. [REDACTED], which are telegram messages purportedly involving [REDACTED], [REDACTED], and [REDACTED] from a group chat called "Savage". Ms. [REDACTED]'s outgoing messages to that group were not recovered. Cellphone #6 was not identified as containing responsive data.

⁵ The timestamp in the GrayKey Progress Report produced in discovery (Exhibit D to Morrissey Decl.) indicates that the extraction process began on January 2, 2024 at 13:29:16 UTC or Universal Coordinated Time. Converting to Eastern Standard Time (EST) requires subtracting 5 hours.

secret, GrayKey essentially works by exploiting a security vulnerability in the Apple iOS operating system to permit the installation of a software agent on the phone, that then permits the full contents of the phone to be extracted. (Morrissey Decl. at ¶ 16).

The [REDACTED] iPhone filesystem extraction was fully completed on January 2, 2024 at approximately 5:11 P.M, nearly 9 hours after the process began.⁶ During that process, GrayKey extracted a full copy of the [REDACTED] iPhone's full filesystem. (Morrissey Decl. at ¶ 17).⁷ A full filesystem extraction differs from a hardware level bit-for-bit copy because it does not include the entire content of the iPhone's internal storage. (*Id.*). Because GrayKey is a proprietary, secretive tool available only to law enforcement, the forensic reliability of data obtained by it, and specifically Telegram data, cannot be verified independently without access to the tool. (Morrissey Decl. at ¶ 18).

Cellebrite Analysis of the Extracted Data from [REDACTED]'s iPhone

Once the Gray Key file system extraction was completed, forensic analysis of the extraction was conducted utilizing Cellebrite, a leading cell phone forensic analysis tool. (Morrissey Decl. at ¶ 19). It appears that Cellebrite analysis of the [REDACTED] iPhone was completed on or about January 9, 2024.⁸ (Horowitz Decl. at ¶ 4). Analyzing the output of the GrayKey filesystem extraction using Cellebrite results in the creation of a .UFDR file,

⁶ GrayKey Extraction Report (Ex. D to Morrissey Decl.), indicates that the extraction was completed at 22:11:09 UTC on January 2, 2024.

⁷ *See also*, Full File System Extraction, Cellebrite Digital Intelligence Glossary, available at: <https://cellebrite.com/en/glossary/full-file-system-extraction-mobile-device-forensics/> (last accessed June 26, 2025).

⁸ The Cellebrite analysis report itself does not contain the precise date and time that the analysis was conducted; however the filename of the .UFDR file provided in discovery is Cellphone_5_2024-01-09_Report.ufdr; that file also appears to have been created/modified on January 9, 2024.

i.e. a Universal Forensic Extraction Device Report.⁹ (Morrissey Decl. at ¶ 20). That file ultimately contains the forensically extracted and analyzed data in a “human-readable” format and is the format in which it is produced to defense counsel. (*Id.*) While the content of the UFDR file is “human-readable”, review and interpretation of the data it contains requires specialized skill and expertise. (*Id.*)

The processes underlying Cellebrite’s analysis of the phone data are complex. (Morrissey Decl. at ¶ 21). Cellebrite programmatically parses the iPhone system files from various databases and files contained within the phone, such as SQLite databases, plists (property lists), system log files, system library files, etc. (*Id.*). Adding to the complexity of this process is that some of the data that Cellebrite parses from various databases contained in an iPhone is stored in a non-human readable format called BLOB, or Binary Large Object.¹⁰ (Morrissey Decl. at ¶ 22). That data needs to be decoded in order to be readable, a process programmatically undertaken by Cellebrite. (*Id.*). In short, there is a lot going on “under the hood” when a Cellebrite analysis of a cell phone forensic extraction is performed. It is a process that is technologically complex; analyzing and interpreting the resulting data is a process that requires specialized training and expertise.

The “Savage” Group Chat From the [REDACTED] iPhone

Central to the government’s case against Mr. [REDACTED] is a purported Telegram group chat that was recovered from law enforcement’s forensic examination of the [REDACTED]

⁹ UFDR – Mobile Device Forensics, Cellebrite Digital Intelligence Glossary, available at: <https://cellebrite.com/en/glossary/ufdr-mobile-device-forensics/> (last accessed June 26, 2025).

¹⁰ SQLite BLOB, SQLite Tutorial, available at: <https://www.sqlitetutorial.net/sqlite-blob/> (last accessed June 26, 2025).

iPhone. Indeed, throughout the dozens of search warrant applications submitted by the government in connection with its investigation of this case, it relied upon this chat and related messages from the [REDACTED] iPhone.¹¹ It is anticipated that these messages will be the foundation of the government's case against Mr. [REDACTED] at trial.

What the government's warrant applications fail to disclose is that the Telegram messages it so heavily relies upon were *not* recovered directly from the [REDACTED] iPhone's Telegram messaging application but were instead recovered from an SQLite database contained in the iPhone called "knowledgec.db." (Morrissey Decl at ¶ 24). The knowledgec.db database file stores a variety of information about an iPhone's usage, background processes, and other information about the operation of the phone and is of significant value in mobile forensic examinations. (*Id.*).¹² In other words, the Knowledgec Database file keeps a detailed journal of a phone user's activity and system processes, for example, login events to the phone (successful or failed), screen status, and even minute bits of data such as whether a phone's backlight was on, or even if the phone was in portrait mode or landscape mode at a particular time.¹³

¹¹ The content of those messages are annexed to the Morrissey Decl. as Exhibit E, excerpted from a May 14, 2025 search warrant application produced in discovery at USAO_282786-282846. Because the content of that warrant application is designated as APO material under the Protective Order in this matter (ECF Dkt. No. 52), it is being redacted from the ECF-filed version of this motion.

¹² See also, Knowledgec Database / Knowledgec.db, Cellebrite Digital Intelligence Glossary, available at: <https://cellebrite.com/en/glossary/knowledgec-database-knowledgec-db/> (last accessed June 27, 2025).

¹³ *Id.*, see also I Beg to DFIR – How Knowledgec.db Can Impact Your Investigation, available at: <https://cellebrite.com/en/episode-5-nothing-to-see-here-i-beg-to-dfir-how-knowledgec-db-can-impact-your-investigation/> (last accessed June 27, 2025).

Germane to the issues presented here, the database also stores application notifications.¹⁴ Indeed, the “Savage” Group chat recovered from the Knowledgec.db in the [REDACTED] iPhone contains only messages involving users with the name “[REDACTED]” and “[REDACTED] ([REDACTED])”, who the government attribute to [REDACTED] and [REDACTED], respectively. Significantly, the “Savage” group chat does not contain any outgoing messages from Ms. [REDACTED]. It is therefore an incomplete rendition of the purported group conversation. That is because when messages were sent to the group chat, which the [REDACTED] iPhone was a member of, that phone would receive an incoming notification of the new message received. (Morrissey Decl. at ¶ 25). That notification was then recorded in the Knowledgec.db file, which would include the text of the incoming message. (*Id.*). Outgoing messages from the [REDACTED] iPhone were not recorded in the database because they did not result in a notification on the phone. (Morrissey Decl. at ¶ 26).

In its most recent warrant applications, the government demonstrates a fundamental misunderstanding of the reasons for the lack of outgoing messages from Ms. [REDACTED] on the [REDACTED] iPhone, stating:

“when viewing an individual’s Telegram account on their mobile device, often times the only visible messages are incoming messages, and the outgoing messages are not saved on the app. Thus, [REDACTED] may have sent messages over Telegram to [REDACTED] and/or [REDACTED] that law enforcement officers are unable to see based solely on their review of the [REDACTED] Cellphones.”¹⁵

¹⁴ *Id.*, see also Scott Koenig, DFIR Review: iOS Knowledgec.db Notifications, November 3, 2022, available at: <https://dfir.pubpub.org/pub/g2v1z97i/release/1> (last accessed June 27, 2025).

¹⁵ May 14, 2025 Sworn Declaration of United States Secret Service Officer [REDACTED], USAO_282801 at fn. 3, Exhibit E to Morrissey Declaration.

That is not the case here and is indeed inconsistent with the government's own cell phone forensic evidence recovered from the [REDACTED] iPhone, which contains approximately 195 *other* Telegram group chats recovered from the [REDACTED] iPhone, the vast majority of which all contain outgoing messages from the username "[REDACTED]" dating all the way back to August 26, 2019. (Morrissey Decl. at ¶ 27). In the "Savage" group chat, the absence of any outgoing messages from [REDACTED] is an anomaly, not the norm, as misstated by the government.

The government's own fundamental misunderstanding of the import of Telegram messaging notifications recovered from the knowledgec.db file demonstrates, *a fortiori*, the need for expert testimony to lay an appropriate foundation for and to explain the import of the complex technical forensic data recovered from the [REDACTED] iPhone in this case. If the government misunderstands the import of its own forensic investigative data, how can a lay jury be expected to understand it without the aid of expert testimony?

The Deleted Group Chat

Beginning on December 28, 2023, in the [REDACTED] iPhone there was a portion of a group chat involving [REDACTED], [REDACTED] ([REDACTED]) and [REDACTED] recovered that Cellebrite indicates was deleted. (Morrissey Decl. at ¶ 28). This portion of the chat was recovered from a separate location within the [REDACTED] Phone, an SQLite database from within the Telegram data folder called "db_sqlite", which is the main Telegram database file and is completely different from the knowledgec.db file. (Morrissey Decl. at ¶ 29).¹⁶

¹⁶ See also, Lukas Jaeckel, Michael Spranger, Dirk Labudde: Forensic Analysis of Telegram Messenger on iOS smartphones, Forensic Science International: Digital Investigation, March 2025, available at: <https://www.sciencedirect.com/science/article/pii/S2666281725000058?via%3Dihub> (last accessed June 30, 2025).

Notably, the portion of this chat that was recovered contains outgoing messages from [REDACTED], again inconsistent with the government's prior representation that "outgoing messages are not saved on the [Telegram] app."¹⁷ The recovery of deleted Telegram messages or any deleted data from an iPhone's databases is a complex process that requires parsing together information from various database tables to piece together the deleted information. (Morrissey Decl. at ¶ 30). Given the complexity of this process, testimony about these messages also requires a cell phone forensics expert to lay an appropriate foundation for and to provide an opinion to the jury on the import of the government's forensic data. The government's lack of appropriate expert notice precludes it from offering this evidence at trial.

Other Memorialization of the "Savage" Group Chat in the [REDACTED] iPhone

In addition to the knowledgedb file, the "Savage" group chat (and other fragmented conversations) are stored in a separate location of the [REDACTED] iPhone that appear to be recorded user notifications from an application called DuetExpertCenter. (Morrissey Decl. at ¶ 31). While the location from which these messages were recovered differs from the knowledgedb, they are nevertheless stored phone user notifications, and the reasons why expert testimony is required to admit them at trial remain the same. (Morrissey Decl. at ¶ 32).

The Government's Lack of Notice for a Cell Phone Forensics Expert

On June 13, 2025, counsel for Mr. [REDACTED] e-mailed the government, noting that Mr. [REDACTED] had not received any expert disclosures, and inquiring as to whether the government intended to introduce any expert witness testimony at trial. (Horowitz Decl.

¹⁷ USAO_282802 *supra* at n. 15.

at ¶ 5). On June 14, 2025, the government responded with an expert disclosure for Andrew Petersohn, a cell site location expert, whose is expected to testify about the interaction between cellular telephones and the cell network, and specifically about his findings and opinions with respect to location data from a variety of cell phones. (Horowitz Decl. at ¶ 6; Gov. June 14, 2025 Expert Disclosure, Annexed to Horowitz Decl. as Exhibit I).

Absent, however, from the government's expert disclosure is any cell phone forensics expert who can lay an appropriate foundation for the [REDACTED] iPhone evidence and who can testify as to their expert opinion on the import of that evidence at trial.

The Court did not set a timeline by order for the timing of expert disclosures.¹⁸ Thus, the operative rule governing the timeline for expert disclosures is Local Criminal Rule 16.2, which states that the government “must make any disclosures required by Fed. R. of Crim. P. 16(a)(1)(G) at least 60 days prior to trial, and the defense must make any such disclosures at least 30 days prior to trial.”¹⁹ The defense has complied with its obligations by serving timely expert notice on June 27, 2025 of its intent to call Sean Morrissey, a cell phone forensics expert at trial. (Horowitz Decl. at ¶ 7).

¹⁸ The Court's January 27, 2025 Scheduling Order (ECF Dkt. No. 63) does not set a timeline for expert disclosures. The Court recently reaffirmed the deadlines set forth in its January 27, 2025 Scheduling Order, stating “[t]he deadlines listed at Docket 63 remain in place.” ECF Dkt. No. 122, June 10, 2025 Scheduling Order.

¹⁹ SDNY Local Criminal Rule 16.2 Timeline for Expert Discovery. Under Fed. R. Crim. P. 16, the government's expert disclosure requirements are triggered upon defense request, which was accomplished by e-mail to the government on June 13, 2025. While that request was made closer to trial than the 60-day cutoff point would have otherwise been, nevertheless the government has declined to notice a cell phone forensics expert for trial. The late request for disclosures does not excuse the government's failure to timely notice an expert in response to the defense request.

For strategic or whatever reasons, the government declined to appropriately notice a cell phone forensics expert to testify about data and evidence critical to its case. We are now well-beyond the window within which the government may notice a cell phone forensics expert for trial. Because the government has failed to appropriately notice an expert, it should be precluded from offering evidence from the [REDACTED] iPhone at trial.

Other Cell Phone Forensic Evidence and ESI as Trial Evidence

It is clear from the government's warrant applications in this case that the "Savage" group chat and other data recovered from the [REDACTED] iPhone is the cornerstone of the government's case against Mr. [REDACTED]. There are however a multitude of other cell phone forensic extractions that were performed by the government in connection with its investigation of this case. To the extent the government intends to offer similar evidence from any other cell phone forensic extraction performed during its investigation, it should be precluded from doing so because it has failed to notice an appropriate expert for the introduction of such evidence at trial.

II. ARGUMENT

A. The Federal Rules of Evidence Preclude the Introduction Non-Expert Testimony and Evidence Relating to the [REDACTED] iPhone at Trial

Federal Rule of Evidence 701 allows lay opinion testimony only to the extent that the testimony is:

(a) rationally based on the witness's perception; (b) helpful to clearly understanding the witness's testimony or to determining a fact in issue; and (c) not based on scientific, technical, or other specialized knowledge within the scope of Rule 702.

The last requirement is designed to "eliminate the risk that the reliability requirements set forth in Rule 702 will be evaded through the simple expedient proffering of an expert in lay witness clothing." Fed. R. Evid. 701 advisory committee's note to

2000 amend.; see *United States v. Rigas*, 490 F.3d 208, 224 (2d Cir. 2007). “Lay opinion under Rule 701 must be limited to opinions that ‘result[] from a process of reasoning familiar in everyday life.’” *United States v. Cuti*, 720 F.3d 453, 459 (2d Cir. 2013) (quoting Fed. R. Evid. 701 advisory committee's note, 2000 amend.).

In a separate, but instructive context, the Second Circuit has held that testimony relating to cell phone towers requires expertise and thus must be offered through expert testimony. *United States v. Natal*, 849 F.3d 530, 536 (2d Cir. 2017). While cell tower technology differs from the cell phone forensic technology at issue here, the Second Circuit’s reasoning is instructive in this context. The Second Circuit reasoned that “testimony concerning how cell phone towers operate constituted expert testimony *because it involved specialized knowledge not readily accessible to any ordinary person.*” *Id.* quoting *United States v. Yeley-Davis*, 632 F.3d 673, 684 (10th Cir. 2011) (emphasis added).

The Second Circuit in *Natal* held that the following areas of testimony on how cell phone towers operate did not “result[] from a process of reasoning familiar in everyday life[.]” *Cuti*, 720 F.3d at 459:

“that a cell phone will connect to the tower with the strongest available signal, which may not be the closest tower; that factors such as radio interference, tower availability, and the line of sight between a phone and a tower affect the tower to which a cell phone connects; and that the phone handset determines which signal is strongest.”

The Second Circuit held that these areas of testimony relating to the operation of cell towers were “based on scientific, technical, or other specialized knowledge within the scope of Rule 702.” *Natal*, 849 F.3d at 537.

Analogous here, any testimony and evidence offered from the [REDACTED] iPhone (and other cell phones) are arguably even more complex and falls further outside of the scope of “a process of reasoning familiar in everyday life” than the categories of testimony relating to the operation of cell towers delineated as “expert” by the Second Circuit in *Natal. Cuti*, 720 F.3d at 459.

Here, specifically with respect to the [REDACTED] iPhone, law enforcement’s ability to break into the phone and perform a full file system extraction of its contents using a law-enforcement-only tool (Graykey); its analysis of that file system extraction using Cellebrite; the forensic recovery of portions of Telegram conversations from incoming user notifications to the [REDACTED] iPhone within the KnowledgeC database file and DuetExpertCenter user notifications file; and the recovery of deleted portions of a conversation from the [REDACTED] iPhone’s Telegram database file, among other evidence, are anything but the “result[] from a process of reasoning familiar in everyday life[,]” *Cuti*, 720 F.3d at 459. They instead require opinions “based on scientific, technical, or other specialized knowledge within the scope of Rule 702.” Fed. R. Evid. 701 (c). The government should be precluded from offering non-expert evidence and testimony relating to the cell phone forensic extraction of the [REDACTED] iPhone and any other cell phone forensic extractions involving similar issues that it intends to rely upon at trial.

While the Second Circuit has deemed certain testimony relating to Cellebrite forensic analysis as non-expert within a certain limited context, the circumstances here and complexity of the analysis are markedly different, warranting a different conclusion. *United States v. Marsh*, 568 Fed. Appx. 15 (2d. Cir. 2014). The Second Circuit described the scope of permissible non-expert testimony in *Marsh* as follows:

“Special Agent Tortorella explained his training in the use of Cellebrite technology to retrieve text messages and other data from a cellular phone; described how he used Cellebrite to do so in this case; and testified that he confirmed the results by checking the messages on the phone itself. He then testified to the contents of the messages retrieved from the phone.

Tortorella did not purport to render an opinion based on the application of specialized knowledge to a particular set of facts; *nor did his testimony turn on or require a technical understanding of the programming or internal mechanics of the technology.*”

Marsh at 17, (emphasis added).

In stark contrast to the evidence considered by the Second Circuit in *Marsh*, the evidence at issue here, particularly from the [REDACTED] iPhone is substantially more complex and triggers the requirements of Fed. R. Evid. 702. As an initial matter, the content of the [REDACTED] iPhone was extracted using GrayKey, a technology that did not even exist at the time that *Marsh* was decided.²⁰ Utilizing the filesystem extraction obtained from GrayKey, an analysis of the phone’s extracted content was performed using Cellebrite. This is a complex process that requires parsing data from various system files and databases stored within the phone. (Morrissey Decl. at ¶¶ 21 – 22).

But it is most critically the location from which the “Savage” group chat and other messaging data were recovered from within the [REDACTED] iPhone that tips the scales to differentiate this case from *Marsh* and the other (non-binding) District Court cases that have followed it.²¹ The fact that fragments of these messages were recovered from the

²⁰ See, Thomas Reed, Malware Bytes Labs: GrayKey iPhone Unlocker Poses Serious Security Concerns, March 15, 2018, available at: <https://www.malwarebytes.com/blog/news/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns> (last accessed June 29, 2025).

²¹ Several District Courts within the Southern and Eastern District have followed the reasoning in *Marsh*: ; *United States v. Saipov*, No. 17-CR-722 (VSB), 2023 WL

KnowledgeC database and other user notifications from the DuetExpertCenter necessarily require specialized technical knowledge and expertise to explain to a lay jury. Indeed, even the government has demonstrated a fundamental misunderstanding of the significance of the locations from which these messages were recovered. (Morrissey Decl. at ¶ 27).

This is not a case of plug it in, download it, and read the content; this is a case in which an expert opinion is required as to the import of forensically recovered data from the cell phone's user notifications within the knowledgc.db file and DuetExpertCenter. The subject matter is a far cry from "a process of reasoning familiar in everyday life." *Cuti*, 720 F.3d at 459 (internal quotations omitted). It is instead testimony that requires "scientific, technical, or other specialized knowledge within the scope of Rule 702." Fed. R. Evid. 701(c). The government has failed to appropriately notice an expert and should be precluded from offering such testimony and evidence from the [REDACTED] iPhone at trial.

The Court should look to the reasoning of a recent Ninth Circuit decision considering the issue of whether the introduction of cell phone forensic evidence requires expert testimony at trial. *United States v. Jimenez-Chaidez*, 96 F.4th 1257 (9th Cir. 2024). In *Jimenez-Chaidez*, the majority ultimately held that the introduction of cell phone forensic evidence in that case did not require expert testimony. However, the majority also noted that:

4199415, at *11 (S.D.N.Y. June 27, 2023); *United States v. Ray*, No. 20-CR-110 (LJL), 2022 WL 817270, at *1 (S.D.N.Y. Mar. 16, 2022); *United States v. Daskal*, 21-Cr-110 (NGG) (LB), 2023 WL 9424080 (E.D.N.Y. Jul. 12, 2023). These cases are all factually distinct from the instant case because the complexities surrounding the cell phone forensic evidence from the [REDACTED] iPhone in this case make it categorically different.

“Our decision today does not foreclose that there may be cases involving Cellebrite or other similar technology that do require expert testimony, particularly where the functionality or reliability of the technology is challenged or otherwise at issue. That simply is not this case. The Government limited the scope of Agent Edasi's testimony to his use of the Cellebrite software and his perceptions of the data that the software produced *that are readily understandable without having him opine about the software's technical processes or reliability or other issues that require specialized knowledge.*”

Jimenez-Chaidez, 96 F.4th at 1269 (emphasis added).

The instant case is the opposite: the technical expertise and specialized knowledge required to explain the import of Telegram messaging fragments recovered from the KnowledgeC Database file and other user notification locations within the [REDACTED] iPhone is not something readily understandable – certainly not to a lay jury, and even the government has demonstrated a fundamental misunderstanding of it.

Rather, given the technical complexities of the issues here, the Court should look to the dissent in *Jimenez-Chaidez*, which sensibly analyzes the admissibility of complex cell phone forensic evidence proffered as lay testimony. *See, Jimenez-Chaidez*, 96 F.4th 1257 at 1270 (Bennet, D.J.²²) (dissenting in part).

The dissent noted that a special agent's trial testimony:

“crossed the threshold into ‘expert’ territory when he discussed the technical aspects of data parsing and analysis and when he explained his findings therefrom. This is because the process of and conclusions drawn from digital evidence analysis required “demonstrable expertise.” Indeed, Edasi testified that he underwent substantial training in order to perform data analysis. Moreover, Edasi testified that cellphone analysis required him to “interpret[] the evidence” and translate it “from a digital code to a legible end-user language.” This information is not within “the common knowledge of the average layman.” *Id.* at 1273 (internal citations omitted).

²² Hon. Richard D. Bennet, United States District Judge for the District of Maryland, sitting by designation.

That is *precisely* the nature of the testimony that the government intends to offer here: interpretation of various message fragments stored as user notifications in the knowledgex database and other database locations from within the [REDACTED] iPhone. This is most definitely not “common knowledge of the average layman” – but rather is testimony that requires specialized knowledge and expertise in obtaining, reading and interpreting cell phone forensic data.

Indeed, the Seventh Circuit has also held that “technical aspects of a forensic examination” of a digital device “constitutes ‘specialized knowledge’ under Rule 702.” *United States v. Wehrle*, 985 F.3d 549, 554 (7th Cir. 2021). There, a law enforcement analyst testified about “data-extraction software,” its “reliability and safeguards,” and “other technical processes such as hashes . . . and metadata.” *Id.* Because that testimony was specialized, it “crosse[d] into Rule 702 territory,” and admitting it without qualifying her as an expert was error. *Id.*

This Court should, most respectfully, follow the reasoning from *Wehrle* and the dissent in *Jimenez-Chaidez*, and preclude the government from sidestepping its obligations under Fed. R. Crim. P. 16 and Rule 702 of the Federal Rules of Evidence. The government should be precluded from offering non-expert testimony and evidence from the forensic extraction of the [REDACTED] iPhone at trial.

B. If the Court Permits The Government to Offer Evidence from the [REDACTED] iPhone it Should Hold a *Daubert* Hearing

For the reasons stated *supra*, the government should be precluded from offering non-expert testimony and evidence from the [REDACTED] iPhone. However, if the Court permits the government to introduce such testimony and evidence at trial, it should hold a *Daubert* hearing to ascertain the reliability of the forensic examination and extraction

process and whether it meets the threshold requirements for admissible evidence under *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 570 (1993).

Specifically, GrayKey was used to extract the contents of the [REDACTED] iPhone. GrayKey's forensic reliability cannot be independently verified because it is a tool that is only available to law enforcement officers. (Morrissey Decl. at ¶ 18). To undersigned counsel's knowledge, there has not been a single case where a court has conducted an evidentiary hearing to ascertain the forensic reliability of cell phone data extracted using GrayKey. It is of particular importance because GrayKey's proprietary, shadowbox technology exploits security vulnerabilities in the Apple iOS operating system to permit the installation of GrayKey's software agent to the phone, which then permits a full file system extraction of the phone to be performed depending on the unlock state of the phone. (Morrissey Decl. at ¶¶ 16 – 17). To counsel's knowledge, the process by which Telegram data is extracted from a cell phone by GrayKey has not yet been forensically verified. (Morrissey Decl. at ¶ 18).

Prior to admitting expert evidence under Rule 702, the district court must make a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and whether that reasoning or methodology properly can be applied to the facts in issue. *United States v. Ashburn*, 88 F. Supp. 3d 239, 242 (E.D.N.Y. 2015) (citing *Daubert*, 509 U.S. at 593-94). These requirements apply to every type of knowledge included in Rule 702, whether scientific, technical, or other specialized knowledge. *See generally, Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999). Some of the factors a trial court may consider in reviewing the reliability of proffered expert testimony include: (1) whether the theory or technique used by the

expert can be, or has been, tested; (2) whether the theory or technique has been subjected to peer review or publication; (3) the known or potential rate of error of the method used; (4) whether there are standards controlling the technique's operation; and (5) whether the theory or method has been generally accepted within the relevant community. *Ashburn*, 88 F.Supp. 3d at 242 (citing *Daubert*, 509 U.S. at 593-94).

While the government has not noticed an expert to testify to these issues that would trigger the requirements of *Daubert*, prior to admitting evidence from the [REDACTED] iPhone, which was extracted using GrayKey, the Court should hold a *Daubert* hearing to determine whether its extraction techniques are forensically reliable to the degree required for admission into evidence and consideration by a trial jury.

III. CONCLUSION

For the foregoing reasons, the Court should preclude the government from offering non-expert evidence and testimony relating to data recovered from the [REDACTED] iPhone and any other cell phone extraction presenting similar issues that it intends to reply upon. In the alternative, the Court should hold a *Daubert* hearing to determine whether testimony and evidence relating to the [REDACTED] iPhone should be admitted at trial.

Respectfully submitted,



JOSHUA J. HOROWITZ, ESQ.
HOROWITZ TECH LAW P.C.

734 Franklin Ave., #605
Garden City, New York 11530
Tel: (212) 203-9011
joshua.horowitz@techlawny.com

STEPHEN TURANO
TURANO LAW

275 Madison Avenue, 35th Fl.
New York, New York 10016
Tel: (917) 594-5666
sturano@turanolaw.com

Counsel for Defendant [REDACTED]