

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

_____ /

NOTICE OF FILING

The Government hereby gives notice that it has filed the Government's Classified Notice of Expert Testimony under seal with the Court by delivering it to the Classified Information Security Officer ("CISO") on January 12, 2024. An unclassified cover sheet for the notice is attached hereto.

Having provided a complete statement of its expert witnesses' qualifications, opinions and anticipated testimony, and the basis for their opinions, the Government requests the reciprocal disclosures required by Federal Rule of Criminal Procedure 16(b)(1)(C) and Local Rule

88.10(o)(3) — the latter of which typically requires an “initial written summary” within 14 days of the request — by a date to be set by the Court.

Respectfully submitted,

JACK SMITH
Special Counsel

By: /s/ Brett C. Reynolds
Jay I. Bratt, Counselor to the Special Counsel
Julie A. Edelstein, Senior Assistant Special Counsel
David V. Harbach, II, Assistant Special Counsel
David Raskin, Assistant Special Counsel
Brett C. Reynolds, Assistant Special Counsel

950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

January 12, 2024

CERTIFICATE OF SERVICE

I certify that on January 12, 2024 I electronically filed the foregoing document with the Clerk of Court using CM/ECF.

/s/ Brett C. Reynolds
Brett C. Reynolds

ATTACHMENT A

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

GOVERNMENT’S NOTICE OF EXPERT TESTIMONY OF GABRIELA MANCINI

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court’s Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

**Gabriela Mancini, Information Technology Specialist / Digital Forensic Examiner,
Computer Analysis Response Team, Federal Bureau of Investigation**

a. Training and Qualifications

The United States intends to call Digital Forensic Examiner Gabriela Mancini as an expert in forensic extraction and examination of digital devices. Ms. Mancini has worked for the Federal Bureau of Investigation (“FBI”) Computer Analysis Response Team (“CART”) Washington Field Office since June 2018.

Ms. Mancini has extensive professional training regarding the forensic analysis of electronic information, including cell phone data. She has completed dozens of professional training courses relating to forensics and the analysis of electronic information, to include courses

that specifically focused on the analysis of smartphone data. Ms. Mancini has also obtained numerous professional certifications related to digital forensic exams, including the Global Information Assurance Certification in Advanced Smartphone Forensics (August 2023), GrayShift GrayKey Operator Certification (August 2023), and FBI CART Senior Examiner Certification (November 2022). During her time at CART, Ms. Mancini has performed search and seizure operations, and conducted numerous forensic examinations of digital devices, including processing more than one hundred cellular phones.

Ms. Mancini's qualifications to extract, process, and analyze data from digital devices are based on her knowledge, skill, expertise, training, and education, as further described in her curriculum vitae, which has been provided to the defense (USA-01286146 – USA-01286147).

b. Publications and Prior Testimony as an Expert

Ms. Mancini has not authored any publications in the last ten years, nor has she testified as an expert at trial or by deposition in the last four years.

c. Report Provided under Federal Rule of Criminal Procedure 16(a)(1)(F)

The Government produced to the defense Ms. Mancini's digital forensic extraction report (USA-01287076 – USA-01287083).

d. Complete Statement of Testimony/Opinion and Basis

The Government anticipates that Ms. Mancini will testify that she forensically extracted and processed content and data from two digital devices: (1) an Apple iPhone 12 Pro Max (IMEI 354506122270257, designated FBI evidence item 1B2, associated with a phone number ending in -6091) and (2) an Apple iPhone 13 Pro Max (IMEI 350879907498888, designated FBI evidence item 1B3, associated with a phone number ending in -8611). Both devices were used by defendant

Waltine Nauta and searched after the Government obtained a court-authorized search warrant for those devices.¹

The Government expects that Ms. Mancini will testify as to the manner in which she handled the two digital devices, the forensic extraction and processing tools she used, and the reports generated as a result of the forensic examinations. Ms. Mancini will testify that she used forensic tools such as GrayKey to extract data from both devices, and tools such as Axiom and Cellebrite to process data from the two devices used by defendant Nauta. She will also explain the purpose of verification procedures, such as hash matching, that she used to ensure that the forensic extraction and processing yielded reliable and accurate copies of the data found on each digital device. Additionally, Ms. Mancini will testify about the reliability of the programs she used throughout the process.

Ms. Mancini will also testify about certain types of data obtained from each digital device, including, *inter alia*, any account names, iCloud accounts, phone numbers, and email addresses associated with the respective device. Likewise, she will testify about data and metadata relating to certain messaging platforms found on the devices, to include Signal and WhatsApp, as well as other data associated with certain images, videos, messages, and applications.

The Government anticipates that Ms. Mancini will testify that on Nauta's Apple iPhone 12 Pro Max device she located three thumbnail photos containing classification markings and tagged them as such using the Cellebrite program. She will testify that the three images include two unique thumbnail images and one duplicate thumbnail image, on Nauta's Apple iPhone 12 Pro

¹ The contents of those devices, after a filter review was conducted for attorney-client privilege and scoping within the parameters of the search warrant, were provided to the defense in discovery. See USA-00792879 – USA-00798834; USA-01125897 – USA-01208507; USA-00798835 – USA-00798834; and USA-01208508 – USA-01260871.

Max device associated with a phone number ending in -6091. Ms. Mancini will also describe where within the device these photos were located.

Ms. Mancini's opinions are based upon her knowledge, skill, education, training, and experience working in law enforcement and as a digital device examiner.

e. Approval of Disclosure

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this disclosure and approve of its contents.

Date: January 9, 2024



Gabriela Mancini
Digital Forensic Examiner
Information Technology Specialist
FBI

ATTACHMENT B

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

GOVERNMENT’S NOTICE OF EXPERT TESTIMONY OF STACY SHAHRANI

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court’s Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

Stacy Shahrani, FBI Special Agent, Digital Forensic Examiner for Computer Analysis Response Team, Washington Field Office

a. Training and Qualifications

Special Agent Shahrani is a digital forensic examiner who has worked for the Federal Bureau of Investigation (“FBI”) since 2008. She conducted criminal investigations involving transnational organized crime and violent crimes against children from 2008 to 2019, including as a digital evidence examiner technician beginning in 2017. From April 2019 to August 2020, Special Agent Shahrani served as a supervisory special agent in the FBI Cyber Division, and, since August 2020, as a digital forensic examiner as part of the Computer Analysis Response Team (“CART”) in the Washington Field Office. Before her service in the FBI, Special Agent Shahrani

served in the U.S. Air Force, first as a lieutenant managing the Chemical Biological Radiological Nuclear and Explosive program for Holloman Air Force Base in New Mexico, and then, as a captain, leading engineering and repair teams in Iraq, Afghanistan, and Peru. She was awarded the Air Force Commendation Medal twice (2003, 2004), the Army Commendation Medal (2006), and the Meritorious Service Medal (2008). Special Agent Shahrani holds a Bachelor of Science degree in Mechanical Engineering from the University of Rhode Island.

Special Agent Shahrani has received professional training in digital forensic analysis, including over 400 hours in digital forensic training and over 250 hours in cyber training. Special Agent Shahrani received an FBI digital extraction technician certification in 2017 and a digital forensic examiner certification in 2022. Special Agent Shahrani has analyzed over 100 electronic devices as an FBI digital forensic examiner.

A copy of Special Agent Shahrani's curriculum vitae has been provided to the defense. *See* USA-01287326 – USA-01287327.

b. Publications and Prior Testimony as an Expert

Special Agent Shahrani has not authored any publications in the last ten years, nor has she testified as an expert at trial or by deposition in the last four years. However, Special Agent Shahrani has, within the last four years, testified as a fact witness in two cases regarding digital forensic extractions and examinations she has conducted: *United States v. Guy Reffitt*, Case Number 21-cr-00032-DLF (D.C.) (trial) and *United States v. Luis Escobosa*, Case Number 16-cr-6-WFK (E.D.N.Y.) (supervised release hearing).

c. Report Provided under Federal Rule of Criminal Procedure 16(a)(1)(F)

The Government produced to the defense Special Agent Shahrani's digital forensic reports. *See* USA-01286194 – USA-01286274.

d. Complete Statement of Testimony/Opinion and Basis

Special Agent Shahrani will testify that she conducted a forensic analysis of two electronic accounts: (1) the Apple iCloud account associated with Waltine Nauta's Gmail email account and Apple DSID (designated FBI evidence item 1B1) and (2) the Apple iCloud account associated with the Nauta's 45 Office email account and Apple DSID (designated FBI evidence item 1B4), which the Government obtained from court-authorized search warrants for those accounts used by defendant Waltine Nauta.¹ In her testimony, Special Agent Shahrani will explain that records from the Apple iCloud account associated with the Nauta's Gmail email account indicate that this account was set to receive iMessages from both the phone number ending in 8611 and the phone number ending in 6091.

The Government anticipates that Special Agent Shahrani will also testify that she conducted a forensic extraction and forensic analysis of an Apple iPhone 13 Pro Max, IMEI 355380250576912 (designated FBI evidence item 1B4), and forensic imaging of a Dell Vostro Laptop, Service tag 6TVR503, serial number CN07N722915007S6H (designated FBI evidence item 1B5), both used by Trump Employee 2 (as that person is referred to in the Superseding Indictment, whose identify the Government has provided to the defense) and searched after the Government obtained a court-authorized search warrant for those devices.²

¹ The unclassified contents of those accounts, after a filter review was conducted for attorney-client privilege and scoping within the parameters of the search warrant, was provided to the defense in Production 1. *See* USA-00544137 – USA-00637698. The portions of the Nauta iCloud accounts with images containing visible classification markings were produced in classified discovery.

² The contents of those devices, after a filter review was conducted for attorney-client privilege and scoping within the parameters of the search warrant, was provided to the defense in discovery. *See* USA-00416469 – USA-00447955 (laptop) and USA-00492118 – USA-00509692 (phone).

The Government expects that Special Agent Shahrani will testify as to the manner in which she handled the electronic accounts and devices, the forensic examination tools she used, and the reports generated as a result of the forensic examinations. Special Agent Shahrani will explain how verification procedures were used to ensure that the forensic processing yielded reliable and accurate copies of the data found on the digital devices. Special Agent Shahrani will also explain how certain text communications, images, and call records were found on the iCloud accounts and electronic devices, as well as the metadata for certain communications and images.

Additionally, Special Agent Shahrani will describe how she conducted a physical inventory of the devices, removed the Subscriber Identity Module (commonly referred to as a SIM) card from the phone and used Graykey hardware/software for data extraction, and used write-blocking technology to protect the integrity of the original laptop evidence when creating a forensic image for later examination. Furthermore, for the iCloud accounts, Special Agent Shahrani retrieved the decrypted data contained in the Nauta iCloud warrants, obtained the hash value of the decrypted production to ensure the data remained unchanged during her subsequent review and analysis, processed the images contained using Axiom and Cellebrite software, and selected all available applications to be examined.

The Government anticipates that Special Agent Shahrani will also testify that she was asked to review Nauta's iCloud accounts and the two aforementioned devices, used by Trump Employee 2, for documents with classification markings. Special Agent Shahrani found that two photos containing classification markings were texted to Trump Employee 2 from an Apple iPhone with metadata matching the identifying information obtained by the Government from Nauta's iPhone ending in phone number 6091. The metadata included information that the photos were taken using "Walt's phone" and the IMEI number matched the known IMEI number of Nauta's

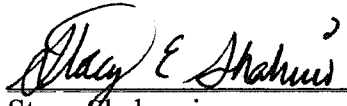
phone with the phone number ending in 6091. The first photo containing a classification marking was taken and texted on October 27, 2021,³ and the second, which is referenced in the Superseding Indictment in paragraph 32 and Count 8, was taken on December 7, 2021. Special Agent Shahrani will describe where within the iCloud account and devices these photos were located. Additionally, Special Agent Shahrani generated a redacted Cellebrite reader report with the items containing classification markings excluded, as well as an HTML report that was provided in classified discovery. *See* Disc_004, Classified Production 3, produced on October 6, 2023.

In addition to the two photos, Special Agent Shahrani will testify that she located the same two images with classification markings on the Apple iPhone 13 Pro Max (items 1B4), for which she generated an HTML report that was provided in classified discovery. *See* Disc_004, Classified Production 3, produced on October 6, 2023.

e. Approval of Disclosure

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this disclosure and approve of its contents.

Date: January 10, 2024


Stacy Shahrani
Digital Forensic Examiner
FBI

³ The document depicted in the October 27, 2021 photo was subsequently declassified and produced in unclassified discovery. *See* USA-01285830.

ATTACHMENT C

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

_____ /

GOVERNMENT’S NOTICE OF EXPERT TESTIMONY OF HENRY HA¹

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court’s Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

**Henry K. Ha, Digital Forensic Examiner, Computer Analysis Response Team,
Federal Bureau of Investigation**

a. Training and Qualifications

The United States intends to call Federal Bureau of Investigation (“FBI”) Supervisory Special Agent (“SSA”) Henry K. Ha as an expert in forensic extraction and examination of digital devices. SSA Ha has worked for the FBI since 2009. From July 2009 through July 2017, SSA Ha

¹ The Government files this expert notice out of an abundance of caution. Numerous circuit courts have indicated that the type of digital data extraction about which SSA Ha would testify does not require expert testimony for admission. *See United States v. Williams*, 83 F.4th 994, 997 (5th Cir. 2023) (reviewing circuits and citing *United States v. Chavez-Lopez*, 767 F. App’x 431, 434 (4th Cir. 2019), *United States v. Marsh*, 568 F. App’x 15, 17 (2d Cir. 2014), and *United States v. Ovies*, 783 F. App’x 704, 707 (9th Cir. 2019)).

was a special agent with the FBI Las Vegas Field Office Cyber Squad, where he conducted cyber investigations, performed search and seizure operations, and conducted arrests and search warrants. From July 2017 through August 2019, SSA Ha served as a supervisory special agent in the FBI Cyber Division. Thereafter, from August 2019 through March 2023, he served as a special agent with the FBI Computer Analysis Response Team (“CART”) in the Washington Field Office, first as a digital forensic examiner trainee, and then as a digital forensic examiner. In March 2023, SSA Ha was assigned to his current role as a supervisory special agent with the FBI Counterterrorism Division in Washington, D.C.

SSA Ha has received extensive professional training in digital forensic analysis. He also obtained various certifications related to digital forensic exams, including FBI Digital Evidence Extraction Technician Authorization (August 2014), FBI CART Technician Certification (August 2014), GIAC Certified Forensic Examiner Certification (January 2015), FBI CART Digital Evidence Laboratory Technician Certification (October 2019), FBI CART Mobile Device Authorization (January 2020), FBI CART MacOS Authorization (January 2020), FBI CART Linux Command Line Authorization (February 2020), and FBI CART Basic Wintel FE Certification (July 2021). In his role as a digital forensic examiner with CART, SSA Ha performed search and seizure operations and conducted numerous forensic examinations of digital devices, including cellular phones.

SSA Ha’s qualifications to extract and analyze data from digital devices are based on his knowledge, skill, expertise, training, and education, as further described in his curriculum vitae, which has been provided to the defense. *See* USA-01286124 – USA-01286126.

b. Publications and Prior Testimony as an Expert

SSA Ha has not authored any publications in the last ten years, nor has he testified as an expert at trial or by deposition in the last four years.

c. Report Provided under Federal Rule of Criminal Procedure 16(a)(1)(F)

The Government produced to the defense SSA Ha's forensic extraction report. *See* USA-00944449 – USA-00944463.

d. Complete Statement of Testimony/Opinion and Basis

The Government expects that SSA Ha will testify that he conducted a forensic extraction of content and data from an Apple iPhone 12 Mini, IMEI 353008113083766, Serial Number F4GDN8040GRN (designated FBI evidence item 1B1) used by defendant Carlos De Oliveira, that was searched after the Government obtained a court-authorized search warrant for the device.² SSA Ha will explain that for purposes of this device, his role was limited to forensic extraction and verification of data from De Oliveira's phone.

In his testimony, SSA Ha will explain the manner in which he handled the digital device and the process he used to extract data from the device and create a forensic image of it. SSA Ha will describe that on February 13, 2023, he conducted a physical inventory of the device, and then obtained an extraction of the digital device and the SIM card using GrayKey and Cellebrite software. He will also testify about how a Cellebrite Reader report was generated as a result of the forensic extraction of data from the phone and SIM card.

Additionally, SSA Ha will testify about why the extractions he performed are reliable and accurate renditions of the data found on the digital device. For example, SSA Ha will explain how

² The contents of the device, after a filter review was conducted for attorney-client privilege and scoping within the parameters of the search warrant, were provided to the defense in discovery. *See* USA-00402920 – USA-00413873.


hash values were generated and used to verify that the forensic image of the digital device was an exact match of the original evidence item. Similarly, SSA Ha will testify about the purpose behind imaging and hash-matching the original digital evidence, including to ensure that the original evidence is not damaged or altered during any subsequent forensic examination, and that the forensic image being analyzed contains the same data as the original evidence. SSA Ha will also explain how GrayKey has internal verification procedures to confirm that it has properly extracted the data from the device.

SSA Ha's opinions are based upon his education, training, and experience working in law enforcement and as a digital device examiner.

e. Approval of Disclosure

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this disclosure and approve of its contents.

Date: January 10, 2024



Henry K. Ha
Digital Forensic Examiner
Special Supervisory Agent
FBI

ATTACHMENT D

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

GOVERNMENT’S NOTICE OF EXPERT TESTIMONY OF ANDREW KOCHY

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court’s Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

Andrew Kochy, Special Agent, Computer Analysis Response Team, Federal Bureau of Investigation

a. Training and Qualifications

The United States intends to call Federal Bureau of Investigation (“FBI”) Special Agent Andrew Kochy as an expert in forensic extraction and examination of digital devices. Special Agent Kochy has worked for the FBI since 2002. He has been assigned to multiple units focusing on cyber crime, including the Asia Cyber Crimes Unit and Major Cyber Crimes Squad. From April 2018 through the present, Special Agent Kochy has been assigned to the FBI Computer Analysis Response Team (“CART”) Washington Field Office as both a Special Agent and

Supervisory Special Agent. While with CART, SA Kochy has conducted numerous forensic examinations of various digital devices, including cellular phones.

Special Agent Kochy has received extensive professional training in digital forensic analysis. He also obtained various certifications related to digital forensic exams, including GIAC Certified Forensic Examiner (August 2023), Magnet Certified Forensic Examiner (May 2022), GIAC Advanced Smartphone Forensics Certification (Aug. 2021), Cellebrite Certified Physical Analyst (April 2020), Cellebrite Certified Operator (April 2020), and FBI CART Mobile Device Authorization (June 2018).

Special Agent Kochy's qualifications to analyze data extracted from digital devices are based on his knowledge, skill, expertise, training, and education, as further described in his curriculum vitae, which has been provided to the defense. *See* USA-01286130 – USA-01286132.

b. Publications and Prior Testimony as an Expert

Special Agent Kochy has not authored any publications in the last ten years. He has testified as an expert witness in the following two Eastern District of Virginia federal cases in connection to his extraction and analysis of data from digital devices, within the last four years: *United States v. Zackary Ellis Sanders* (20-CR-143-TSE) and *United States v. Moises Zelaya Veliz, et al.* (20-CR-196-AJT).

c. Report Provided under Federal Rule of Criminal Procedure 16(a)(1)(F)

The Government produced to the defense Special Agent Kochy's forensic examination reports *See* USA-00042129 – USA-00042130; USA-01286148 – USA-01286193.

d. Complete Statement of Testimony/Opinion and Basis

The Government expects that Special Agent Kochy will testify that he conducted a forensic analysis of content and data extracted from an Apple iPhone 12 Mini, IMEI 353008113083766,

Serial Number F4GDN8040GRN (designated FBI evidence item 1B1) used by defendant Carlos De Oliveira, that was searched after the Government obtained a court-authorized search warrant for the device.¹

Special Agent Kochy will testify about the forensic examination tools he used, to include Axion and Cellebrite, and the reports generated as a result of the forensic examinations. He will also testify about data obtained from the digital device, including, *inter alia*, certain geolocation information, metadata, device information, evidence of user attribution, phone numbers connected to the device, phone contacts, call information, electronic messages, photographs, videos, messaging platforms, device location data, device power information, and corresponding time and location data of certain photos and videos. For example, Special Agent Kochy will testify about his analysis of geolocation data artifacts extracted from the device that pertain to certain images taken on various dates, to include June 27, 2022 and July 12, 2022. Special Agent Kochy will explain how certain text communications, images, and call records were found on the digital device, and how he documented the geolocation information and other metadata for certain images.

During his testimony, Special Agent Kochy will also explain how the data contained in the Government's cell phone exhibits is a reliable and accurate depiction of the data obtained from the digital device and the corresponding extraction. For example, the Government anticipates that Special Agent Kochy will explain how verification procedures were used to ensure that the forensic processing yielded reliable and accurate copies of the data extracted from the digital device. Likewise, he will testify about how hash values are generated and used to verify that the forensic image of a digital device is an exact match of the original evidence item. Special Agent

¹ The contents of the device, after a filter review was conducted for attorney-client privilege and scoping within the parameters of the search warrant, was provided to the defense in discovery. *See* USA-00402920 – USA-00413873.

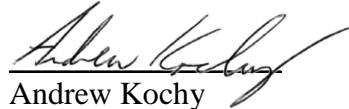
Kochy is expected to testify about the purpose behind imaging and hash-matching the original digital evidence, including to ensure that the original evidence is not damaged or altered during any subsequent forensic examination and that the forensic image being analyzed contains the same data as the original evidence. Additionally, Special Agent Kochy will testify about the reliability of the programs he used to parse, examine, and analyze the matching data contained on the forensic image of the cellular phone.

Special Agent Kochy's opinions are based upon his education, training, and experience working in law enforcement and as a digital device examiner.

e. Approval of Disclosure

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this disclosure and approve of its contents.

Date: January _10_, 2024


Andrew Kochy
Special Agent
FBI

ATTACHMENT E

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

GOVERNMENT NOTICE OF EXPERT TESTIMONY OF JOHNATHON HOYT

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court's Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

I. Johnathon Hoyt, FBI Special Agent, certified member of the Cellular Analysis Survey Team

a. Training and Qualifications

Special Agent Hoyt is a certified member of the Federal Bureau of Investigation ("FBI") Cellular Analysis Survey Team ("CAST"), a specialized unit in the FBI that provides technical expertise, case consultation, and instruction in the analysis of historical call detail records, cell site location information, and other forms of geolocation information. Special Agent Hoyt has worked for the FBI since 2018 and served in various roles, including on a Joint Terrorism Task Force, a violent crimes task force, and, since September 2022, as a member of the CAST team.

Special Agent Hoyt has received professional training in cellular analysis, including over 230 hours of historical cell site analysis with 40 hours of instruction from the Florida Institute of Technology on the engineering of cellular networks, radio frequency technology and propagation, cellular network architecture, cellular network technologies, and cellular network measurements. Special Agent Hoyt has also served as an instructor in historical cell site analysis.

A copy of Special Agent Hoyt's curriculum vitae, which summarizes his background, education, and experience, has been provided to the defense. *See* USA-01286127 – USA-01286129.

b. Publications and Prior Testimony as an Expert

In the previous 10 years, Special Agent Hoyt has not authored any publications. He has testified as a CAST expert in three criminal trials within the past four years: *Loudoun County CW v. Furqan Syed*, Case No. CR00037455-00 (Loudoun County, Virginia Circuit Court); *United States v. Lewkus Turner*, Case No. 2020-CF1-009637 (D.C. Superior Court); and *United States v. Jalen Browne*, Case No. 2021-CF1-007103 (D.C. Superior Court).

c. Reports Provided under Federal Rule of Criminal Procedure 16(a)(1)(F)

Special Agent Hoyt created three reports that detail his historical cell site analysis of the call detail records for two cell phones (phone numbers ending in 6091 and 8611, respectively), which the Government's investigation shows belonged to defendant Waltine Nauta (hereinafter, "Nauta's cell phones") and one cell phone (phone number ending in 8426), which the Government's investigation shows belonged to defendant Carlos De Oliveira (hereinafter, "De Oliveira's cell phone"). All three reports were produced to the defense in discovery. *See* USA-00947182 – USA-00947214; USA-01286057 – USA-01286087; and USA-01286088 – USA-01286123.

The reports provide Special Agent Hoyt's methodology, as well as the bases for his opinions, including explanations of cell towers, sectors, orientation, and call detail records. The reports further contain visual depictions of cell-site activity locations overlayed on maps for Nauta's cell phones on May 25-June 3, 2022; June 25-28, 2022; July 10-12, 2022; and July 22-23, 2022; and for De Oliveira's cell phone on June 25-27, 2022; July 10-12, 2022; and July 22-23, 2022.

d. Complete Statement of Testimony/Opinion and Basis

The Government anticipates that Special Agent Hoyt will testify that, using cell tower latitude/longitude coordinates obtained from Nauta's and De Oliveira's cell phone service providers pursuant to court-authorized search warrants,¹ he mapped cell site data into mapping software that plotted cell tower location and the cell sector, including the general direction of the radio frequency signal, that serviced the cell phone activity.

Special Agent Hoyt is also expected to testify about his analysis of historical cell site and location data for Nauta's and De Oliveira's phones contained in his reports and the data produced to the defense. For example, Special Agent Hoyt will explain that location data on Saturday, June 25, 2022, shows Nauta's cell phone ending in 6091 moving from the area of Bedminster, New Jersey, to La Guardia Airport in New York, Logan Airport in Boston, and finally Palm Beach International Airport in West Palm Beach. At 10:16 a.m. that day, Nauta's cell phone ending in 6091 connected with the cell tower at Logan Airport, when a call was made to De Oliveira's cell number ending in 8426, which connected with the cell tower closest to Mar-a-Lago. At 5:40 p.m., the cell tower closest to Mar-a-Lago provided network coverage for a call made from Nauta's cell

¹ The latitude/longitude data obtained pursuant to the search warrant for Nauta's cell site location was provided in discovery at USA-00788381 – USA-00788430. The latitude/longitude data for De Oliveira's phone was provided in discovery at USA-01115989 – USA-01116024.

phone ending in 6091 to De Oliveira's cell phone, which also connected with the cell tower closest to Mar-a-Lago.

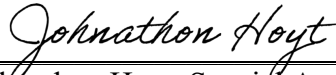
The location data will also show Nauta's cell phone locations in South Florida until it returned to the area of Bedminster, New Jersey, on June 28, 2022. For example, on Monday, June 27, 2022, at 10:15 a.m., De Oliveira's cell phone, connecting with the cell tower closest to Mar-a-Lago, made a call to Nauta's cell phone ending in 6091, which connected with the cell tower located near Nauta's residence in West Palm Beach. At 1:29 p.m., when a call was made from Nauta's cell phone ending in 6091 to De Oliveira's phone, and again at 1:46 p.m. when a call was made from De Oliveira's cell phone to Nauta's cell phone ending in 6091, both phones connected with the cell tower closest to Mar-a-Lago.

Special Agent Hoyt will also testify about how cellular networks operate and factors that affect which tower or sector a cellular telephone will use. Special Agent Hoyt will explain how location analysis is a reliable means to approximate a cellular telephone's location when it connects to a particular cellular tower.

e. Approval of Disclosure

In accordance with Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this disclosure and approve of its contents.

Date: January 10, 2024



Johnathon Hoyt, Special Agent
Cellular Analysis Survey Team
FBI

ATTACHMENT F

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO. 23-80101-CR-CANNON(s)

UNITED STATES OF AMERICA,

Plaintiff,

v.

**DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,**

Defendants.

GOVERNMENT’S NOTICE OF EXPERT TESTIMONY OF DAVID LOVEALL II

The Government hereby files under Federal Rule of Criminal Procedure 16(a)(1)(G), Local Rule 88.10(o)(3), and this Court’s Order (ECF No. 215) its notice of intent to use the following expert testimony in its case-in-chief at trial.

**David Loveall II, Senior Computer Scientist, Operational Technology Division,
Federal Bureau of Investigation**

a. Training and Qualifications

The Government intends to call Federal Bureau of Investigation (“FBI”) Senior Computer Scientist David Loveall II as an expert in electronic evidence and digital media forensics. Mr. Loveall has worked for the FBI in various capacities in the field of digital forensics since 2000, including as a Senior Technical Forensic Advisor, Computer Scientist, Digital Forensic Examiner, and Information Technology Specialist. From December 2013 through the present, he has been assigned to the Operational Technology Division of the FBI in Quantico, Virginia, where he serves as a Senior Technical Forensic Advisor. In this capacity, Mr. Loveall advises FBI personnel on

issues related to digital forensics and computer science. Prior to that, Mr. Loveall worked as a digital forensic examiner in the FBI's Kansas City office. During his more than two decades with the FBI, Mr. Loveall has conducted hundreds of digital forensic examinations.

Mr. Loveall holds a Bachelor of Science in Computer Science, Mathematics, and Physics, and a Master of Science in Computer Forensics. He has received extensive professional training and obtained various certifications related to digital forensic analysis and exams, including certifications for FBI Computer Analysis Response Team ("CART") Forensic Examiner, Senior Forensic Examiner, Macintosh Field Examiner, DOS / Windows Field Examiner, and Unix Field Examiner. Since 2014, Mr. Loveall has served as an Adjunct Professor at George Mason University in Fairfax, Virginia, teaching various courses including Advanced Computer Forensics, Windows Registry Forensics, and Linux Forensics. Mr. Loveall is also the recipient of the FBI Director's Award for Outstanding Technical Advancement, the Presidential Early Career Award for Scientists and Engineers for his contributions to the field of digital forensics, and the Intelligence Community Seal Medallion.

Mr. Loveall's qualifications to analyze publicly available data captured from the internet are based on his knowledge, skill, expertise, training, and education, as further described in his curriculum vitae, which was provided to the defense in discovery (USA-01286133 – USA-01286145).

b. Publications and Prior Testimony as an Expert

Mr. Loveall has not authored any publications in the last ten years. He also has not testified as an expert at trial or by deposition in the last four years, though in July 2023 he submitted a sworn certification responding to a digital forensic analysis report filed by the defense during post-trial litigation in *United States v. Keith Raniere* (18-204-NGG) (E.D.N.Y. 2018).

c. Complete Statement of Testimony/Opinion and Basis

The Government expects that Mr. Loveall will testify, if necessary, as to the authenticity of certain publicly available videos, images, and social media posts captured from the internet—to include some of defendant Trump’s speeches, media interviews, and Truth Social posts—that the Government intends to offer into evidence during its case-in-chief at trial.¹ Mr. Loveall will explain the forensic process of digital identification that he used to confirm that such videos, images, and social media posts captured from various publicly available internet websites are reliable, accurate, and unaltered depictions of what was presented on those websites at the time the data was captured.

Mr. Loveall will also explain the methodology and basis for his testimony. For example, he will testify about how website security certificates are used and hash values are generated, as well as how these are leveraged to verify that the forensic image of data captured from a website is an exact match of the data that was presented by the website at the time it was captured. Furthermore, Mr. Loveall is expected to testify about the purpose behind imaging and hash-matching, including explaining how these steps ensure that the data captured from the internet was not damaged, modified, or altered when it was captured, or during any subsequent examination. Additionally, Mr. Loveall will testify about the reliability of the programs he used to parse, examine, and analyze such data.

d. Approval of Disclosure

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G)(v), I have reviewed this

¹ These would include, for example, videos of the public statements identified in Paragraphs 23 and 37 of the Superseding Indictment (ECF No. 85), which were provided to the defense in discovery. *See* USA-00390664 – USA-00390669.

disclosure and approve of its contents.

Date: January 9, 2024

A handwritten signature in black ink, appearing to read "DLoveall II", written over a horizontal line.

David Loveall II
Senior Computer Scientist
FBI