

2023 SW000425NC

STATE OF FLORIDA)
 12TH JUDICIAL CIRCUIT) SEARCH WARRANT (GOOGLE LLC)
 COUNTY OF SARASOTA)

THIS ORDER IS ISSUED PURSUANT TO SECTION 92.605, FLORIDA STATUTES. A
 RESPONSE IS DUE WITHIN 20 BUSINESS DAYS OF RECEIPT OF THIS ORDER
 UNLESS A LONGER TIME PERIOD IS STATED HEREIN.

IN THE NAME OF THE STATE OF FLORIDA, to all and singular the Sheriffs and
 their Deputies, the Director of the Florida Highway Patrol and his Troopers, the
 Commissioner of the Florida Department of Law Enforcement and his Designees, the
 Director of the Florida Fish and Wildlife Conservation Commission and his Officers, and
 Constables, Municipal Police Officers and State Attorney's Investigators all acting within
 their jurisdiction;

WHEREAS, I have received affidavit for search warrant, on this date made before
 me by the Affiant, Detective/Officer A. Cox 1746, who has prepared same in his/her
 capacity as a law enforcement officer; and

WHEREAS, the stated Detective/Officer having been placed under oath and
 having sworn to the facts as stated therein, and having examined the said facts set forth in
 support of said application for search warrant, and the facts contained therein which are
 now incorporated herein by reference and made a part of this Warrant, and;

WHEREAS, said facts so made known to me by such affidavit as set forth, have caused
 me to certify and find that there is probable cause to believe that the laws of the State of
 Florida relative to prohibiting Sexual Battery (Mentally Incapacitated), controlled by
 Florida State Statute 794.011(4)(b), has been violated by Christian Ziegler, and the
 officer has reason to believe and does believe that evidence connected with the crime is
 currently located within the below identified Google account.

A user account identified by Unique Google ID: christianmziegler@gmail.com

This account is under the control of: Google LLC.

Attention: Custodian of Records

Google LLC.

1600 Amphitheatre Parkway

Mountain View, CA 94043

Email: USLawEnforcement@google.com

THEREFORE, the Court having found that Google is an out-of-state corporation
 that provides electronic communication services or remote computing services to the
 public and pursuant to Florida Statutes § 92.605 and § 934.23, as well as the United

States Code 18 U.S.C. § 2703, and California Statute § 1524.2, a Judge of the Circuit Court of Florida has jurisdiction to issue a search warrant for a Google account, consequently these presents are to command you, with the proper and necessary assistance, either in the day time or in the night time, as the exigencies of the situation may demand or require or on Sundays, or holidays, to enter the said Google account described above, and diligently search said account and seize as evidence any of the following:

PROPERTY TO BE PROVIDED BY GOOGLE LLC.

1. Stored electronic communications or files associated with the user accounts identified as Google User ID: **christianmziegler@gmail.com** and any related accounts concerning the same account subscribers or users, since creation of such account until the date of production, including but not limited to:
 - a. content and header information of email or other messages and any attachments;
 - b. user contact information, group contact information;
 - c. IP logs, and instant messages if any, whether drafted, sent, received, opened or unopened, read or unread, and/or forwarded; and
 - d. any buddy lists or contact lists, calendars, transactional data, account passwords or identifiers, and/or any other files related to that account;
2. Records concerning the identity of the user of the above-listed user account(s); consisting of name, postal code, country, e-mail address, date of account creation, IP address at account sign-up, logs showing IP address, and date stamps for account accesses.
3. Any photo prints linked to or associated with the above-listed user account(s). The photo prints are to include a compilation of all photos and or videos uploaded by the user that have not been deleted, along with all photos and videos uploaded by any user that has the user tagged in them.
4. Any additional video and/or images uploaded or downloaded to the account with any associated metadata, timestamps, and IP addresses associated with the upload or download, as well as any transactional logs that show user interaction with the videos/images.
5. Stored Android backups;
6. Stored web bookmarks, web history, and autofill data that are stored under this account;
7. Files stored in the Google Drive related to this account, to include shared folders that are accessible by this account;
8. Files stored in the Google Photos related to this account, to include shared folders that are accessible by this account with any associated metadata (EXIF), timestamps, IP addresses associated with the upload or download, any transactional logs that show user interaction with the videos/images;

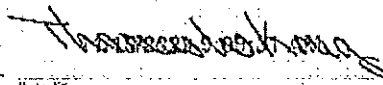
9. Google Hangouts conversation content and history associated to this account;
10. Any additional Google Account or Google Play account, to include; account information, and account history;
11. Any location history including global positioning coordinates;
12. Google wallet/checkout service information; and
13. Installed application, device make(s), model(s) and international mobile identification number (IMEI) or mobile equipment identifier number (MEID) for Google account.

YOU ARE FURTHER DIRECTED to bring the property so seized before a court having jurisdiction to be disposed of and dealt with according to law and make return of your doings under this warrant to me or to my designated clerk, and give proper receipts for any property taken hereunder, and deliver a copy of this warrant to the person at whom directed.

GIVEN UNDER MY HAND AND SEAL THIS DAY

11/15/2023

DATE



SIGNATURE/ELECTRONIC SIGNATURE

1710

JBT

IN THE CIRCUIT COURT OF THE 12TH JUDICIAL CIRCUIT IN AND FOR
SARASOTA COUNTY, FLORIDA

APPLICATION FOR COURT ORDER/SEARCH WARRANT COMPELLING
PRODUCTION OF GOOGLE RECORDS

In Re: A Criminal Investigation

Case No. 23-048937

A user account identified by:

Unique Google ID: Email: christianmziegler@gmail.com

This account is under the control of: Google LLC.

Attention: Custodian of Records

Google LLC.

1600 Amphitheatre Parkway

Mountain View, CA 94043

Email: USLawEnforcement@google.com

BEFORE ME, a Judge of the Circuit Court, personally or by sworn attestation appeared Detective/Officer A. Cox #1746, a duly sworn law enforcement officer of the Sarasota County Sheriff's Office, State of Florida, who after being first properly sworn, makes application for an order compelling Google to search for, and obtain, and to provide information and data in the above described Google account to the applicant Detective/Officer listed above, who states under oath that he/she has sufficient grounds to believe and does believe that the laws of the State of Florida have been violated by Christian Ziegler, to-wit:

The laws prohibiting Sexual Battery (Mentally Incapacitated) controlled by Florida State Statute 794.011(4)(b), has been violated, and the officer has reason to believe and does believe that evidence connected with the crime is currently located within the below identified Google account.

THE DESCRIPTION OF THE USER ACCOUNT is as follows:

A user account identified by Unique Google ID: Email: christianmziegler@gmail.com

GROUND FOR ISSUANCE:

The following grounds for issuance of the Order Compelling Production of Google Records, as required by Florida Statutes exist, to-wit: the evidence sought is relevant to proving the above described offense has been committed and such evidence is contained

within the Google account described above. See Florida Statute 933.02(3). Google, is an out-of-state corporation that provides electronic communication services or remote computing services to the public. Your Affiant seeks to seize the below-described evidence pursuant to Florida Statute § 92.605 and § 934.23, as well as the United States Code 18 U.S.C. 2703, and California Statute § 1524.2, which compel out-of-state electronic communication service or remote computing service that provides such services to the public to provide information requested pursuant to search warrants, court orders or subpoenas issued in the State of Florida.

FACTS STATED IN SUPPORT OF APPLICATION:

Your Affiant has sufficient reasonable grounds to believe that the above-named crime has been committed and that evidence in the form of electronic communication and or data held or possessed by Google may be discovered for the following reasons:

1. Your Affiant has been employed with the Sarasota Police Department since April 2015. Your Affiant is assigned to the Criminal Investigation Division unit and has been in this unit for 4 years., specializing in Crimes against Children and all other crimes against persons or property. Your Affiant is tasked with conducting computer-related investigations and examining digital evidence.

THE FOLLOWING FACTS SUPPORT YOUR AFFIANT'S PROBABLE CAUSE:

1. On 10/04/23, the victim [REDACTED] reported she had been sexually assaulted by Christian Ziegler on 10/02/23. The victim was treated and examined at Sarasota Memorial Hospital where a sexual assault kit was completed. The sexual assault occurred at the victim's apartment [REDACTED].
2. On 10/05/23, Detectives began the investigation which revealed the following. The victim and Christian Ziegler have known each other for twenty years. On 10/02/23, the victim and Christian Ziegler agreed to have a sexual encounter that included Christian's wife Bridget Ziegler. When the victim learned that Bridget could not make it, she changed her mind and cancelled with Christian. On 10/02/23, the victim opened her apartment door to walk her dog and Christian was standing outside in the hallway. Christian entered the apartment, bent the victim over the bar stool and vaginally penetrated her with his penis. The victim advised Christian did not wear a condom, and he stated "I'm leaving the same way I came in." The victim said she, Christian and Bridget were sexually involved one time over a year ago at their house. The victim stated that when Christian came over, she was not in a place to consent because it was her day off and she had been drinking Tequila all day. The victim advised she called her twin sister [REDACTED] and told her she was raped. [REDACTED] immediately went to the victim's house.
3. Detectives interviewed [REDACTED] who confirmed her sister called her and told her she was raped but did not tell her who did it. [REDACTED] said her sister (victim) was very emotional and distraught.

4. On 10/24/23, Detective viewed the video surveillance footage from the victim apartment complex. The video captured Christian Ziegler arriving in his gray Ford truck bearing FL., tag SRQG0P on 10/02/23, at 1429 hours. Christian immediately entered the apartment complex, is seen coming off the elevator and driving away in the parking lot at 1507 hours. Christian was wearing dark shorts and a red shirt.
5. As part of the investigation, Detectives performed a digital extraction on the victim's cell phone. Detectives located several digital messages from Christian to the victim on 10/02/23 starting at 0729 hours. In the messages Christian told the victim to go to Instagram. The victim said Christian liked to use Instagram because he conceals the messages using vanish mode.
6. In another message he asked the victim for her address and told her they were driving around referring to him and Bridget. Christian continued sending the victim messages, but she did not respond in a timely manner. When the victim finally responded she asked who was coming. At 1412 Christian said "Prob just me this time now. Was ready at 1:30." Christian was referring to Bridget being ready at 1:30. At 1424 hours, the victim responded "Sorry I was mostly in for her" referring to Bridget.
7. On 10/27/23, Detectives learned that Christian was trying to contact the victim by sending her messages via Instagram. Detectives and the victim began communicating with Christian via controlled/recorded messages. The following is a summary of the communication:
 - Victim: I'm not okay with what happened the other day between us.
 - Christian: Oh. That's not good. You are my friend. Known ya for like twenty years now. Lol. Note: Christian goes on to talk about how long they have been friends.
 - Victim: Yeah I know but that was not cool and you didn't bring her and then did that to me.
 - Christian: She was in. Then couldn't because no response. She said in next time. But I understand. Your my friend I actually like you as a person, so sorry you got upset, but I can leave you alone if you prefer. Note: Christian then tried to change the conversation to getting his hair cut.
 - Victim: I don't know if I can do that anymore after what you did to me last time it freaked me out.
 - Christian: Ok. Well, sorry. Not the intention. I want you to be happy and not have drama. You have dealt with enough BS. Note: Christian again tried to change the subject by talking about getting a haircut.
 - Victim: I have not been able to work since you came over.
 - Christian: I am pretty loyal to my friends. Tried to call. Hard to text. How can I help?
 - Victim: I really can't even talk to you right now.

During the messaging, Christian continuously asked how he could help, and the victim responded, "You caused this. You can't help me." Christian repeatedly referred to the victim as his friend in an effort to minimize the situation; he would deflect by trying to change the subject when confronted.

- Victim: I'd prefer you to tell me why you think what you did was okay?
- Christian: Where r u? Wanna meet and chat? Worried about you. You are my friend.
- Victim: Hell no not after what you did to me. Do you not understand I am terrified of you? Christian responded that he had to go soon.

Christian then began calling the victim. The calls were audio recorded.

In the first phone call the victim told Christian he hurt her when he came over. Christian said he did not think that was the case and if she was upset, he did not need her upset. Christian tried to change the subject, and the victim asked why he did that. Christian said he was not trying to start any issues, and she knows who he is. Christian asked the victim if she wanted him to leave her alone. The victim said she needed him to know that he hurt her. Christian responded by saying he would leave her alone.

In the second controlled phone call, the victim called Christian back. When he answered the phone, the victim asked him why he forced her to have sex with him when she never wanted to. Christian said he has never done that then said he had to go because some guy was giving him a hard time. Christian asked the victim if she wanted him to call her later and she said no.

In the third controlled phone call, Christian called the victim. Christian started asking the victim what she was going through. The victim told Christian he sexually assaulted her. Christian said, "Those are big words, please don't, no I didn't. You invited me in, that's it. I did not at all, and I never want you to feel that way." Christian went on to say the victim was his friend and asked her what she needed. Christian asked the victim if she needed financial help or anything else. Christian asked the victim what the issue was. The victim responded twice that he was the issue. Christian told the victim she was his friend, and he apologized for whatever is going on. Christian said he did not need any drama, and he did not want to create any issues for her, and if she was upset with him, he would leave her alone. Christian told the victim she was a good person, and he would leave her alone. The victim asked Christian to help her understand why he came over. Christian responded that he thought she wanted him to come over. The victim said no, I told you not to. Christian said that's not true. The victim asked Christian to acknowledge that he has been using her all these years. Christian said he was not going to acknowledge that, and he asked her if she was recording him. Christian said the victim was trying to get him on record saying something. Christian once again asked the victim what he could do to help her. The victim told Christian to leave her alone. End of call.

8. On 11/01/23, Detectives interviewed Bridget Ziegler. Bridget confirmed that she knew the victim through her husband. Bridget confirmed having a sexual encounter with the victim and Christian over a year ago and that it only happened one time.
9. On 11/02/23, Detectives interviewed Christian Ziegler with his attorney present. Christian advised he had consensual sex with the victim, and that he took a video of the encounter on 10/02/23 of the victim. Christian said he initially deleted the video, but since the allegation, he uploaded the video to his Google Drive. Which we have not been able to locate upon a digital extraction.
10. Based on the above information, I believe a search warrant for the content stored on Google's servers for data relating to the Gmail address:
christianmziegler@gmail.com will lead to locating evidence of the crime, and will authenticate the date, time, and location of when the video was created.
11. Google is a web service provider that provides users the ability to communicate with other users by various means; this includes the ability to email, post videos, and past photographs for others to view and to keep privately stored; messaging services to communicate directly between users; and sharing of media between users, among other services.
12. Your Affiant knows from experience that items can be synced to multiple electronic devices including mobile devices, by the installation and use of the application Google Drive. Specifically, Google Drive is a cloud-based storage service that enables users to store and access files online. The service syncs stored documents, photos, and more across all the user's devices, including mobile devices, tablets, and PCs. These files can be saved on a folder and synced across any device that Google Drive is installed on, thus allowing the user to access these files on any device at any time.
13. Your Affiant knows from experience that Google Drive is one of Google's cloud-based storage services that allows customers to access videos, photos, and documents from their mobile devices and Mac or Windows personal computers. It also enables customers to back up the data within the Google Drive folder which as a result allows the information and data from the customer's device stored by Google to be available offline.
14. Your Affiant knows from training and experience that iPhones, iPads, Androids, and **Apple iPhone 15 Pro Max** are devices that can have Google Drive installed. Specifically, Android based device have Google Drive installed automatically when the device is purchased and activated.
15. Your Affiant knows from training and experience that searches and seizures of electronic communications evidence may require the seizure of most, or all communications currently stored to be processed later. Furthermore, you Affiant believes that there is no way to minimize or narrow the focus of the items being

requested herein and this data can only be narrow after you Affiant has an opportunity to search all of the data being stored within the aforementioned Google Drive account.

16. Because the out-of-state electronic communication service or remote computing service provider has no reasonable means to distinguish evidence of the crimes from any other records contained within the sought-after account, your Affiant seeks to compel the service provider to seize a copy of all records pertaining to the account and provide the entirety of the records to your Affiant. Once your Affiant has obtained those records, your Affiant and/or other representatives of his/her agency shall conduct an actual search of the items obtained from the out-of-state electronic communication service or remote computing service provider in order to sort the evidence of the violations articulated above and specifically sought herein, which may be intermingled with innocent or innocuous documents or records.

On the basis of the foregoing facts, Affiant believes the following evidence may be found:

INFORMATION AND DATA SOUGHT BY LAW ENFORCEMENT


PROPERTY TO BE PROVIDED BY GOOGLE LLC.

1. Stored electronic communications or files associated with the user accounts identified as Google User ID: **Email: christianmziegler@gmail.com** and any related accounts concerning the same account subscribers or users, since creation of such account until the date of production, including but not limited to:
 - a. content and header information of email or other messages and any attachments;
 - b. user contact information, group contact information;
 - c. IP logs, and instant messages if any, whether drafted, sent, received, opened or unopened, read or unread, and/or forwarded; and
 - d. any buddy lists or contact lists, calendars, transactional data, account passwords or identifiers, and/or any other files related to that account;
2. Records concerning the identity of the user of the above-listed user account(s); consisting of name, postal code, country, e-mail address, date of account creation, IP address at account sign-up, logs showing IP address, and date stamps for account accesses.
3. Any photo prints linked to or associated with the above-listed user account(s). The photo prints are to include a compilation of all photos and or videos uploaded by the user that have not been deleted, along with all photos and videos uploaded by any user that has the user tagged in them.
4. Any additional video and/or images uploaded or downloaded to the account with any associated metadata, timestamps, and IP addresses associated with the upload or

download, as well as any transactional logs that show user interaction with the videos/images.

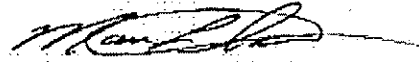
5. Stored Android backups;
6. Stored web bookmarks, web history, and autofill data that are stored under this account;
7. Files stored in the Google Drive related to this account, to include shared folders that are accessible by this account;
8. Files stored in the Google Photos related to this account, to include shared folders that are accessible by this account with any associated metadata (EXIF), timestamps, IP addresses associated with the upload or download, any transactional logs that show user interaction with the videos/images;
9. Google Hangouts conversation content and history associated to this account;
10. Any additional Google Account or Google Play account, to include, account information, and account history;
11. Any location history including global positioning coordinates;
12. Google wallet/checkout service information; and
13. Installed application, device make(s), model(s) and international mobile identification number (IMEI) or mobile equipment identifier number (MEID) for Google account.

WHEREFORE, your Affiant respectfully requests that a Search Warrant be issued commanding all and singular the Sheriffs and their Deputies, the Director of the Florida Highway Patrol and his Troopers, the Commissioner of the Florida Department of Law Enforcement and his designees, Constables and Municipal Police Officers and State Attorney's Investigators acting within their jurisdiction, with proper and necessary assistance, to search the above described Google account in a manner consistent with F.S. S. § 92.605 and California Penal Code §15.24.2, by delivering said warrant via facsimile or U.S. mail to an authorized legal representative of Google, and to seize any and all of the aforesaid property found by virtue of such Search Warrant and to list the property seized on a return and inventory, to be filed within this Judicial Circuit within ten days of this date.


Detective Angela Cox #1746
Affiant / Signature
Electronic Signature

STATE OF FLORIDA)
COUNTY OF SARASOTA)

The foregoing instrument was acknowledged before me this 13th day of November 2023, by the individual whose name and signature appear above, and who is personally known to me and who did take an oath.



Detective Maria Llovio #1312
Signature/Electronic Signature
Law Enforcement Officer
Notary Public, State of Florida

2023 SW 001012 MC
 IC. Chase

IN THE CIRCUIT COURT OF THE 12TH JUDICIAL CIRCUIT IN AND FOR
 SARASOTA COUNTY, FLORIDA

SEARCH WARRANT
 (CELLULAR TELEPHONE)

IN THE NAME OF THE STATE OF FLORIDA, to all and singular the Sheriffs and their Deputies, the Director of the Florida Highway Patrol and his Troopers, the Commissioner of the Florida Department of Law Enforcement and his Special Agents, the Director of the Florida Fish and Wildlife Conservation Commission and his Officers, and Constables, Municipal Police Officers and State Attorney's Investigators all acting within their jurisdiction.

WHEREAS, I have received affidavit for search warrant, on this date made before me by the Affiant, Detective Angela Cox #1746 who has prepared same in his/her capacity as a law enforcement officer; and

WHEREAS, the Detective/Officer having been placed under oath and having sworn to the facts as stated therein, and having examined the said facts set forth in support of said application for search warrant, and the facts contained therein which are now incorporated herein by reference and made a part of this Warrant, and;

WHEREAS, said facts so made known to me by such affidavit as set forth, have caused me to certify and find that there is probable cause to believe that the laws of the State of Florida relative to: Sexual Battery pursuant to Florida Statute 794.011(4)(b) "Mentally Incapacitated" have been violated by Christian M. Ziegler, W/M, DOB 05/27/1983 and that evidence of the crime is currently located at or within the below described cellular telephone(s).

THE DESCRIPTION AND LOCATION OF THE CELL PHONE(S) TO BE SEARCHED is as follows: Cellular phone belonging to Christian Ziegler, telephone number 202-731-7213. The cellular device is currently located in the custody of Christian Ziegler. The aforesaid location is within the jurisdictional boundaries of Sarasota County.

THEREFORE, these presents are to command you, with the proper and necessary assistance, including off-site forensic cellular telephone analyst experts, either in the daytime or in the nighttime, as the exigencies of the situation may demand or require or on Sundays, or holidays, to search the said cellular telephone(s) described above, and seize as evidence any of the following:

EVIDENCE SOUGHT:

1. All data regarding the target device identity information including the assigned phone number, serial number, make, model, IMEI, carrier, and owner information.²
2. All data regarding text communication including SMS, MMS, and 3rd party application communication whether incoming, outgoing, and drafts including any associated metadata.
3. All data regarding contacts including any associated logs and metadata.
4. All data regarding call log history, including incoming, outgoing, missed, and dialed and any associated metadata.
5. All data regarding images, videos, and audio files, including any associated metadata.
6. All data regarding web history, including web sites visited, internet searches, web bookmarks, internet cookies, downloaded data, and any associated metadata.
7. All data regarding emails whether incoming, outgoing and drafts and associated metadata.
8. All data regarding GPS locations, location information, longitude and latitude data, cell tower locations, Wi-Fi connections, Bluetooth connections, hot-spot connections, including any associated metadata.
9. All data regarding documents, installed applications, autofill data, user accounts, passwords, PINs, notes, pattern locks, financial transaction records, credit card numbers, including any associated metadata.
10. In order to successfully complete a forensic extraction from a mobile device, it may be necessary to repair the device, replace the display screen, replace the chassis, replace the battery, and repair or replace switches and other components that are necessary to make the device operational. It may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include, but are not limited to, brute-force attack methods, third party proprietary services and methods, destructive and potentially destructive processes such as gaining root and/or super-user level access, and employing methods such as JTAG, ISP and chip-off in order to extract data.

² While the search warrant being sought does not contain a time period or date restriction, it does contain a subject-matter limitation, which also satisfies the 4th Amendment particularity requirement. See *United States v. Bucuvalas*, 970 F. 2d 937, 942 n. 7 (1st Cir. 1992), abrogated on other grounds by *Cleveland v. United States*, 531 U.S. 12 (2000); *Libretti v. Woodson*, 2013 WL 6634249 (N.D. Ohio 2013), *United States v. Kernell*, 2010 WL 1491873 (E.D. Tenn. 2010), and *United States v. Ogden*, 2008 WL 2247074 (W.D. Tenn. 2008). Because a forensic search of a cell phone does not involve the use of search parameters, but instead requires an examiner using one or more specialized devices to extract all cell phone data -- including deleted items -- and display same in a human-readable format designed by the creator of the extraction software, date restrictions cannot be used in the forensic examination of a cell phone. A date restriction is also impractical because the dates associated with deleted files that have been restored during a successful extraction are oftentimes unavailable.

- 11. The executing law enforcement officer(s) may enlist the aid of a law enforcement computer forensic laboratory and/or certified digital forensic examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of all of the information described.
- 12. Digital items listed in this warrant may have associated content that is stored remotely on a server(s) at a third-party electronic service provider. If seized, Law enforcement will return with a second warrant request to search these items.

If any of the same be found in said object, you are hereby authorized, with proper and necessary assistance (to include forensic computer analyst experts), to seize and secure same, to make return of your doings under this Warrant within ten (10) days of the date hereof. You may conduct an off-site forensic examination for the data listed in this warrant. You are likewise to give proper receipt for said property, and to deliver a copy of this Warrant to the person from whom the item was taken, or the person in charge of the item, or in the absence of any such person, to leave a copy of this Warrant in the place where said property was found.

This Warrant authorizes the seizure of electronic storage media and/or the seizure or copying of electronically stored information. This Warrant further authorizes a later review of the media or information. The 10-day timeframe for executing the warrant in accordance with the provisions of Section 933.05, Florida Statutes, refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

GIVEN UNDER MY HAND AND SEAL THIS DAY

11/1/2023

Click or tap here to enter text.

DATE

Thomas J. King

Thomas J. King
Circuit Judge
CIRCUIT JUDGE 12TH JUDICIAL CIRCUIT
SIGNATURE/ELECTRONIC SIGNATURE

IN THE CIRCUIT COURT OF THE 12TH JUDICIAL CIRCUIT IN AND FOR
SARASOTA COUNTY, FLORIDA

SEARCH WARRANT
AFFIDAVIT & APPLICATION
(CELLULAR TELEPHONE)

BEFORE ME, a Judge of the Circuit Court, personally or by sworn attestation appeared Affiant Detective Angela Cox. Your affiant is a duly sworn law enforcement officer of the Sarasota Police Department, State of Florida, who after being first properly sworn, deposes and says that he has probable cause to believe and does believe that the laws of the State of Florida have been violated, to-wit:

The laws prohibiting Sexual Battery controlled by Florida State Statute 794.011(4)(b) "Mentally incapacitated" have been violated by Christian M. Ziegler, W/M, 05/27/1983.

That the officer has reason to believe and does believe that evidence connected with the crime is currently located within the below described cellular telephone.

THE DESCRIPTION AND LOCATION OF THE CELLULAR TELEPHONE(S) TO
BE SEARCHED:

The cellular phone belonging to Christian Ziegler, telephone number 202-731-7213 and any and all digitally stored data on the device.

The cellular device is currently located in the custody of Christian Ziegler.

The aforesaid location is within the jurisdictional boundaries of Sarasota County.

GROUND(S) FOR ISSUANCE:

The following grounds for issuance of a Search Warrant, as required by Florida Statutes exist, to-wit:

Florida Statutes provides that a warrant to search an item, structure, or conveyance other than a dwelling may be issued when any property constitutes evidence relevant to proving that a felony has been committed. See Florida Statute 933.02(3).

PROBABLE CAUSE FOR ISSUANCE:

Your Affiants have probable cause to believe that the above-named crime has been committed and that evidence may be discovered for the following reasons:

1. Your Affiant has been employed with the Sarasota Police Department since April 2015. Your Affiant is assigned to the Criminal Investigation Division unit and has been in

this unit for 4 years, specializing in Crimes against Children and all other crimes against persons or property.

2. On 10/04/23, the victim [REDACTED] reported she had been sexually assaulted by Christian Ziegler on 10/02/23. The victim was treated and examined at Sarasota Memorial Hospital where a sexual assault kit was completed. The sexual assault occurred at the victim's apartment [REDACTED]
3. On 10/05/23, Detectives began the investigation which revealed the following. The victim and Christian Ziegler have known each other for twenty years. On 10/02/23, the victim and Christian Ziegler agreed to have a sexual encounter that included Christian's wife, Bridget Ziegler. When the victim learned that Bridget could not make it, she changed her mind and cancelled with Christian. On 10/02/23, the victim opened her apartment door to walk her dog and Christian was standing outside in the hallway. Christian entered the apartment, bent the victim over the bar stool and vaginally penetrated her with his penis. The victim advised Christian did not wear a condom, and he stated, "I'm leaving the same way I came in." The victim said she, Christian and Bridget were sexually involved one time over a year ago at their house. The victim stated that when Christian came over, she was not in a place to consent because it was her day off and she had been drinking Tequila all day. The victim advised she called her twin sister [REDACTED] and told her she was raped [REDACTED] immediately went to the victim's house.
4. Detectives interviewed [REDACTED] who confirmed her sister called her and told her she was raped but did not tell her who did it [REDACTED] said her sister (victim) was very emotional and distraught.
5. On 10/24/23, Detective viewed the video surveillance footage from the victim's apartment complex. The video captured Christian Ziegler arriving in his gray Ford truck bearing FL tag SRQG0P on 10/02/23, at 1429 hours. Christian immediately entered the apartment complex. He is seen coming off the elevator and driving away in the parking lot at 1507 hours. Christian was wearing dark shorts and a red shirt.
6. As part of the investigation, Detectives performed a digital extraction on the victim's cell phone. Detectives located several digital messages from Christian to the victim on 10/02/23 starting at 0729 hours. In the messages, Christian told the victim to go to Instagram. The victim said Christian liked to use Instagram because he conceals the messages using vanish mode.
7. In another message, he asked the victim for her address and told her they were driving around referring to him and Bridget. Christian continued sending the victim messages, but she did not respond in a timely manner. When the victim finally responded she asked who was coming. At 1412 Christian said, "Prob just me this time now. Was ready at 1:30." Christian was referring to Bridget being ready at 1:30. At 1424 hours, the victim responded, "Sorry I was mostly in for her" referring to Bridget.

8. On 10/27/23, Detectives learned that Christian was trying to contact the victim by sending her messages via Instagram. Detectives and the victim began communicating with Christian via controlled/recorded messages. The following is a summary of the communication:

- Victim: I'm not okay with what happened the other day between us.
- Christian: Oh. That's not good. You are my friend. Known ya for like twenty years now. Lol. Note: Christian goes on to talk about how long they have been friends.
- Victim: Yeah I know but that was not cool and you didn't bring her and then did that to me.
- Christian: She was in. Then couldn't because no response. She said in next time. But I understand. Your my friend I actually like you as a person, so sorry you got upset, but I can leave you alone if you prefer. Note: Christian then tried to change the conversation to getting his haircut.
- Victim: I don't know if I can do that anymore after what you did to me last time it freaked me out.
- Christian: Ok. Well, sorry. Not the intention. I want you to be happy and not have drama. You have dealt with enough BS. Note: Christian again tried to change the subject by talking about getting a haircut.
- Victim: I have not been able to work since you came over.
- Christian: I am pretty loyal to my friends. Tried to call. Hard to text. How can I help?
- Victim: I really can't even talk to you right now.

During the messaging, Christian continuously asked how he could help, and the victim responded, "You caused this. You can't help me." Christian repeatedly referred to the victim as his friend in an effort to minimize the situation, he would deflect by trying to change the subject when confronted.

- Victim: I'd prefer you to tell me why you think what you did was okay?
- Christian: Where r u? Wanna meet and chat? Worried about you. You are my friend.
- Victim: Hell no not after what you did to me. Do you not understand I am terrified of you? Christian responded that he had to go soon.

Christian then began calling the victim. The calls were audio recorded.

In the first phone call the victim told Christian he hurt her when he came over. Christian said he did not think that was the case and if she was upset, he did not need her upset. Christian tried to change the subject, and the victim asked why he did that. Christian said he was not trying to start any issues, and she knows who he is. Christian asked the victim if she wanted him to leave her alone. The victim said she needed him to know that he hurt her. Christian responded by saying he would leave her alone.

In the second controlled phone call, the victim called Christian back. When he answered the phone, the victim asked him why he forced her to have sex with him when she never wanted to. Christian said he has never done that then said he had to go because some guy was giving him a hard time. Christian asked the victim if she wanted him to call her later and she said no.

In the third controlled phone call, Christian called the victim. Christian started asking the victim what she was going through. The victim told Christian he sexually assaulted her. Christian said, "Those are big words, please don't, no I didn't. You invited me in, that's it. I did not at all, and I never want you to feel that way." Christian went on to say the victim was his friend and asked her what she needed. Christian asked the victim if she needed financial help or anything else. Christian asked the victim what the issue was. The victim responded twice that he was the issue. Christian told the victim she was his friend, and he apologized for whatever is going on. Christian said he did not need any drama, and he did not want to create any issues for her, and if she was upset with him, he would leave her alone. Christian told the victim she was a good person, and he would leave her alone. The victim asked Christian to help her understand why he came over. Christian responded that he thought she wanted him to come over. The victim said no, I told you not to. Christian said that's not true. The victim asked Christian to acknowledge that he has been using her all these years. Christian said he was not going to acknowledge that, and he asked her if she was recording him. Christian said the victim was trying to get him on record saying something. Christian once again asked the victim what he could do to help her. The victim told Christian to leave her alone. End of call.

9. On 11/01/23, Detectives interviewed Bridget Ziegler. Bridget confirmed that she knew the victim through her husband. Bridget confirmed having a sexual encounter with the victim and Christian over a year ago and that it only happened one time.
10. Based on the above information, Affiant has reason to believe that evidence of the crime will be found within the cellular phone device belonging to Christian Ziegler telephone number 202-731-7213.
11. Your Affiant knows from other investigations that it is common for a suspect, in advance of criminal activity, to communicate about their motives and plans via text message, phone calls, emails, or through other communication programs/applications/platforms, and also to utilize an electronic device's access to the internet to research information that may play a role in the person's plan or motive for the crime to be committed.
12. Your Affiant also knows from other investigations it is common for a suspect, post crime, to communicate about their recently committed criminal activity with other suspects or accomplices via text message, phone calls, emails, or through other communication programs/applications/platforms, and also to utilize an electronic device's access to the internet to research information that may assist the suspect in disposing of evidence, a path of flight/getaway from the crime and/or to coordinate a

meeting location with other suspects in order to discuss the recently committed crimes in an attempt to thwart law enforcements efforts.

13. Your Affiant knows through his training and experience as a criminal investigator that individuals who participate in such crimes communicate via cellular telephones, text messages, calls, emails, etc.
14. Your Affiant also knows cellular devices such as iPhones/Androids continuously scan their environment for the best signal, which generally comes from the closest cell site and thus records and stores the phone's location.
15. Additionally, your Affiant knows that cellular devices such as an iPhones/Androids also have the ability to and routinely do store satellite-based location data within the phone when a user opens certain applications, sends messages over cellular data or does other tasks on the iPhones/Androids.
16. Two-way communication is a term used to express any form of sent or received communication between two electronic devices. This includes, but is not limited to the following: e-mails, text messages, data messages, picture messages, dialed phone calls, incoming phone calls, and missed phone calls.
17. Text messages are a vernacular term for two-way communication between mobile device systems which contain words, symbols, pictures, and files. Text messages include SMS (short message service), MMS (multimedia messaging service), iMessage, Data Messaging, and various other applications which express communication across visible letters between electronic devices. iMessage is the most common way to communicate between iPhones, which is data based in internet activity.
18. With my training and experience, your affiant knows cellular telephones, and the stored data, may be important to a criminal investigation because they may contain evidence or fruits of the crime.
19. Databases within the phone can be integrated and correlated to each other making it unrealistic to simply remove certain data sections of a cellular phone to extract evidence sought during a data extraction. It is not feasible, with the nature of current technology, to only extract specific sections of a cell phone during a cell phone data extraction and guarantee all the sought evidence is properly and completely extracted.
20. Based on the aforementioned facts, your Affiant believes that probable cause exists to show Christian Ziegler's cellular phone, an AT&T carrier, #202-731-7213 which is currently in Christian Ziegler's custody; contains valuable evidence relevant to the subject matter of this warrant.

THE ROLE OF CELLULAR TELEPHONES IN CRIMINAL ACTS:

A cellular telephone is a long-range, electronic device used for mobile voice or data communication over a cellular network of specialized base stations known as cell sites. The cell sites are interconnected to the public switched telephone network (PSTN), which is most commonly associated with fixed/stationary telephones that were in use for the majority of the twentieth century.

A smartphone is a cellular telephone that has Wi-Fi and cellular connectivity. It can shoot videos, take photographs, play music, send, and receive email, browse the web/internet, send text messages, and receive voicemail. Smartphones are also used for banking, as well as scheduling appointments through their calendar operations. Other smartphone functions – video games, GPS navigation, social networking, etc. – can be enabled by downloading application programs.

A typical smartphone feature is the contact/name and address book, an internal database used for storing entries called contacts. Each contact entry typically consists of a few standard fields (e.g., first name, last name, company name, address, telephone number, e-mail address, fax number, and mobile phone number). Most smartphones store the details in alphabetical order of the individuals' names.

Additionally, the contact/name and address book of a suspect's cell phone can provide information relevant and material to a criminal investigation. Such information can include leads relating to the names of individuals associated with the suspect, who may themselves: (a) know of the suspect's role in the offense(s) under investigation, and/or (b) have participated in the offense(s).

Affiant also knows that smartphones and the data stored in same may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. In this case, the warrant application requests permission to search and seize electronically stored data and images as the stored data and images constitute evidence of a crime.

Furthermore, I know that if location data is enabled on a cell phone, a unique set of metadata is assigned. This metadata is able to show the origin, capture time, and real time GPS location in which a photograph or video is taken, or from where a message is sent. Additionally, this location-based metadata would show an approximate location where the cell phone was at a given date and time depending on the defendant's usage of the phone.

Based on the Affiant's training and experience, it is common for a suspect to use his or her smartphone to make and/or receive calls while in the area of a crime that he or she is committing.

Based on Affiant's training and experience, the text message feature of a smartphone has proven increasingly popular in recent years. "Text messaging" or "texting" is the practice of sending short text messages from cellular telephones or similar devices to their intended recipients. According to a September 2010 report by the Pew Research Center, as of May 2010, 72 percent of adults in the United States who own cell phones use their phones' "texting" features. See: Cell Phones and American Adults by clicking [HERE](#). That same report notes that "[a]dults who text typically send and receive a median of 10 texts a day; teens who text send and receive a median of 50 texts per day."

Affiant has further learned that when a smartphone user "deletes" data on his or her smartphone, the data is not actually erased, but is instead retained in the smartphone's memory until overwritten when additional memory space is needed by the device. This process leaves deleted data retrievable by digital evidence experts, sometimes long after the data has been deleted.

The aforementioned crimes are still under investigation and the evidence sought may corroborate information already known and/or provide additional leads for further investigation.

NECESSITY TO REMOVE CELLULAR TELEPHONE TO CONDUCT A THOROUGH SEARCH

This affidavit also requests permission to seize the cellular telephone hardware that may contain the stored data if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the cellular telephone is a container for evidence and an instrumentality of the crime under investigation.

Based upon my knowledge, training, and experience, I know that searching and seizing information from a cellular telephone often requires agents to seize the object to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

(1) The volume of evidence. Cellular telephones can store the equivalent of hundreds of pages of information. Searching this vast amount of information is a very time-consuming task. This sorting process can take an extended period of time and require special cellular telephone software, and it would be impractical and invasive to attempt this kind of data search on-site.

(2) Technical Requirements. Searching a cellular telephone for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because cellular telephone evidence is vulnerable to inadvertent or intentional modification or destruction, a controlled environment may be necessary to complete an accurate analysis. Data recovery techniques used with forensic examination

of cellular telephones have been proven effective in recovering data long after its creation, transmission, or receipt.

(3) Necessity to Establish a Timeline. It is important in investigations of this manner to place the suspect with the cellular telephone at the time of the offense. Since this evidence must frequently be proven circumstantially, the forensic examiner may need to compile a timeline of cellular telephone files that were altered by the phone's use at or near the time of the offense. An analysis of such files may provide evidence that the suspect was utilizing his or her cellular telephone in the appropriate time frames. This is analogous to reviewing a suspect's telephone records to prove he was at home at the time of the offense.

In light of these concerns, your Affiant hereby requests the Court's permission to search the cellular telephone that is believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the cellular telephone for the evidence described below.

EVIDENCE SOUGHT:

1. All data regarding the target device identity information including the assigned phone number, serial number, make, model, IMEI, carrier, and owner information.¹
2. All data regarding text communication including SMS, MMS, and 3rd party application communication whether incoming, outgoing, and drafts including any associated metadata.
3. All data regarding contacts including any associated logs and metadata.
4. All data regarding call log history, including incoming, outgoing, missed, and dialed and any associated metadata.
5. All data regarding images, videos, and audio files, including any associated metadata.
6. All data regarding web history, including web sites visited internet searches, web bookmarks, internet cookies, downloaded data, and any associated metadata.
7. All data regarding emails whether incoming, outgoing and drafts and associated metadata.

¹ While the search warrant being sought does not contain a time period or date restriction, it does contain a subject-matter limitation, which also satisfies the 4th Amendment particularity requirement. See *United States v. Bucuvalas*, 970 F. 2d 937, 942 n. 7 (1st Cir. 1992), abrogated on other grounds by *Cleveland v. United States*, 531 U.S. 12 (2000), *Libretti v. Woodson*, 2013 WL 6634249 (N.D. Ohio 2013), *United States v. Kernell*, 2010 WL 1491873 (E.D. Tenn. 2010), and *United States v. Ogden*, 2008 WL 2247074 (W.D. Tenn. 2008). Because a forensic search of a cell phone does not involve the use of search parameters, but instead requires an examiner using one or more specialized devices to extract all cell phone data -- including deleted items -- and display same in a human-readable format designed by the creator of the extraction software, date restrictions cannot be used in the forensic examination of a cell phone. A date restriction is also impractical because the dates associated with deleted files that have been restored during a successful extraction are oftentimes unavailable.

8. All data regarding GPS locations, location information, longitude and latitude data, cell tower locations, Wi-Fi connections, Bluetooth connections, hot-spot connections, including any associated metadata.
9. All data regarding documents, installed applications, autofill data, user accounts, passwords, PINs, notes, pattern locks, financial transaction records, credit card numbers, including any associated metadata.
10. In order to successfully complete a forensic extraction from a mobile device, it may be necessary to repair the device, replace the display screen, replace the chassis, replace the battery, and repair or replace switches and other components that are necessary to make the device operational. It may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include, but are not limited to, brute-force attack methods, third party proprietary services and methods, destructive and potentially destructive processes such as gaining root and/or super-user level access, and employing methods such as JTAG, ISP and chip-off in order to extract data.
11. The executing law enforcement officer(s) may enlist the aid of a law enforcement computer forensic laboratory and/or certified digital forensic examiner(s) in the searching, viewing, photographing, recording, copying, forensic imaging, and analysis of all of the information described.
12. I also know that digital items listed in this warrant may have associated content that is stored remotely on a server(s) at a third-party electronic service provider. If seized, I will return with a second warrant request to search these items.

On the basis of the foregoing facts, Affiant believes the above-described evidence may be found.

WHEREFORE, your Affiant respectfully requests that a Search Warrant be issued commanding all and singular the Sheriffs and their Deputies, the Director of the Florida Highway Patrol and his Troopers, the Commissioner of the Florida Department of Law Enforcement and his Special Agents, the Director of the Florida Fish and Wildlife Conservation Commission and his Officers, Constables, Municipal Police Officers and State Attorney's Investigators all acting within their jurisdiction, either in the day time or night time, as the exigencies of the occasion may demand or require, or on Sunday, or holidays with proper and necessary assistance, including using forensic cellular telephone analyst experts off-site to search the above described cellular telephone(s), and seize as evidence any of the above mentioned items or any other evidence relating to the subject matter of this warrant that could be used in further violation of, or has been used in violation of the laws of the State of Florida in order that evidence may be procured to be used in the prosecution of the Criminal Laws of the State of Florida.

Affiant / Signature
Electronic Signature

STATE OF FLORIDA)
COUNTY OF SARASOTA)

The foregoing instrument was acknowledged before me this 01 day of November, 2023, by the individual whose name and signature appear above, and who is personally known to me and who did take an oath.

X *Detective Maria [Signature]* 1312

Signature/Electronic Signature
Law Enforcement Officer
Notary Public, State of Florida

RETURN TO SEARCH WARRANT

RECEIVED THIS WARRANT on the 01 day of November,
A.D., 2023, and EXECUTED the same on the 02 day of November,
A.D., 2023, by READING THIS WARRANT TO, and delivering a true COPY hereof
to one Christian Ziegler (or by leaving a
COPY at the premises), and seizure of the item(s) described previously. Upon
the completion of said SEIZURE, a WRITTEN INVENTORY OF THE PROPERTY
seized was delivered to the aforementioned PERSON (or such a copy was left at the
premises). A TRUE and CORRECT LIST of the item(s) seized is set forth in the following
INVENTORY:

iPhone 15 Black in color

I, Angela Cox, the officer by whom this
WARRANT was executed, DO SWEAR that the above INVENTORY contains a TRUE
AND DETAILED ACCOUNT of all the PROPERTY seized by me on said WARRANT.

x Angela Cox
AFFIANT

(SEAL) x M. Clivio 1312
DET. M. CLIVIO

SWORN TO AND SUBSCRIBED BEFORE ME THIS THE 02 day of
November, A.D., 2023.