STATE OF WISCONSIN CIRCUIT COURT MILWAUKEE COUNTY

AFFIDAVIT SUPPORTING THE NEXUS PORTION OF SEARCH WARRANT AUTHORIZING A FORENSIC EXAMINATION OF CELLULAR PHONE(S) OR MOBILE DEVICE(S)

AFFIDAVIT OF BRETT MENDOLA

STATE OF WISCONSIN)
) ss.
MILWAUKEE COUNTY)

Brett Mendola, being duly sworn on oath, states the following:

1) Affiant is a full-time, state certified law enforcement officer. Affiant has been employed as a Milwaukee County District Attorney Investigator, assigned to the Milwaukee County District Attorney's Office Investigations Unit since November 2022. Affiant has been a full-time sworn officer for over thirty (30) years with prior experience as a police officer and detective with the Oak Creek Police Department.

2) Affiants duties as a Milwaukee County District Attorney Investigator relate primarily to the law enforcement computer and mobile data field. Affiant has been working in the law enforcement telecommunications field since April of 2017.

3) Affiant has assisted other agencies with cell phone, computer, and computer accessory extraction and analysis. The agencies affiant has assisted include the following: Milwaukee Police Department, Wauwatosa Police Department, Marquette University Police Department, West Allis Police Department, Greenfield Police Department, Glendale Police Department, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Cudahy Police Department, South Milwaukee Police Department, Shorewood Police Department, Franklin Police Department, Oak Creek Police Department, Whitefish Bay Police Department, University of Wisconsin Milwaukee Police Department, Bayside Police Department, Brown Deer Police Department, and Fox Point Police Department.

4) Affiant has specialized training related to the law enforcement extractions of mobile devices, imaging of computers and related items, and their analysis.

5) In addition to other training, affiant has received the following training related to extractions of mobile devices, imaging of computers and related items, and their analysis:

    (a) Affiant has received one hundred and fifty-six (156) hours of training focusing on the extraction and analysis of mobile devices;
    (b) Affiant has received one hundred and ninety-six (196) hours of training focused on computer evidence recovery and analysis;

(c) Affiant has seventy-six (76) hours of training focused on Apple computer evidence recovery and analysis;
(d) Affiant received seventy-six (76) hours of advanced training in the extraction and analysis of mobile devices;
(e) Affiant received forty (40) hours of training related to the repair of mobile devices;
(f) Affiant has obtained, or assisted other officers in obtaining phone extractions on over one thousand (1000) occasions;

6) This affidavit is based on affiant's training and experience, including that recited above;

7) Affiant knows from their training and experience that mobile devices, including cellular telephones and tablet computers, commonly contain live and deleted user attribution data including, but not limited to, user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, pictures, videos, metadata, or other information and evidence that may demonstrate attribution to a particular user or users.

8) Affiant knows from their training and experience that mobile devices can be connected to a cellular network (Mobile Network Operator) or to the Internet via Wi-Fi. A mobile device usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, mobile device connectivity allows users to make and receive calls, send and receive text messages, take and send pictures and videos, communicate using third party applications "apps," access social media, navigate using mapping and navigation apps and access the World Wide Web. Affiant knows that videos and images can be e-mailed, sent through messaging systems such as SMS (Short Message Service) and MMS (Multi-media Message Service) messages and other forms of communication located within specialized applications. Affiant knows when mobile devices are examined it is common to identify a spectrum of communication methods. Videos and images can be seamlessly emailed or transmitted through messaging systems such as SMS and MMS. Additionally, specialized applications house various forms of communication, often revealing email addresses and other online account details. These details become vital as they could contain evidence related to the distribution of images, videos, text communication, file sharing, and remote cloud storage. Affiant also knows that metadata associated with these images and videos may include details such as the camera used, date and time the image or video were recorded, and GPS location information. Affiant knows that the metadata linked to these images and videos holds critical information. This includes specifics like the camera used, the date and time of recording, and GPS location data. Recognizing the significance of these details enhances the overall understanding of the digital footprint and aids in establishing a comprehensive picture during forensic analysis.

9) Affiant knows from their training and experience that messaging services and applications allow users to send encrypted and unencrypted text messages, photos, videos, and other data between mobile devices. These services do not appear in carrier records, which only reflect general data usage rather than message content. The content of these messages exists only on the device itself or within associated cloud backups. Without a full extraction of the device, critical communications between suspects and co-conspirators may never be identified. The same applies to encrypted and unencrypted messaging platforms such as WhatsApp, Signal, Telegram, iMessage and similar services, which also do not provide content through carrier records.

10) Affiant knows from their training and experience that mobile device users can utilize and store health and movement data, including steps, sleep, heart rate, activity routes, and exertion levels. Health data may show whether a suspect was awake, moving, driving, or stationary during an incident. These records can corroborate or contradict suspect statements and assist in determining device possession.

11) Affiant knows from their training and experience that mobile devices often store financial data, such as information from banking apps, payment platforms, digital wallets, and transaction receipts. This data may show payments related to criminal activity, transfers to co-conspirators, or purchases relevant to the offense. Much of this information cannot be obtained through provider requests and must be extracted directly from the device.

12) Affiant knows from their training and experience that Bluetooth logs can reveal when a device connected to vehicles, home devices, smart appliances, or other electronics. These connections may show, for example, when a phone paired with a vehicle's infotainment system, placing the user inside that vehicle, or when it connected to a smart TV or speaker inside a residence, helping establish presence at a specific location. Repeated connections to the same devices can also demonstrate patterns of association or residency. Bluetooth logs may lack timestamps, requiring examiners to review the full device extraction to accurately interpret these connections.

13) Affiant knows from their training and experience that mobile device users can install applications that can be used to hide and even encrypt data and conceal specific data from detection. These applications are generally accessed by covert means known by the user and often require a PIN code, pattern, password, or a unique biometric feature such as a fingerprint. Affiant also knows that users sometimes hide contraband images and other content in other, seemingly innocuous, applications and folders such as calendars and games as a way to avoid detection. This strategic concealment is done with the intent of avoiding detection. Given these potential evasion techniques, conducting a comprehensive search of all data on the device is necessary. This ensures that no hidden or encrypted information escapes the search. For these reasons, affiant knows it is necessary to search all data on the device.

14) Affiant knows from their training and experience Facial biometric authentication, such as Face ID, facial recognition unlocks, and similar technologies is commonly used by mobile device users as the primary method of accessing a cellphone. Unlike a PIN or password, which may rarely be entered once biometric access is enabled, facial biometric data is captured and stored on the device to allow immediate unlocking and consistent access. Because many suspects rely exclusively on biometrics for daily phone access, the presence of active facial biometric settings strongly supports user identification. Forensic extraction of biometric configuration data, including timestamps of biometric enrollment or modification, can help identify who set up and regularly accessed the phone. This information is essential for determining device ownership, continuity of possession, and any involvement by co-conspirators who may have enrolled biometrics.

15) A contact stored within a cellphone can contain far more than a name and phone number. Contacts may include multiple numbers, email addresses, physical addresses, social media identifiers, notes, relationship labels, associated photos, and timestamps of when the contact was added or modified. This data may allow investigators to identify the device's primary user, frequent associates, victims, and co-conspirators. Because some contacts lack timestamps or rely on system metadata that does not align with specific dates, the entire device must be reviewed. Contacts often reveal communication networks, organizational roles within conspiracies, and links between individuals that cannot be understood without full extraction and analysis of all device data.

16) Affiant knows based on their training and experience that mobile devices commonly have Global Positioning System (GPS) and other similar geo-location sensors. These sensors may track the historical location of the device geographically and provide a historical record. Affiant also knows that these systems leave log files. Affiant knows that these log files can be recovered and used to locate a device's geographic historical location on a specific date and time. Affiant knows that this information could be used to include or exclude the user from involvement with the planning, execution, and potential post crime cover-up activities.

17) Affiant knows that some mobile devices may contain a Subscriber Identity Module (SIM cards) that may contain data associated with the device and user attribution such as contact lists, call logs, SMS messages, telephone number, and other user data commonly found in cellular telephones. Modern cellphones frequently use eSIMs instead of physical SIM cards. When investigators seize a locked cellphone, the device must be shielded from the network to prevent remote wiping. Because an eSIM profile cannot be physically inspected, investigators cannot determine the phone number associated with the device without conducting a forensic extraction. Without this information, law enforcement cannot identify or request call detail records from providers. A full extraction is the only method to obtain the phone number, eSIM identifiers, and linked account information.

18) Affiant also knows that some mobile devices may contain removable media cards. These cards are commonly referred to as SD cards or MicroSD cards. These cards can be used to store additional data associated with the mobile device including photographic images, videos, text files and other digital data. Affiant knows that additional data contained within these files may also provide dates, times, locations, settings, devices used, and user attribution information.

19) Affiant also knows that such devices can be used to communicate and instantly share information with others and that data can be transferred between various devices – wirelessly and by connected cables.

20) Affiant also knows that if these items are not seized and isolated from network connectivity in a timely manner, potential inculpatory and exculpatory evidence may be destroyed, transferred, encrypted, modified, or otherwise lost forever. Affiant knows that data recovered from mobile devices can be used to corroborate or refute data recovered or obtained from other mobile devices and/or from service provider records.

21) Affiant knows from their training and experience, that it is necessary to search live and deleted data recovered from digital devices from the time when the device was first used through the time when the device was seized. Mobile devices can be used to delete, create, share, and store files and other data including, but not limited to, documents, photographs, videos, electronic mail, search history, financial transactions and other relevant live and deleted user information. This is specifically necessary to establish associations between a particular device and associated applications and files to a particular user (or users). This scope of time is necessary to identify potential inculpatory and exculpatory evidence during the planning, execution and post event activities of potential criminal activity. These activities may include communication, contact, calendar entries, pictures, videos, and location information (including GPS, navigation, and maps). This scope of time is also necessary to determine accurate device date and time settings, including time zone changes, and to determine if the date and time settings are correct and if they are set to synch or not synch with the network. Affiant knows from their training and experience that it is important to understand events of a particular day and time in proper context that may exist months before certain criminal acts and to attribute particular users of a device and associated applications when the device was initially setup.

22) Affiant knows from their training and experience, the date and time the device was first set up is an important detail in a forensic exam. Activation establishes when user accounts, eSIM profiles, Apple or Google IDs, biometric profiles, and device security settings were first configured. Setup data can also show whether the device was erased, restored, or transferred between users or devices. Full access to the device is required to compare internal timestamps with provider records and verify the accuracy of the device's recorded history. Understanding activation timing helps determine who initiated device use, whether that user is connected to the offense timeframe, and whether additional users or co-conspirators were involved.

23) That affiant is aware that the proliferation of mobile phones in society has led to the increase in their use in and connected to criminal activity; that the examination and analysis of all telecommunications equipment has become an important aid to law enforcement in the investigation of crime including their utilization of communication devices, their use of coded communications, and their use of false or fictitious identities; that affiant is also aware that in today's society, people utilize various electronic media in numerous aspects of their lives; that criminals also use a host of electronic media in facilitation of their unlawful activities and that modern and current technology relative to cellular phones permits suspects to commit crimes and store evidence of crimes in their cellular phones.

24) That affiant has also found it incredibly common for crime suspects to use their cellular telephones to communicate aurally, through social media interactions, internet research or via electronic message in "text" format with co-actors and / or co-conspirators during the planning, execution and post stages of the crimes they commit; therefore records contained within said cellular telephones may provide evidence related to the identity of said co-actors and / or co-conspirators.

25) That affiant has found it incredibly common for crime suspects to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and other instrumentalities of crimes; furthermore, that these photographs and visual depictions are typically kept and maintained on their cellular devices. These individuals, whether through intent or circumstance, frequently capture or cause to be taken photographs and other visual depictions featuring themselves, associates, and the illegal items they control, possess, buy, or sell. These incriminating photographs and visual depictions are commonly found residing on their cellular devices, further emphasizing the pivotal role of mobile technology in both criminal activities and subsequent investigations. Further, that affiant has also found it incredibly common for crime suspects to use cellular telephones to communicate aurally or via electronic message in "text" format with individuals whom intend to commit various crimes.

26) Affiant knows that records maintained by the service provider, specifically cell tower data, can assist investigators in determining a phone's location at the time calls are made with the phone. Therefore, affiant believes that by obtaining the information contained within the recovered phone(s) will assist investigators in linking the phone(s) to call detail records and other information that may be sought in this investigation through cellular phones service providers which may also document the location of the cell phones during the time period of the crime(s) described in this affidavit, further assisting investigators with identifying the actors, co-actors and co-conspirators.

27) Affiant has consistently depended on the expertise of forensic cellular phone examiners within the law enforcement community. From these professionals, affiant has gained valuable insights comparing the intricacies of electronic device extractions to the structure of a house. Much like a dwelling, which relies on interconnected systems such as plumbing, electricity, water, and sewage for functionality, the extraction process for electronic devices involves accessing multiple databases, files, and folders. This comprehensive approach ensures that the device becomes operable for further examination.

28) Because modern cell phones are complex and constantly changing, it is not possible to know in advance every type of data that may be extracted from a mobile device. What is stored on a phone depends on the user, the device, and the applications in use. Many types of information such as messages, photos, location data, and application activity are stored across different parts of the device. Attempting to list every possible artifact ahead of time risks excluding relevant evidence simply because the device can store information in an unexpected manner, including potentially exculpatory evidence.

29) Individual artifacts, standing alone, may not have evidentiary significance. However, when multiple artifacts are considered together, they may corroborate one another and provide important information about user activity. Digital evidence is often validated through the relationship between different data points, such as system activity, application usage, security or authentication events, and location information. For example, a photograph by itself may have limited evidentiary value but when combined with data showing that the device was unlocked using biometric authentication, that the camera application was active at the relevant time, and that location data places the device at a specific location during the relevant time, those artifacts, taken together, may corroborate one another and provide the context about how and when the photograph was created.

30) Affiant knows that forensic examinations of mobile devices are complicated and time-consuming tasks that require specialized equipment and expertise. Affiant knows that recognized digital forensic examination practices ordinarily require digital forensic analysts to first acquire an exact copy of the contents of the hard drive of the mobile device being examined and then examine that copy using specialized computer software. Affiant knows that the acquisition of a forensic copy of the mobile device requires use of specialized computer equipment and can take hours, depending on the capacity of the hard drive or storage device and the amount of data present on it. Affiant knows that the analysis of the forensic copy by the digital forensic analyst relies on using sophisticated digital forensic software tools, ordinarily also takes hours, and is best accomplished in a law enforcement-controlled environment.

31) Modern digital devices and media can contain many gigabytes and even terabytes of data. Due to the potential for an extremely large volume of data contained in devices and media, and that fact that evidence can be stored/located in unanticipated locations or formats and/or embedded in other items stored on the device/media, forensic examiners typically need to use specialized equipment in their search. Such large volumes of data also mean that searches can take days or even weeks to complete. Mobile devices store data in complex, interwoven structures, making it challenging to extract specific items without encompassing the entirety of the device. Furthermore, information and files are often distributed across different segments of the device's memory, linked through various databases and metadata. Attempting to extract only specific items while preserving their integrity and context proves to be impractical in the face of these intricate data structures. Therefore, a comprehensive extraction approach remains essential for a thorough and successful forensic investigation.

32) Based upon affiant's training and experience, and affiant's work with forensic analysts and/or trained investigators, affiant knows that when cell phones are downloaded or there is a data extraction/analysis, the entirety of the data on the cell phone is typically downloaded. Not only is this the mechanism of extraction based upon the standards in the field, but it is also necessary because the data being sought can be located in any storage area on the cell phone. Use of creation dates or file names to narrow the search of particular data may be ineffective because the dates intentionally and unintentionally can be changed with movement or storage of files, and file names may be changed by the user or the operating system. Further, the dates may be inaccurate based upon the date set on the cell phone itself and investigators would have to look at other indicators of the date and time of the data. For example, date and timestamps on mobile devices may not necessarily correspond to the occurrence of a specific event or moment. Instead, they often signify the installation or update of an application, the timing of a text message or photograph capture, or the download of a photograph or document. Importantly, users retain the ability to conceal evidence within the device by selectively deleting data or manipulating databases within the file system or specific applications. The search of a cell phone is similar to the search of any other area. When there is probable cause that evidence of a crime exists in the cell phone, the analyst will typically capture the data on the cell phone to search all areas that may contain the information authorized in the warrant in a forensically sound environment. Data storage on an individual cell phone is specific to the user and setup of the cell phone will require, in any case, a complete analysis of the downloaded data in its entirety to determine whether the sought-after evidence is present.

33) Affiant knows it is necessary to search live and deleted data recovered from an electronic device from when the electronic device was first activated to when the device was seized. Live data consists of information on the phone that is actively changing while the device is powered on such as running applications, temporary files and other data that may be lost or altered if the phone is turned off or continues to operate. This is specifically necessary to establish that a particular electronic device and any associated applications can be attributed to a particular user. Additionally, this full range of time may be necessary to identify communications, contacts, calendar entries, pictures, videos, location information (including chats, texts, web searches, GPS, navigation, maps, and other data) that may convey communication between parties and identify suspects, co-conspirators, associates, witnesses and other individuals who may be involved or have knowledge of crimes and to establish planning, execution, and post-event information of criminal activity. Without this information, it may not be possible to understand events of a particular day and time in proper context and/or to identify the user(s) of the device.

34) This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cell phone was used, the purpose of the use, who used the device, and when. Affiant knows the following based on training and experience and work with forensic analysts and/or investigators:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium, but has since been deleted or edited, or a deleted portion of a file. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a phone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal historical information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB storage devices or other external storage media, and the times the phone was in use. Phone file systems can record information about the dates files were created and the sequence in which they were created.

b) The forensic evidence on a cell phone can indicate who has used or controlled a device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. As established in this affidavit, probable cause exists to believe evidence of a crime(s) is located in the cell phone. Therefore, investigators need to establish to whom the evidence is attributed by determining who possessed or had access to the cell phone. Because cell phones can be possessed, owned, and used by multiple people, establishing that an individual was in possession of a cell phone at some point is insufficient. The entirety of the contents of the cell phone must be analyzed to attribute an individual to the cell phone by identifying patterns of possession, control, and use over a period of time. Contents of a cell phone used to establish the identity of the owner and/or user include photographs and videos, text messages, email messages and accounts, contacts logs, website searches, documents, applications, and associated accounts.

c) Data on the storage medium can also contain password "keys," which allow a cell phone to access cloud or other remotely stored data.

RETENTION OF FORENSIC IMAGES AND EXTRACTIONS

35) For the technical reasons described, the digital evidence listed above may be submitted for digital forensic processing.

36) The government will retain a forensic image or forensic extraction of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Dated 22 day of January, 2026.

IW Brett Mendola

Brett Mendola
Investigator

Minerva Salas-Sanchez NOTARY PUBLIC STATE OF WISCONSIN

Subscribed and sworn to before me
this 22 of January 2026.

Minerva Salas-Sanchez

Minerva Salas-Sanchez
Notary Public, State of Wisconsin, Milwaukee County
My Commission ~~is permanent~~ expires 8/19/2027