

IN THE TWELFTH JUDICIAL CIRCUIT COURT  
IN AND FOR SARASOTA COUNTY, FLORIDA

CHRISTIAN ZIEGLER,  
BRIDGET ZIEGLER,  
Plaintiff,

v.

CASE NO. 2024 CA 001409 NC  
DIVISION C CIRCUIT

OFFICE OF THE STATE ATTORNEY  
FOR THE TWELFTH JUDICIAL  
CIRCUIT,  
SARASOTA POLICE DEPARTMENT,  
Defendant.

---

**FINAL JUDGMENT**  
**IN FAVOR OF CHRISTIAN AND BRIDGET ZIEGLER**

Law enforcement seized and searched the entire contents of Christian Ziegler’s cell phone, Google Drive, and Instagram account through a series of three search warrants. As it turns out, these warrants were severely overbroad. And there was no seizure protocol to guide law enforcement’s search of Mr. Ziegler’s property. Law enforcement’s handling of the three overbroad warrants were patently unreasonable and violated Mr. Ziegler’s constitutional rights.

For example, law enforcement rifled through 250,000+ photographs and 30,000+ videos, seizing an indeterminant amount despite concluding they showed no evidence of a crime. They also seized more than 1,200 text communications between Mr. Ziegler and his wife, most of which transpired two years before the alleged criminal incident arose on October 2, 2023. Almost all of these communications had no connection to the crime being investigated. Law enforcement also seized other personal information about Mr. Ziegler with no apparent nexus to the crime investigated.

Cellphones today can contain a person’s entire life story. Law enforcement agents euphemistically described the unlimited search and seizure of Mr. Ziegler’s cellphone data to be “best practice.” But 250 years ago, our forebears fought a Revolution against the tyrannical policies of King George III, including the allowance of general warrants that permitted unreasonable search and seizure. While today’s seizure is not from the entirety of one’s home—but 18 square inches of a cellphone and the content of electronic storage media—it is functionally the same. The Fourth Amendment prohibits general warrants like those advanced by law enforcement in this case.

Mr. Ziegler never was arrested, and all investigations into alleged criminal conduct are over. Joined by his wife, Mr. Ziegler wants the return of his personal property that law enforcement seized involuntarily from him based on the three warrants. To make the return meaningful, Mr. Ziegler wants to regain exclusive possession and control of his data, which he

says cannot occur if his property is publicly disseminated because of Florida’s public records law.

The Intervenors say the Zieglers have no standing to make this request or even access the courts at all. Even if the Zieglers can go to court, say the Intervenors, they have no remedy or ability to prevent the release of the content of the items taken from Mr. Ziegler due to Florida’s broad public record laws. Intervenors are mistaken.

This ruling is long. But the short answer is this: Mr. Ziegler has the constitutional right to recover exclusive control over his personal property seized involuntarily through unconstitutional warrants. His property is not transformed into public record because it was not “made or received pursuant to law” and is outside the “official business” of law enforcement. Because Mr. Ziegler’s personal property is not public record, there is no legal impediment to restoring exclusive possession of Mr. Ziegler’s property to Mr. Ziegler.

Just because the Zieglers may be high profile figures in our community does not mean they have surrendered their constitutional rights. If the contents of an unconstitutional search and seizure allowed by a warrant became a public record simply by virtue of the government’s possession of that material, the Fourth, Fifth, and Fourteenth Amendments’ protections would be functionally nullified. And the entire contents of every cellphone searched and seized based on a warrant issued by a state judge in Florida would also be a public record.

The Court understands the particular interest in this case: the intersection of the Zieglers’ public profile and the nature of the allegations virtually guarantees interest. Despite the intense public interest, the rule of law must apply equally to all. Instead of Mr. Ziegler, what if the cellphone belonged to the Executive Editor of a well-known media outlet and it contained the confidential identity of sources that had nothing to do with the crime being investigated? Should a search of the phone’s contents via an overbroad warrant then convert the confidential identity of sources to a “public record”? If the Intervenor Defendants’ position prevailed, the answer to this question would be “yes,” and the Executive Editor would have no legal recourse to contest the public dissemination of that information. The Court vehemently disagrees.

The Court grants Mr. Ziegler the relief he requested as explained in this Judgment.

## 1.

### **BACKGROUND AND PROCEDURAL HISTORY**

The Sarasota Police Department (“SPD”) investigated Mr. Ziegler for sexual battery based on his sexual activity with Jane Doe (“Ms. Doe”) on October 2, 2023. After concluding there was no crime for sexual battery, SPD investigated Mr. Ziegler for video voyeurism based on a video Mr. Ziegler made of the October 2 encounter.

During its investigation, SPD obtained three separate warrants to search Mr. Ziegler’s cellphone, Google Drive, and Instagram account. Ultimately, SPD referred only a charge of video voyeurism to the State Attorney’s Office and provided that office with a limited set of documents from Mr. Ziegler’s cellphone. (Trial Exhibit Q is the list containing the documents

physically provided by SPD to the State Attorney's Office.) The State Attorney's Office declined to prosecute Mr. Ziegler based on insufficient evidence.

The Zieglers are public officials, and there is substantial public and media interest in the contents contained within the seized items. There have been public record requests, including a request for the entirety of the contents of the seized items. Some items have been produced; others have not.

The Zieglers filed this action on March 15, 2024, seeking to regain exclusive possession of Mr. Ziegler's property and to prevent public disclosure of the contents of the seized items, including through public record requests. Their verified amended complaint [DIN 5] includes four counts, and they sued the City of Sarasota and the State Attorney's Office for the Twelfth Judicial Circuit. Both the City and State Attorney's Office have answered and raised affirmative defenses [DINs 45 and 50, respectively].

Counts 1 and 3 seek a declaratory judgment against the City and State Attorney's Office that the contents of the seized materials were obtained through unreasonable search and seizures and are not public records. Counts 2 and 4 seek to preclude the public dissemination of this material and to destroy this material in the hands of the City and State Attorney's Office. By doing this, the Zieglers say Mr. Ziegler would regain exclusive possession of his personal property.

The Court entered a temporary injunction enjoining the City and the State Attorney's Office from any further release of the documents or data seized from Mr. Ziegler's cellphone, Google Drive, or Instagram account that had not been previously publicly released [DIN 14, p. 5, ¶¶ 3, 4].

The Court on its own motion expedited all further proceedings [DIN 14, p. 5, ¶ 1].

Many intervenors who filed public record requests asked to participate [DINs 6, 11, 16, and 17]. The Court granted all of these requests, allowing Michael Barfield; the Florida Center for Government Accountability, Inc.; and a collection of six media outlets, Gannett Co., Inc., The McClatchy Company, LLC, Nextstar Media Group, Inc., Scripps Media, Inc., TEGNA Inc., and Times Publishing Company to intervene as Intervenor Defendants [DIN 24]. The Court authorized them to file pleadings, motions, and briefs, and to participate in all hearings and trial.

Intervenor Michael Barfield moved to dismiss the amended complaint [DIN 34], and the other Intervenor Defendants joined that motion. After hearing, the Court denied the motion to dismiss. The Court specifically concluded that the Zieglers had standing to bring this lawsuit [DIN 52]. The Court set the final hearing to occur on May 16, 2024 [DIN 38]. Mr. Barfield also sought to dissolve the temporary injunction [DIN 34], but he decided not to seek a hearing on that motion because the Court set the final hearing to occur the following month. That request to dissolve the temporary injunction is now abandoned with the entry of this Final Judgment.

The Intervenor Defendants answered the amended complaint and raised a number of defenses [DINs 44, 58, 60]. Each of the Intervenor Defendants attached a list of documents

provided by SPD to the State Attorney's Office, which list ultimately was introduced into evidence as Exhibit Q. Although they focused on obtaining the items referenced in Exhibit Q, at trial their request was broader and included, at a minimum, any item SPD detectives marked with the F7 key during SPD's review of Mr. Ziegler's property.

The Intervenor Defendants have also filed crossclaims seeking enforcement of Florida's Public Record Act [DINs 53, 61, 70]. By the time of trial, the crossclaims were not at issue and have not yet been tried. The day before the trial, the Court held a hearing, making clear that only the amended complaint would be heard at trial. The crossclaims, not being at issue, could not and would not be addressed during that trial. In essence, the Court severed the crossclaims from the amended complaint.

On May 16, 2024, the Court conducted the trial on the amended complaint. Five individuals testified live, and one individual testified by deposition. Plaintiffs introduced the three warrants as Exhibits 1-3. The Intervenor Defendants introduced 19 exhibits, identified as Exhibits A-S. The City and State Attorney's Office did not introduce any independent exhibits.

At the conclusion of the trial, the Court took the matter under advisement. During trial, the parties discussed, but did not resolve, whether the Court would need to conduct an *in camera* inspection of certain items reviewed by SPD and the State Attorney's Office. The Court deferred during trial. Later, after trial, the Court requested those documents for a potential *in camera* inspection of the materials identified in Paragraphs 15 and 16 of Exhibit Q [DIN 128].

Ultimately, the Court conducted an *in camera* inspection of some but not all of the items delivered. The Court reviewed *in camera* the communications between Mr. and Mrs. Ziegler—the items identified in Paragraph 15 of Exhibit Q. The Court did not conduct an *in camera* inspection of the Video—the item identified in Paragraph 16 of Exhibit Q—because, as explained later in this Final Judgment, the Court finds that Mr. Ziegler voluntarily provided the Video to law enforcement and there is no constitutional violation with SPD's acquiring the Video.

## 2. FINDINGS OF FACT

Based on the evidence from trial, the Court finds as fact—

1. Plaintiffs Christian and Bridget Ziegler have been continuously married since 2013. Each is active in local and state politics. In October 2023, Mr. Ziegler was the Chairman of the Republican Party of Florida and previously was a member of the Sarasota County Commission. Mrs. Ziegler is a sitting member of the School Board of Sarasota County, and she is a sitting member of the Board of Supervisors for the Central Florida Tourism Oversight District.

2. On October 4, 2023, a friend of the undisclosed "Jane Doe" reported to SPD that Ms. Doe had been sexually assaulted on October 2, 2023. The friend requested SPD perform a welfare check on Ms. Doe. SPD found Ms. Doe under the influence of alcohol and extremely

distraught at her apartment. Ms. Doe was taken to the hospital for a sexual assault examination. She was initially reluctant to identify an alleged assailant.

3. During a subsequent SPD interview with Ms. Doe, Ms. Doe alleged that Mr. Ziegler had contacted her on October 2, 2023, about getting together for sex. Ms. Doe agreed to potential sexual activity with Mr. and Mrs. Ziegler that day. When Mr. Ziegler later informed Ms. Doe that his wife would not be participating, Ms. Doe alleges she told him not to come. A short time after cancelling the liaison, Ms. Doe opened her door and found Mr. Ziegler standing there. Ms. Doe stated Mr. Ziegler entered her apartment, forced her over a bar stool, and sexually assaulted her.

4. Ms. Doe showed SPD detectives text messages on her phone confirming that Mr. Ziegler told her it was, “Prob just me this time now,” and her response, “Sorry I was mostly in for her.”

5. Detectives obtained the surveillance video from Ms. Doe’s apartment complex for October 2, 2023, and observed Mr. Ziegler arriving in his vehicle at 2:29 p.m., walking into the building, and leaving at 3:07 p.m.

6. During the subsequent investigation, detectives observed communication between Mr. Ziegler and Ms. Doe. SPD had Ms. Doe perform at least three controlled calls between she and Mr. Ziegler. None of these calls produced any incriminating admissions from Mr. Ziegler.

7. On November 1, 2023, detectives interviewed Mrs. Ziegler. She cooperated with law enforcement and advised she did not know about the prearranged October 2d rendezvous. She told detectives she knew Ms. Doe and previously participated in sexual activities with Ms. Doe and Mr. Ziegler. Mrs. Ziegler cooperated with SPD. There is no evidence, though, that Mrs. Ziegler ever agreed to turn over her text communications with her husband.

8. Also on November 1, 2023, SPD Detective Cox (lead detective) and Sergeant Riffe (investigative commander and Detective Cox’s supervisor) began to interview Mr. Ziegler concerning the sexual battery allegation. Mr. Ziegler suspended the interview to hire an attorney. See Ex. E. Mr. Ziegler retained criminal defense attorney Derek Byrd.

9. Mr. Ziegler met with Mr. Byrd around noon on November 1, 2023, and showed him a video of the sexual encounter (“the Video”) with Ms. Doe which, in both Mr. Ziegler’s and Mr. Byrd’s opinions, exonerated Mr. Ziegler of the alleged sexual battery.

10. Mr. Byrd, who knew Sergeant Riffe, called him at approximately 1:30 p.m. on November 1, 2023. This is the same day SPD began its interview with Mr. Ziegler. Mr. Byrd told Sergeant Riffe about the Video and that it exonerated Mr. Ziegler. During that call, Mr. Byrd and Sergeant Riffe agreed to meet at Mr. Byrd’s office at 8:00 a.m. the next morning to show the Video to SPD and permit further interview of Mr. Ziegler.

11. Detective Cox testified that she was aware of the planned November 2 meeting but did not recall being told of the Video. Sergeant Riffe testified that he told Detective Cox of

his call with Mr. Byrd and that the purpose of the meeting the next morning was to observe the Video.

12. By 1:30 p.m. on November 1, 2023, SPD had actual knowledge of Mr. Ziegler's possession of the Video and the claim it exonerated Mr. Ziegler.

13. At 9:49 p.m. on November 1, 2023, Detective Cox sent to the State Attorney's Office via email a proposed warrant for review that sought to search and seize Mr. Ziegler's cellphone. Detective Cox identified she was investigating an alleged violation of section 794.011(4)(b), sexual battery by a person 18 years of age or older upon a person 18 years of age or older under the circumstance that the victim was mentally defective. Although SPD knew at that time that Mr. Ziegler had the Video in his possession and that he contended it exonerated him, SPD did not inform the State Attorney's Office of that fact. The State Attorney's Office approved the warrant for submission at 10:30 p.m. that night. A judge of this Court signed the warrant before midnight that same day. See Exs. S and 1.

14. Detective Cox's affidavit in support of the warrant did not reference Mr. Byrd's call to Sergeant Riffe regarding the forecasted exonerating Video. See Ex. 1. In fact, the affidavit did not contain any mention that SPD was meeting with Messrs. Ziegler and Byrd at 8:00 a.m. the next day.

15. While the affidavit affirmed that, in Detective Cox's training and experience, evidence of a crime may be found in the phone's messaging programs, phone calls, historical cell tower and GPS data, it did not indicate that the phone's photo or video storage applications could also contain evidence. Id.

16. The warrant ***broadly and without limitation*** authorized the search of Mr. Ziegler's phone and the seizure of ***all data*** contained on the phone, including all communication, contacts, photos, videos, audio files, web history, historical location data, data regarding documents, autofill data, user account data, passwords, PINs, financial transaction records, and credit card numbers. Id.

17. On November 2, 2023, Sergeant Riffe, Detective Cox, Detective Llovio, Mr. Byrd, Mr. Ziegler, and another unidentified person met. See Ex. F. Mr. Ziegler showed SPD the Video. After SPD asked about when the Video was created, Mr. Byrd asked if they could provide the cellphone to SPD for the limited purpose of verifying the Video's date and time. See Ex. F at p. 21. SPD declined this offer and, instead, served the search warrant authorizing them to seize Mr. Ziegler's phone. Id. at p. 22.

18. At the time SPD seized Mr. Ziegler's cellphone, SPD told Mr. Ziegler that the entire cellphone would be downloaded but assured him that they would use software to limit their search to "look at what you told us, the Video. We're going to try and tailor that down, as Mr. Byrd explained, to look to see when that video was created" and to attempt to find the message where Ms. Doe asked Mr. Ziegler if his wife enjoyed the video. Id. at p. 23.

19. This explanation of the scope of SPD's search was all that was provided to Mr. Ziegler as his attorney then waived reading of the warrant. *Id.* at p. 30. Mr. Ziegler also explained that the Video did not reside on his cellphone but instead was in cloud storage. *Id.* at p. 29.

20. SPD downloaded the entire contents of Mr. Ziegler's cellphone into a software program identified as Cellebrite. This program allows detectives to search the cellphone's contents for key words and to review text messages, documents, photos, and videos. When detectives reviewed the contents of Mr. Ziegler's cellphone and saw something they felt may require further review, the detectives would mark those files by hitting the F7 key on the keyboard.

21. Mr. Ziegler's cellphone contained the most data of any cellphone extraction previously performed by SPD. It took approximately 5 days to download because SPD's software kept crashing given the enormous quantity of data taken. Detective Cox testified that Mr. Ziegler's cellphone contained more than a terabyte of data, including 30,000 videos and 250,000 photographs. There was also a substantial number of text messages.

22. Detective Cox and another detective reviewed each of the videos and photographs, regardless of when they were created or the contents of them. In other words, law enforcement reviewed videos and photographs created years before the alleged sexual battery, even if they had nothing to do with Ms. Doe. Detective Cox used the F7 key to identify files which on her initial cursory review were of interest and potentially needed further review. Detective Cox testified these images and videos marked with the F7 key ***did not depict Ms. Doe or any apparent criminal activity***. Instead, SPD uploaded them into Evidence.com regardless, for the off chance they might subsequently prove to contain evidence of prior bad acts relating to other crimes. This, of course, was not identified in the warrant.

23. SPD detectives also sought to review any text, social, or other type of messages stored on Mr. Ziegler's cellphone either mentioning or involving Ms. Doe. Despite this announced self-limitation, the reviewed messages were not constrained to this scope. Again, the use of the F7 key flagged messages greatly exceeded what would be relevant—either inculpatory or exculpatory—for the alleged crime being investigated, as identified in the warrant.

24. SPD was not able to locate the Video on Mr. Ziegler's cellphone. SPD detectives, therefore, prepared another warrant for the purpose of obtaining the Video. This November 13, 2023 warrant was directed to Google, LLC, for the entire contents of Mr. Ziegler's Google Drive ***since the inception of his account***. The wide-scope of this request sought data including, but not limited to: all communication, account access information, all photos uploaded by Mr. Ziegler, all photos in *any* Google Drive where Mr. Ziegler was tagged, all phone back-ups, web bookmarks and browsing history, stored autofill data, all files stored in the account, all files shared with Mr. Ziegler via Google Drive, historical GPS data, Google Hangouts conversation content, and wallet information. *See* Ex. 2. Like the original warrant, the crime identified was an alleged violation of section 794.011(4)(b), sexual battery by a person 18 years of age or older upon a person 18 years of age or older under the circumstance that the victim was mentally defective. The date of the alleged crime was October 2, 2023.

25. Despite having viewed the Video in Mr. Byrd's office, Detective Cox's affidavit in support of the Google warrant did not mention this fact or the exculpatory nature of the Video. Instead, Detective Cox wrote:

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 [sic] we have not been able to locate upon a digital extraction.

Ex. 2, pdf. P. 8, ¶8.

26. The affidavit affirmed that Detective Cox believed a search warrant for the entire contents of Mr. Ziegler's Google Drive would "lead to locating evidence of the crime and will authenticate the date, time, and location when the video was created." *Id.* at ¶ 9. Besides this conclusory statement, there was no explanation in the affidavit how information from years prior could authenticate the Video allegedly made on October 2, 2023.

27. Google responded to this warrant and provided SPD with all the requested information. Detective Cox testified that, in her opinion, the Google warrant did not produce any information relevant to SPD's investigation.

28. Despite now having Mr. Ziegler's Google drive, SPD still was unable to locate a copy of the Video. SPD contacted Mr. Ziegler to ask for his help. Mr. Ziegler agreed to show SPD how to access the Video, as he had previously offered on November 2. That meeting took place in a Big Lots parking lot on December 1, 2023. Present were Mr. Ziegler (without his attorney), Detective Cox, Sergeant Riffe, and Brian Yang, SPD's Digital Forensic Specialist. *See* Ex. G.

29. During that December 1, 2023, meeting, Mr. Ziegler voluntarily provided Specialist Yang access to the Video, and Specialist Yang downloaded the Video and associated data. Specialist Yang also took 14 photographs of Mr. Ziegler's cellphone and various images on Mr. Ziegler's cellphone. Mr. Ziegler consented to Specialist Yang taking these 14 photographs.

30. Additionally, during the December 1, 2023 meeting, Mr. Ziegler voluntarily provided SPD with a DNA sample. There was also discussion concerning how Mr. Barfield knew about aspects of the on-going investigation and whether SPD was leaking information concerning the investigation to Mr. Barfield or the media. (Mr. Barfield is an intervenor in this lawsuit.)

31. The Court specifically finds that its voluntariness finding with respect to the Video, the 14 photographs taken by Specialist Yang, and the DNA is made to the clear and convincing evidence standard. Despite the two preceding warrants being unconstitutional (as discussed later in this Final Judgment), given the passage of time and Mr. Ziegler's consent to



meet with SPD personnel on December 1, 2023, the Court finds there was an unequivocal break in the chain of illegal conduct sufficient to dissipate the taint of SPD's illegal actions to make the voluntariness finding.

32. Using the Video's metadata, SPD confirmed that the Video's date and time was consistent with the incident reported by Ms. Doe. SPD ceased investigating Mr. Ziegler for sexual battery; instead, SPD refocused its investigation on an allegation of video voyeurism in violation of sections 810.145(2)(a) and (6)(b), Florida Statutes.

33. While investigating this new alleged crime, on December 8, 2023, SPD prepared and obtained a third search warrant to serve upon Meta/Instagram. SPD sought to determine if Ms. Doe sent Mr. Ziegler a message in vanish mode *after* the October 2d encounter asking Mr. Ziegler if his wife enjoyed the video—evidence that would suggest Ms. Doe agreed to the videoing of their sexual encounter. Despite this date, the warrant sought all information associated with Mr. Ziegler's account and any other account operated by Mr. Ziegler *since its inception* including: messages, buddy lists, contact lists, calendars, transactional data, passwords, wall postings, photographs, videos, historical login information, and journal entries. See Ex. 3.

34. This third warrant affidavit informed the judge that they had observed the Video and Mr. Ziegler "claimed" it was consensual. The affiant, who was not Detective Cox, also stated that during the November 2, 2023, meeting, Mr. Byrd "made mention of a message (on Instagram vanish mode) between the victim and Mr. Ziegler where the victim asked him if he showed his wife the video." Id. at ¶13.

35. SPD served the third warrant on Meta/Instagram, but Detective Cox testified that it did not produce any evidence relevant to their investigation.

36. Mr. Ziegler voluntarily provided the Video to SPD. And Mr. Ziegler voluntarily allowed Specialist Yang to take the 14 photographs of Mr. Ziegler's cell phone. Mr. Ziegler, however, did not consent to providing SPD with the contents of his cellphone, Google Drive, or Meta/Instagram accounts. SPD obtained that data based on the three warrants. SPD's searches and seizures of Mr. Ziegler's property was involuntary from Mr. Ziegler's perspective.

37. On January 19, 2024, SPD referred to the State Attorney's Office a charge of video voyeurism. On March 6, 2024, the State Attorney's Office declined to file a formal charge against Mr. Ziegler for video voyeurism due to insufficient evidence. See Ex. P. In its declination memorandum, the State Attorney's Office noted that Ms. Doe did not recall whether she consented for the Video being taken, and she explained that she possibly allowed Mr. Ziegler to film the October 2, 2023, sexual encounter.

38. Trial Exhibit Q is an index of materials SPD provided the State Attorney's Office associated with SPD's referral of the video voyeurism charge. This list contains 16 separate paragraphs of records. Paragraphs 1-14 previously have been released publicly. The items in Paragraphs 15 and 16 have not been released publicly.

39. Paragraph 15 of Exhibit Q contains 11 separate subparagraphs, lettered a through k. The items in Paragraph 15 were obtained from Mr. Ziegler’s cellphone, which SPD seized from the first warrant while investigating the alleged October 2, 2023, sexual battery. Notably, SPD did not seek a separate warrant to investigate or seize evidence of a video voyeurism crime. And the first warrant did not reference an alleged crime of video voyeurism at all. The items in Paragraph 15 include:

- i. Approximately 1,270 text messages between Mr. and Mrs. Ziegler spanning approximately 408 pages (subparagraphs a-d);
- ii. Screenshot of text between Mr. Ziegler and Ms. Doe (subparagraph e);
- iii. Facebook messages between Mr. Ziegler and Ms. Doe (subparagraph f);
- iv. Call logs between Mr. Ziegler and Ms. Doe (subparagraph g)
- v. “Secret email CZ- Cellebrite extraction report” (subparagraph h);
- vi. “The List—a list of names/pseudonyms placed into various categories” (subparagraph i);
- vii. Mr. Ziegler’s web browsing history 11/1/23 – 11/2/23 (subparagraph j); and,
- viii. A blank Snapchat message from 11/1/23 extraction showing evidence of message sent from Mr. Ziegler to Jane Doe (subparagraph k).

40. Paragraph 16 of Exhibit Q is the Video. As noted above, Mr. Ziegler consented to producing the Video to SPD.

41. In addition to the items in Paragraphs 15 and 16 of Exhibit Q, there are an indeterminate number of photographs, videos, and other material from Mr. Ziegler’s cell phone that were seized by SPD—marked by hitting the F7 key—and uploaded into Evidence.com, which have not been publicly released. This information marked using the F7 key does not contain any evidence of criminal activity.

42. Given the Zieglers’ public profile, SPD’s investigation has generated numerous requests for public access to SPD’s investigative file. At least one of the many requests sought release of all contents of the records seized pursuant to the warrants, including all contents of Mr. Ziegler’s cellphone, Google Drive, and Meta/Instagram account.

43. Mr. Ziegler has never been charged with any crime, and there is no active investigation into his conduct. SPD concluded there was no crime of sexual battery, and the State

Attorney's Office declined to bring formal charges against him for video voyeurism. Mr. Ziegler never was arrested, and thus no criminal court case ever was opened.

44. Mrs. Ziegler never was the subject of any criminal investigation, and she has never been accused of any criminal conduct. Mrs. Ziegler has never consented to the release of her private text messages between herself and her husband.

45. There is no longer any need for law enforcement or the State Attorney's Office to retain the contents of Mr. Ziegler's cellphone, Google Drive, or Meta/Instagram accounts for purposes as evidence against Mr. Ziegler. These items remain in the possession of SPD, and to a lesser extent, the State Attorney's Office.

### 3. STANDING

The Intervenor Defendants hotly contest the Zieglers' standing in this action. The Court in its April 12, 2024 Order [DIN 52], concluded the Zieglers have standing. The Court now provides further analysis of the standing issue.

#### A. Christian Ziegler

The thrust of Plaintiffs' lawsuit is not an action brought under chapter 119, Florida Statutes, to enforce the disclosure of public records. Instead, the main purpose is to adjudicate Mr. Ziegler's request for the return of his private property. Included in that request is Mr. Ziegler demand he regain exclusive control over his electronically stored information ("ESI") seized pursuant to unconstitutional warrants served on his cellphone, Google account, and Meta/Instagram account, where, as here, the government no longer has a legitimate investigative or prosecutorial purpose for their retention.

Putting that more directly, the issue is whether the government must return to Mr. Ziegler his property and not publicly disclose the contents of that property. Only after this issue has been determined will the Court be able to consider whether and to what extent the records are subject to public disclosure and analyze whether there are any applicable exemptions. See Hill v. Prudential Ins. Co. of Am., 701 So. 2d 1218, 1219 (Fla. 1st DCA 1997) ("In determining whether materials are subject to disclosure pursuant to the Florida public records law, the court must perform a two-step analysis. It must first determine whether the documents sought are, in fact, public records and whether the documents are exempt from public disclosure as a result of a constitutional or statutorily created exemption.").

Plaintiffs' Amended Complaint alleges that SPD seized Mr. Ziegler's private information pursuant to the three warrants. See Verified Amended Complaint for Declaratory and Injunctive Relief [DIN 5] at ¶¶ 9, 12, and 15. Plaintiffs further allege that Mr. Ziegler retains a protected privacy interest in those records. Id. at ¶¶ 27-28.

Intervenor Defendants contend that section 933.14, Florida Statutes, provides a procedure for the return of evidence seized pursuant to a search warrant. This remedy, however, is not exclusive, and the Court maintains inherent power to direct the return of seized property to its rightful owner. Moore v. State, 533 So. 2d 924, 925 (Fla. 2d DCA 1988), *citing* Garmire v. Red Lake, 265 So. 2d 2, 5 (Fla. 1972). Indeed, the Court would err if it failed to exercise its inherent power upon receipt of a facially sufficient motion, and an individual may seek mandamus relief if a court wrongfully denied that motion. Butler v. State, 613 So. 2d 1348, 1349 (Fla. 2d DCA 1993).

A facially sufficient motion for the return of property must allege that “the property at issue was his personal property, was not the fruit of criminal activity, and was not being held as evidence.” Bolden v. State, 875 So. 2d 780, 782 (Fla. 2d DCA 2004), *quoting* Durain v. State, 765 So. 2d 880, 880 (Fla. 2d DCA 2000). The person seeking the return must specifically identify the “property at issue” but need not establish proof of ownership in order to allege a facially sufficient motion. Bolden, 875 So. 2d at 782. Where there is no criminal prosecution—as in this case—“the court to which the warrant and property are returned obtains jurisdiction to order its return.” Sawyer v. Gable, 400 So. 2d 992, 994 (Fla. 3d DCA 1981). Interestingly, because there was no arrest—and no criminal court case file—there was no case number within which Mr. Ziegler could file his motion for return of his property.

Here, the Twelfth Judicial Circuit Court issued the warrant, and the Twelfth Judicial Circuit Court is the court with jurisdiction to address the return of Mr. Ziegler’s seized property. This Court has jurisdiction over the seized items. And it is this Court that has jurisdiction to address the disposition of those seized items. The fact the undersigned judge currently sits in the civil division is not material; the undersigned is a judge of the Court that issued the warrant.

Mr. Ziegler more than adequately alleged a facially sufficient claim for the return of his property. As previously noted, Mr. Ziegler alleged ownership of seized ESI in the possession of SPD and the State Attorney’s Office. See Verified Amended Complaint for Declaratory and Injunctive Relief [DIN 5] at ¶¶ 9, 12, 15 and 21. He also alleged that the criminal investigation has concluded with no arrest, charges, or criminal conviction, implying that the records at issue are neither the fruit of criminal activity nor evidence of a crime. Id. at ¶¶ 17, 20.

The Amended Complaint specifically requests an order requiring that the SAO and SPD permanently erase or destroy all ESI seized pursuant to the warrants that are not public records and “grant any other relief that this Court deems just and necessary.” Essentially, the proposed order would once again return exclusive control over the records to Mr. Ziegler and result in the “return” of his property. Mr. Ziegler’s claim is proper.

The Court finds Intervenor Defendants’ “absolutist position” that Mr. Ziegler has no standing to assert his constitutionally protected privacy and property rights pursuant to the Fourth Amendment to be without merit. See Florida Freedom Newspapers, Inc. v. McCrary, 520 So. 2d 32, 34 (Fla. 1988) (rejecting media’s absolutist position that a criminal defendant had no standing to enforce the constitutional right of a fair trial by seeking a prohibition of public dissemination of public records). Suggesting that a citizen may not even access the courts to enforce a constitutional right is a stunning proposition.

The public's right to public records "does not extinguish an individual's constitutional and statutory rights in private information." O'Boyle v. Town of Gulf Stream, 257 So. 3d 1036, 1042 (Fla. 4th DCA 2018). In fact, neither article I, section 24 nor the Public Record Act is "a zero-sum choice between personal liberty and governmental accountability." Id. The Florida Supreme Court previously has determined the location of a person's private information existing on a government's electronic system does not automatically transform that private information into a public record. State v. City of Clearwater, 863 So. 2d 149 (Fla. 2003) (city employee's use of government email for private message does not transfer that email into a public record). In other words, "[c]ommon sense . . . opposes a mere possession rule." Id. at 154 (*quoting* trial judge's order; alterations in original).

In Roberts v. News-Press Pub. Co., Inc., 409 So. 2d 1089, 1094 (Fla. 2d DCA 1982), the Second District posed the critical question: "If, then, there are federal constitutional rights of nondisclosure, . . . what is the process by which those rights . . . are to be exercised?" Id. at 1094. The Roberts court answered this question by ruling that when a statutory exemption or constitutional right of nondisclosure is a personal right, it may be protected only by the individual asserting the right "and not by the custodian of the file." Id.

Returning to this case, not only does Mr. Ziegler assert ownership of the ESI at issue, but he also alleges that the three warrants the government used to seize these records (i.e., the entire contents of his cellphone, information stored in his Google Drive account from its inception, and information contained in his Meta/Instagram accounts from its inception) were unconstitutionally overbroad. If true, the ESI may have been seized in violation of Mr. Ziegler's Fourth Amendment rights and further disclosure may also implicate Fourteenth Amendment protections against arbitrary or unjustifiable state deprivations of personal property. Ironically, had Mr. Ziegler been criminally charged, he would have had a well-established forum in the criminal case within which to seek suppression based on a violation of the Fourth Amendment. That Mr. Ziegler never was arrested nor criminally charged cannot preclude Mr. Ziegler from vindicating the violation of his constitutional rights.

For all of these reasons, and for the reasons stated in the Court's April 12, 2024 Order, the Court finds that Mr. Ziegler has standing to assert the claims he has made in this matter.

**B.**  
**Bridget Ziegler**

Mrs. Ziegler's standing analysis is different than her husbands. In large part, this analysis is secondary given the Court's resolution of Mr. Ziegler's contention. It only applies if the Second District or a reviewing court ultimately disagrees with the Court's conclusions regarding Mr. Ziegler's claims.

Plaintiffs' Amended Complaint does not allege that Mrs. Ziegler owned the records seized from Mr. Ziegler. The only interest Mrs. Ziegler asserts is her section 90.504, Florida Statutes, statutory right to prevent disclosure of privileged spousal communications. The relevant part of that statute provides:

A spouse has a privilege during and after the marital relationship to refuse to disclose, *and to prevent another from disclosing*, communications which were intended to be made in confidence between the spouses while they were husband and wife.

§90.504(1), Fla. Stat. (italicized emphasis added).

The ultimate question for the Court is this: does this statute permit Mrs. Ziegler to prevent a government entity from disclosing as a public record her spousal communications that are covered by the statute? In reviewing the meaning of a statute, “our focus is the statutory text at issue.” DeSantis v. Dream Defenders, 2024 WL 3058653, at \*3 (Fla. June 20, 2024). “To determine its best reading, we exhaust all the textual and structural clues.” Id. Justice Couriel, writing for the Florida Supreme Court, most recently warned not to ignore the whole-texts canon, “which calls on the judicial interpreter to consider the entire text, in view of its structure and of the physical and logical relation of its many parts. Id. at \*8, n.12, *quoting* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 167 (2012).

On the one hand, section 90.504 expressly provides that a spouse may “prevent another from disclosing” a spousal communication. There is no qualification on this statutory right, which suggests that a spouse like Mrs. Ziegler can do this.

On the other hand, this privilege is contained in Florida’s Evidence Code, not chapter 119. But for public records, omission from chapter 119 does not mean much, though, as the Legislature creates exemptions throughout *Florida Statutes* and not simply in chapter 119. See Government-in-the-Sunshine Manual, Florida Office of the Attorney General, Volume 46 (2024 Ed.) (reviewing pages 225-234 and 240-306 for exemptions in *Florida Statutes* not contained within chapter 119). Perhaps more concerning to Mrs. Ziegler is the absence of an express statement in section 90.504 that it is intended to exempt information from being disclosed as a public record. This type of language exists in many other statutes. The absence of this language in section 90.504 suggest that it does not allow Mrs. Ziegler to prevent a governmental agency from producing her spousal communications.

The Court must also consider the applicability of article 1, section 24(d) that provides: “All laws that are in effect on July 1, 1993 that limit public access to records shall remain in force, and such laws apply to records of the legislative and judicial branches, until they are repealed.” Without question, section 90.504 existed in its present-day form prior to that date.

Interestingly, the Florida Supreme Court adoption of Rule 1-14.1I, sheds light on this situation. On October 29, 1992—just days before the general election that included the vote on the constitutional amendment that would become article I, section 24, that court recognized there could be public record restrictions on the production of documents contained within the Evidence Code. The rule adopted provides as follows:

Except as otherwise provided in these Rules Regulating The Florida Bar, *any restrictions to production of records contained in the Florida Evidence Code*

*(chapter 90, Florida Statutes, as amended), Florida Rules of Civil Procedure, or Florida Rules of Criminal Procedure shall apply to requests for access to the records of The Florida Bar.*

In re Amendments to Florida Rules of Judicial Admin.-Pub. Access to Judicial Records, 608 So. 2d 472, 475 (Fla. 1992) (emphasis added).

This action by the Florida Supreme Court is powerful, contemporaneous evidence that chapter 90 contained restrictions on the production of records.

Because the statutory spousal privilege to “prevent another from disclosing” confidential spousal communications was adopted prior to the effective July 1, 1993 date—and it has not been repealed—the Court finds Mrs. Ziegler has standing to assert this exemption relating to privileged spousal communications.

Having determined both Mr. and Mrs. Ziegler have standing to bring this action, the Court turns its attention to the substance of the legal analysis.

#### 4.

### WARRANTS AND THE FOURTH AMENDMENT

In this section, the Court discusses the Fourth Amendment, the need for particularity in search warrants, and the reasonableness requirement.

#### A.

### Discussion of the Fourth Amendment

The Fourth Amendment demands that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Amend. IV, U.S. Const. “Article 1, section 12, of the Florida Constitution provides virtually identical protections.” State v. Peltier, 373 So. 3d 380, 384 (Fla. 2d DCA 2023).

“These words are precise and clear. They reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever be secure in their persons, houses, papers, and effects from intrusion and seizure by officers acting under the unbridled authority of a general warrant.” Stanford v. State of Texas, 379 U.S. 476, 481 (1965) (holding the sweeping language of the warrant “constitutionally intolerable” that permitted the seizure of 2,000 books, pamphlets, and papers where warrant attempted to allow seizure of written instruments concerning the Communist Party of Texas).

In reversing a criminal defendant’s conviction based on evidence obtained from a general warrant, the Second District quoted United States Supreme Court decisions from 1886 and 1927 discussing the historical importance of the Fourth Amendment:

In Marron [v. United States, 275 U.S. 192, 195 (1927)], the United States Supreme Court explained why the prohibition against general searches was so important as to be placed in the Constitution:

The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis announced “the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book;” since they placed “the liberty of every man in the hands of every petty officer.”

Id. (*quoting Boyd v. United States*, 116 U.S. 616 (1886)).

Ingraham v. State, 811 So. 2d 770, 773 (Fla. 2d DCA 2002) (only first bracketed alteration added).

“The text of the Amendment thus expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless probable cause is properly established, and the scope of the authorized search is set out with particularity.” Kentucky v. King, 563 U.S. 452, 459, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011) (internal citation omitted). The particularity requirement “ensures that the search is confined in scope to particularly described evidence relating to a specific crime for which there is probable cause.” United States v. Oloyede, 982 F.2d 133, 138 (4th Cir. 1993).

“[T]he particularity requirement stands as a bar to exploratory searches by officers armed with a general warrant.” Carlton v. State, 449 So. 2d 250, 252 (Fla. 1984) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”) (*quoting Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 76, 72 L.Ed. 231 (1927)). This requirement also safeguards the “privacy and security of individuals against arbitrary invasions by governmental officials.” Id. (citations omitted).

A warrant must sufficiently describe what is to be searched and seized; using generic terms such as “documents” is insufficient. The Fifth District has explained:

Warrants attempting to authorize a search for, and seizure of, a class or group of objects, such as “documents” are too general and do not describe the thing or things to be seized with the particularity that the constitution requires. *If the original source of information upon which the search warrant affidavit relies cannot describe existing objects or things other than in terms of generic reference such as “papers”, “documents”, the information is too vague and indefinite upon which to authorize a search.* General searches are not permitted.



Polakoff v. State, 586 So. 2d 385, 392 (Fla. 5th DCA).

In addressing the issue of particularity as applied to a subpoena duces tecum for documents, the Florida Supreme Court noted that “reasonable particularity” may be satisfied by the description of a category of documents being sought “along with a reasonable period of time covered by the documents and a statement of the subject matter to which the documents pertain.” Vann v. State, 85 So. 2d 133, 136 (Fla. 1956); see also State v. Showcase Products, Inc., 501 So. 2d 11, 14 (Fla. 4th DCA 1986) (“It is universally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit.”). In each case, however, the category of documents being sought must be particularly described, and their seizure must be supported by a nexus to the crime being investigated.

## **B.**

### **Particularity as Applied to Electronically Stored Information (“ESI”)**

“The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]” Riley v. California, 573 U.S. 373, 394 (2014). Ten years ago, the United States Supreme Court held that law enforcement must obtain a warrant to search the cellphone of an arrested individual. Id. In explaining the need for law enforcement to obtain a warrant to search and seize the contents of a cellphone, the United States Supreme Court observed:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life.” The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Id. at 403 (internal citation omitted).

That was 10 years ago. The use and storage capabilities of cellphones and social media accounts have grown exponentially since then. To say that cellphones and social media accounts are omnipresent today would be the understatement of the century. For many of us, a cellphone contains our life story.

On the stand, SPD detectives testified that it was “best practice” to make an identical copy of the complete contents of the cellphone and then search across the entire contents to ensure deleted or altered material would be discovered. In a civil case, the Third District recently rejected that very concept, noting the historical importance of the Fourth Amendment. Roque v. Swezy, 49 Fla. L. Weekly D921, 2024 WL 1895141, \*3 (Fla. 3d DCA May 1, 2024) (rejecting view that a forensic search and seizure of a cellphone should occur because it is “quicker and

more efficient means of obtaining evidence”). As that court explained: “Such a contention is reminiscent of arguments advanced to justify warrantless searches otherwise prohibited under the Fourth Amendment.” *Id.* This principle is of a constitutional dimension, recognized by the United States Supreme Court:

[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment. The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment reflects the view of those who wrote the Bill of Rights that the privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law.

Mincey v. Arizona, 437 U.S. 385, 393 (1978) (internal citation omitted).

That takes us to the rules associated with searching for ESI. If law enforcement is not permitted to obtain a general warrant to rummage through a home, would law enforcement be able to execute a general warrant to search and seize all of an individual’s ESI? And the answer is, law enforcement cannot.

In analyzing the sufficiency of the warrants authorizing the seizure of ESI, the particularity requirement assumes even greater importance. United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013). That is because the seizure and subsequent retention of ESI “can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.” United States v. Ganius, 824 F.3d 199, 217 (2d Cir. 2016) (*en banc*). “The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous”—a “threat [that] is compounded by the nature of digital storage.” Galpin, 720 F.3d at 447.

The Court, of course, recognizes that in the search for specifically identified incriminating digital data, “it is almost inevitable that officers will have to review some data that is unrelated to the criminal activity alleged in the authorizing warrant.” People v. Hughes, 506 Mich. 512, 547 (2020). “[O]n occasion in the course of a reasonable search [of digital data], investigating officers may examine, ‘at least cursorily,’ some ‘innocuous documents ... in order to determine whether they are, in fact, among those papers authorized to be seized.’” United States v. Richards, 659 F.3d 527, 539 (6th Cir. 2011). However,

[a]lthough computer technology may in theory justify blanket seizures ..., the government must still demonstrate to the magistrate [judge] factually why such a broad search and seizure authority is reasonable in the case at hand.... Thus, there must be some threshold showing before the government may ‘seize the haystack to look for the needle.’

United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006) (emphasis added).

Unfortunately, Florida law provides little guidance on how to apply the particularity requirement to searches of ESI. In the Fifth Amendment context concerning compelled production by a defendant of a cellphone passcode, the First District had occasion to comment on the scope and breadth of a search warrant for the defendant's cell phone. Pollard v. State, 287 So. 3d 649, 657 (Fla. 1st DCA 2019). In agreeing with the Fourth District's observation in G.A.Q.L. v. State, 257 So. 3d 1058, 287 So. 3d 249 (Fla. 4th DCA 2018), the Pollard court stated "unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images amounts to a mere fishing expedition." 287 So. 3d at 657 (internal citation, quotation, and alteration omitted); see G.A.Q.L. v. State, 257 So. 3d at 1064 ("It is not enough for the state to infer that evidence exists—it must identify what evidence lies beyond the passcode wall with reasonable particularity.").

Two years ago, a federal judge in Georgia found that a warrant that allowed the government unbridled authority to rummage through a defendant's Instagram account looking for evidence of possession of firearm by a felon to be unnecessarily overbroad and amounted to a general warrant in violation of the Fourth Amendment's particularity clause. United States v. Mercery, 591 F. Supp. 3d 1369, 1381 (M.D. Ga. 2022). The court explained:

The Instagram Warrant authorizes the government to search and seize data that is not related to the probable cause established in Sergeant Frost's affidavit. It allows officers to search and seize virtually all of the information on Mercery's Instagram account, with no temporal limitations or limitations defined by the crime of possession of a firearm by a convicted felon. Such warrant is akin to a general warrant and therefore violates the Fourth Amendment's particularity clause.

Id. at 1382.

The Mercery court noted that, under the federal rules relating to ESI, normally there is a two-step investigatory process, "the 'search' wherein the warrant will compel the third party to produce a broad array of electronic information, and the 'seizure' wherein the warrant will authorize the seizure of a specified information." Id. The Court then found that the Instagram warrant in question described the broad production of data to be produced but failed to describe any subset of information subject to seizure. Id. In excluding the evidence, the court spoke directly to law enforcement and the types of limitations that must be followed relating to ESI:

Finally, and most important, excluding the evidence obtained under the unconstitutional warrant will deter future violations. Social media networks like Instagram and Facebook are an ever-increasing form of communication and hubs of personal information for which law enforcement routinely seek and obtain search warrants. ***Officers need to know that a warrant must provide guidelines for determining what evidence may be searched and seized and must be tailored to the probable cause established in the supporting affidavit.*** Thus, the Court finds the good faith exception inapplicable under the circumstances here,

and Defendant's Motion to Suppress evidence seized pursuant to the Instagram Warrant is GRANTED.

Id. at 1383 (emphasis added).

The Court also finds other state and federal courts' analyses of these principles as applied to ESI searches to be instructive. These courts have consistently held that when a search warrant uses "catchall" language which permits law enforcement to search all data on a cell phone or other data storage accounts, this amounts to an invalid "general warrant."

- State v. Henderson, 289 Neb. 271, 854 N.W.2d 616, 625, 633 (Neb. 2014) (warrants to search cell phones violated particularity requirement where they authorized a search of "[a]ny and all information," as well as "any other information that can be gained from the internal components and/or memory Cards").
- State v. Allen, 288 Or. App. 244, 406 P.3d 89, 93 (Or. Ct. App. 2017) (holding that search warrant for cell phone failed the particularity requirement because it "placed no limitations on the types of files to be seized and examined").
- United States v. Otero, 563 F.3d 1127, 1133 (10th Cir. 2009) (government conceded and reviewing court agreed that warrant "authorizing a search of 'any and all information and/or data' stored on computer" was "the sort of wide-ranging search that fails to satisfy the particularity requirement").
- United States v. Clough, 246 F. Supp. 2d 84, 87 (D. Me. 2013) (warrant that authorized seizure of any and all text messages and digital images on computer was "clearly excessive" and was not sufficiently particularized).
- United States v. Fleet Mgmt. Ltd., 521 F. Supp. 2d 436, 439 (E.D. Pa. 2007) (warrant to search hard drives of three computers lacked particularity because it sought "[a]ny and all data in the computers or contained in the computer storage devices, including, but not limited to, software and all records including e-mail, photographs, and documents relating to the ship's operation, engineering, maintenance, pollution control equipment, navigational charts, and crew").
- United States v. Winn, 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) ("The major, overriding problem with the description of the object of the search – 'any or all files' – is that the police did not have probable cause to believe that everything on the phone was evidence of the crime of public indecency.")

Where there is a limitation built into the warrant, there is greater chance that it will be constitutional. United States v. Lee, Crim. No. 14-227-TCB-2, 2015 WL 5667102, at \*3 (N.D. Ga. Sept. 25, 2015) ("[T]he weight of the authority supports the conclusion that a warrant that requires disclosure of the entire contents of an [electronic source] and then describes a subset of that information that will be subject to seizure is reasonable.").

The language of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701, et seq., and the corresponding Florida law contained in section 934.23(5), Florida Statutes, is also instructive, especially as applied to the Google and Meta warrants. Both statutes govern the warrant requirements for disclosure of ESI held by a third-party provider and use identical language requiring that the government’s application for a search warrant provide:

specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

The Court finds that as applied to ESI, the warrant and supporting documents being reviewed must describe with particularity a specific record being sought or describe a specifically identified *type* of record (i.e. text, email, photo, etc.), which also contains case-specific facts demonstrating how this particular record is relevant and material to the ongoing investigation.

**C.**  
**Reasonableness of Search Methods**

Even prior to the advent of the everyday use of ESI in the lives of virtually every citizen, the U.S. Supreme Court recognized,

[T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the “seizure” of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

As with searches for tangible evidence, determining whether an ESI search exceeded the scope of the authorizing warrant is an exercise in reasonableness assessed on a case-by-case basis. Dalia v. United States, 441 U.S. 238, 258 (1979) (holding that the manner of a search is subject to “later judicial review as to its reasonableness”). The general Fourth Amendment rule is that investigators executing a warrant can look anywhere where evidence described in the warrant might conceivably be located. United States v. Ross, 456 U.S. 798 (1982).

This principle is equally applicable to warrants served upon ESI. In re Nextel Cellular Telephone, No 14-MJ-8005, 2014 WL 2898262, at 13 (D. Kan. June 26, 2014) (noting just as probable cause to believe “that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe drug trafficking communication may be found in [a] phone's . . . mail application will not support the search of the phone's Angry Birds application”). As previously noted, however, even when an electronic records warrant is narrowly tailored to search for specific items, the enormous amount of data and infinite places ESI evidence may be located inevitably results in the “seizure of the haystack looking for the needle.” Hill, 459 F.3d at 975. Thus, it becomes critical for courts to also examine the reasonableness of the search method the government employed.

In In re Cellular Telephones, No. 14-MJ-8017-DJW, 2014 WL 7793690 (D. Kan. Dec. 30, 2014), a magistrate judge noted that in ESI searches, the “reasonableness of the manner of search is necessarily implicated because particularity and reasonableness are functionally related.” Therefore, “[a]s the description of such places and things becomes more general, the method by which the search is executed becomes more important—the search method must be tailored to meet allowed ends.” Id. (quoting United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009)). For this reason, the magistrate required that the government must not only “provide the court with as specific a description of the place to be searched and the things to be seized as the circumstances reasonably allow,” but they must also outline “a search protocol explaining how it will separate what is permitted to be seized from what is not.” Id. at \*8. These limitations must “maintain the privacy of materials that are intermingled with seizable materials” and are necessary to “avoid turning a limited search for particular information into a general search of office file systems and computer databases.” Id. at \*9.

This is akin to what Mercery, 591 F. Supp. 3d 1369, 1381 (M.D. Ga. 2022), explained as the two-step process between a wide search but more narrow seizure. Other courts across the country have recognized the need for protocols to protect the cellphone owner’s constitutional rights, as well as a subsequent warrant to seek evidence of a separate crime than identified in the original warrant.

- Matter of the Search of Apple iPhone IMEI 01388803738427, 31 F. Supp. 3d 159, 166 (D.D.C. 2014) (“a sufficient search protocol, i.e. an explanation of the scientific methodology the government will use to separate what is permitted to be seized from what is not, will explain to the Court how the government will decide where it is going to search—and it is thus squarely aimed at satisfying the particularity requirement of the Fourth Amendment.”)
- United States v. Nasher-Alneam, 399 F. Supp. 3d 579, 593-94 (S.D. W. Va. 2019) (“Even when a seizure of electronic data is legal, any search of that data must be within the scope of the original warrant.” Thus, if the government subsequently develops probable cause to believe the seized ESI contains evidence of a crime different from the subject of the original warrant, they are required to get a second warrant prior to the subsequent search.).

- United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (suppressing child pornography evidence where police, conducting search under warrant for drug offenses, continued to search for child pornography without obtaining warrant).
- United States v. Hulscher, 2017 WL 657436, \*2 (D. S.D. Feb. 17, 2017) (suppressing evidence from second search of iPhone for evidence to support federal firearms charges where search warrant allowing seizure and search of phone was to investigate forgery, counterfeiting, and identify theft offenses because agent “should have applied for and obtained a second warrant [that] would have authorized him to search Mr. Hulscher's cell phone data for evidence of firearms offenses”).
- United States v. Schlingloff, 901 F. Supp. 2d 1101, 1106 (C.D. Ill. 2012) (concluding scope of search warrant was exceeded and suppressing evidence of child pornography where law enforcement agent was searching computer for evidence of passport fraud and identify theft but, upon discovering evidence of child pornography, failed to seek a second warrant).
- United States v. Cawthorn, 682 F. Supp. 3d 449, 457 (D. Md. 2023) (noting that in exercising an ESI warrant “the government ‘may not seize and retain items outside the scope of a warrant’”).

The lesson from these cases demonstrates that, to the extent the warrants appropriately described with particularity the items being sought, the Court must also review the search methods employed by SPD to determine whether they reasonably restricted the search to exclude private, irrelevant information. It is within this framework that the Court now examines the three warrants at issue in this case.

## 5. THE CELL PHONE SEARCH WARRANT (NOVEMBER 1, 2023)

On November 1, 2023, SPD obtained a search warrant to seize and search Mr. Ziegler’s iPhone. The affidavit in support of this warrant, signed by Detective Cox, stated facts in support of this warrant as outlined in paragraphs 2-6 of Section 2, “Findings of Fact.”

As it pertains to evidence contained on Mr. Ziegler’s cellphone, the warrant alleged the following:

Based upon the above information, Affiant has reason to believe that evidence of a crime will be found within the cellular phone device belonging to Christian Ziegler telephone number XXX-XXX-XXXX.

See Ex. 1, at ¶ 10.

Additionally, the attesting detective alleged that in her experience it is common for a suspect to use the phone's text messages, calls, emails, applications, and internet access to assist in the commission of a crime. Id. at ¶¶ 11, 12, and 13. She also alleged that the devices store cell tower data and GPS coordinates. Id. at ¶¶ 14, 15. All of this data "may contain evidence or fruits of the crime." Id. at ¶18. Finally,

Based on the aforementioned facts, your Affiant believes that probable cause exists to show Christian Ziegler's cellular phone, an AT&T carrier # XXX-XXX-XXXX which is currently in Christian Ziegler's custody, contains valuable evidence relevant to the matter of this warrant.

The warrant then authorized the seizure of Mr. Ziegler's cell phone for the following "evidence":

1. All data regarding target device identity information including the assigned phone number, serial number, make, model, IMEI, carrier, and owner information.
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 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.



Id. at p. 2 (footnote omitted).

Upon serving the warrant, Detective Cox testified that over five days SPD imaged the phone's entire contents onto their computer. She and other detectives then utilized the Cellebrite program to identify potentially relevant information from the phone. This process was not spelled out in the warrant or otherwise controlled by the terms of the warrant.

In other words, SPD had unfettered access to, and unbridled discretion in, seizing anything SPD wanted from Mr. Ziegler's cellphone. During this process, Detective Cox marked numerous items using the F7 functionality to "seize" the records as evidence. Some of the F7 records include the items listed in paragraph 15 of Intervenor's Exhibit Q.

Recall the warrant sought evidence for an alleged crime of sexual battery occurring on October 2, 2023. And the affidavit identified that a digital extraction of Ms. Doe's cellphone revealed several messages from Mr. Ziegler to her "on 10/02/23 starting at 0729 hours." Given SPD's knowledge of the date of the alleged crime and when messages began there was absolutely no explanation why a time restriction or content restriction could not be used to guard against law enforcement's unfettered seizure of Mr. Ziegler's personal, private property.

During their subsequent review of 30,000+ videos and 250,000+ electronic photographs, SPD detectives seized an indeterminate number of these files, again using the F7 functionality. These were of a private nature. Incredibly, Detective Cox testified that ***none of them involved Ms. Doe, and none of them depicted any illegal activity, but they were seized anyway.***

Despite this, SPD detectives uploaded this media into Evidence.com to provide the State Attorney's Office with access to determine whether it *might* provide useful information of similar crimes pursuant to the rule established in Williams v. State, 110 So. 2d 654, 658 (Fla. 1959) (holding that evidence of other crimes is admissible and relevant if it tends to show a common scheme or plan). ***Again, even by the lead detective's own admission, none of the videos or images depicted any illegal activity.***

This practice of using the F7 key to seize videos and photographs with no apparent criminal activity displayed on the off chance that prosecutors in the future may use this as Williams' rule evidence is constitutionally intolerable. Certainly, these non-criminal items were not identified as evidence of the sexual battery allegation being investigated. And they were not identified in the warrant.

Presumably, had there been a criminal prosecution, the State's position would have been these videos and photos were in plain view of the SPD detectives during the search of the cellphone for evidence of a sexual battery occurring on October 2, 2023. Yet, the "plain view" doctrine allowing warrantless seizures only applies "where it is immediately apparent to the police" the item to be seized is of a criminal character; the doctrine "may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971). More, law enforcement must have probable cause to seize an item in plain view where there is no warrant. Arizona v. Hicks,

480 U.S. 321, 327 (1987); Young v. State, 207 So. 3d 267, 269 (Fla. 2d DCA 2016) (holding that the incriminating nature of the evidence must immediately be apparent to seize items in plain view when performing a warranted search); see also Doane v. United States, 2009 WL 1619642 (S.D.N.Y. June 5, 2009) (“The fact that the prosecution ultimately recognizes the evidentiary value of the document is immaterial. The plain view doctrine requires that the objects evidentiary value be apparent at the time of the seizure.”).

There is no scenario where the federal or state constitution would permit law enforcement outside of a warrant to knowingly seize property that, by law enforcement’s own admission, is not contraband or criminally suspect on the off chance that some future prosecutor may divine a way to transform it into evidence of a crime.

Based upon these facts, the Court finds that the phone warrant’s seizure of essentially the entire contents of Mr. Ziegler’s cellphone as “evidence” wholly fails to sufficiently identify *specific* records which were reasonably related to the investigation. In other words, while the warrant accurately described the places which may be searched for evidence (i.e., the messages, photos, web-browsing history etc.) it failed to identify with *any reasonable specificity* the evidence which might be discovered at these locations. Even when construing the warrant application in its entirety, *at best*, it only particularly describes potentially relevant communication between Mr. Ziegler and Ms. Doe to be found on the cellphone. The search for this limited information did not permit SPD the legal authority to search the entirety of the phone’s contents including images, videos, web browsing history, financial data, or passwords.

The request and warrant were absolutely overbroad and violated the particularity clause of the Fourth Amendment.

The Court further finds that, despite using Cellebrite to search the phone’s contents, SPD failed to conduct the search in a manner designed to minimize unwarranted intrusion upon irrelevant private communications or other ESI. There was no established protocol governing how SPD would conduct its review of the contents to focus on seizing particularly identified items.

This unrestrained search led to the seizure of, among other things, more than **1,200 spousal communications** between the Zieglers **predating by more than two years** the alleged October 2, 2023, crime. And, making the seizure worse, only a handful of these communications even referenced Ms. Doe. (The Court knows this based on the *in camera* inspection of the marital communications referenced in paragraph 15 of Exhibit Q.) This seizure was entirely unreasonable and unconstitutional.

The Court is aware that search warrants have been upheld, in part, under the concept of severability. West v. State, 439 So. 2d 907, 914 (Fla. 2d DCA 1983), *decision quashed on other grounds*, 449 So. 2d 1286 (Fla. 1984); see also State v. Nuckolls, 617 So. 2d 724, 728 (Fla. 5th DCA 1993) (finding portions of the seized evidence was admissible because they were described with particularity).

But, where, as here, the violations are so fundamental and substantial, severance does not apply. Otherwise, law enforcement’s unconstitutional practices could continue with no meaningful sanction. To be clear, the Court holds that the concept of severance does not apply to this unconstitutional warrant.

But if Second District or any reviewing court were to conclude the doctrine of severability applies to the facts of this case, the Court finds that no valid portion of the cellphone warrant was exercised as to the following items seized: the photos and videos marked by SPD detectives using the F7 key and uploaded into Evidence.com; the communications between Mr. and Mrs. Ziegler (Paragraph 15a-15d of Exhibit Q); the Cellebrite extraction report (Paragraph 15h of Exhibit Q); the “List” (Paragraph 15i of Exhibit Q); and web browsing history (Paragraph 15j of Exhibit Q). Thus—and even if severance were to apply here—these items were seized in violation of Mr. Ziegler’s rights secured by the Fourth Amendment to the United States Constitution and article I, sections 12 and 23 of Florida’s Constitution.

Although unnecessary for a finding of unconstitutionality, the Court also comments on yet another concerning factor of SPD’s investigation. Despite knowledge, SPD in obtaining the cellphone warrant failed to include any information in the affidavit about the existence of the potentially exculpatory video or Mr. Ziegler’s offer to show the Video to law enforcement. Law enforcement simply cannot withhold relevant, potentially exculpatory information from the judge reviewing a warrant. Because of the Court’s prior conclusion of unconstitutionality, the Court need not further analyze this issue or perform a hearing contemplated by Franks v. Delaware, 438 U.S. 154 (1978).

But the Court remains troubled by this glaring omission.

**6.**  
**THE GOOGLE WARRANT**  
**(NOVEMBER 15, 2023)**

SPD obtained the Google warrant pursuant to 18 U.S.C. §§ 2701, et seq., and section 934.23(5), Florida Statutes. See Ex. 2, p. 1. The supporting documents for the warrant contained the same factual allegations to the November 1st cellphone warrant with one substantive addition:

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 10/2/23 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.

Id. at ¶ 9.

Disconcertingly, this statement of fact failed to alert the reviewing judge that during the November 2nd interview, SPD officers watched the Video and that the sexual encounter

appeared consensual. The affidavit also failed to alert the reviewing judge of Detective Riffe's observation after watching the Video that the victim appeared to be "coherent." See Ex. F, Transcript of 11/2/23 interview of Christian Ziegler at p. 19 ("Just on the video and I don't know if [Mr. Byrd] heard it was well, I mean you could hear she's coherent, but she's slurring a little bit.").

After outlining these facts, Detective Cox's affidavit affirmed:

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: [redacted@gmail.com](mailto:redacted@gmail.com) will lead to locating evidence of the crime, and will authenticate the date, time and location of when the video was created.

See Ex. 2 at ¶ 10. The warrant then stated that based upon Detective Cox's training and experience,

searches and seizures of electronic communications evidence may require the seizure of most, or all communication currently stored to be processed later. Furthermore, your 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 [sic] after you [sic] Affiant has an opportunity to search all the data being stored within the aforementioned Google Drive account.

Id. at ¶ 15. The Google warrant then authorized them to "seize as evidence any of the following:"

1. Stored electronic communications or files associated with the user accounts identified as Google User ID: Email: [redacted@gmail.com](mailto:redacted@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 identifies, and/or any other files related to that account;
2. Records concerning the identity of the user of the above-listed user accounts(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 access;

3. Any photoprints linked to or associated with the above-listed user account(s). The photoprints 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 video/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 transaction logs that show user interaction with the video/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.

Id. at pp. 2-3.

Notably, Detective Cox testified that no relevant evidence was seized during the search of the ESI produced pursuant to the Google warrant.

The Court finds that the Google warrant was overly broad in that it authorized the seizure of Mr. Ziegler’s **entire Google account** as “evidence” despite investigating a crime allegedly occurring on October 2, 2023. Again, the warrant described the locations to be searched (i.e. web bookmarks, autofill data, wallet information, buddy lists, etc.) but it failed to identify the particular evidence being sought in those locations.

Further exacerbating this “over-seizing” mentality, there is no technological reason to obtain the entire contents of a Google or social media accounts because Google and other social media companies have the ability to produce only what is requested. This stands in stark contrast to the affidavit that affirmed there can be no narrowing or minimization until after searching the entire contents of the Google Drive.

Two cases—each more than six years old—demonstrate this point. These cases are examples like others across the country warning of the constitutional problems associated with seizing everything even though there is a technological means to seize a limited subset of data from Google. This ability to narrowly search an account is not a “new” technological invention, and the age of these cases fully support a generalized view that law enforcement (and courts) nationwide should understand this functionality.

In 2018, a federal judge quashed similar expansive search warrants seeking searches of the entirety of Google accounts:

***That “accepted reality” [of needing to seize everything] has evolved. The Target asserts, and the government does not dispute, that Google is now willing and able to date-restrict the email content it discloses to the government. [ . . . S]ee also In re [Redacted]@gmail.com, 62 F. Supp.3d 1100, 1103 n.4 (N.D. Cal. 2014). In other words, Google is capable of producing to the government a much smaller haystack to search: only emails restricted to the probable cause time period of October 1, 2016, to April 14, 2017, rather than every email dating back to the creation of the email accounts. It is no longer a necessary evil to order Google to disclose to the government emails the government does not have probable cause to search. . . .***

***The Court finds that the search warrants challenged here, which require Google to disclose to the government the “contents of all emails associated with the Email Account[s,]” are overbroad because it is unreasonable to compel a provider to disclose every email in its client's account when the provider is able to disclose only those emails the government has probable cause to search. See In the Matter of the Search of Google Email Accts., 92 F. Supp. 3d 944, 946 (D. Alaska 2015) (denying two-step Google search warrant application as overbroad where although “the government promises to limit its search to the relevant date ranges, nothing in the proposed warrant precludes its agents from perusing other email content regardless how remote or how unrelated that content***

may be to the current investigation”); In re [Redacted]@gmail.com, 62 F. Supp. 3d at 1104 (denying two-step Google search warrant application and stating that “[t]he court is nevertheless unpersuaded that the particular seize first, search second [warrant] proposed here is reasonable in the Fourth Amendment sense of the word”); U.S. v. Matter of Search of Info. Assoc. with Fifteen Email Addresses, 2017 WL 4322826, at \*7, 10 (M.D. Ala. Sept. 28, 2017) (holding that “the Government's current request for all data related to all the [Google and other] email accounts is too broad” and ordering the government to include “a date restriction on the data to be turned over by the provider based on an individualized assessment of the accompanying probable cause evidence for each email account”).

Matter of Search of Info. Associated With Four Redacted Gmail Accounts, 371 F. Supp. 3d 843, 845–46 (D. Or. 2018) (bolded, italicized emphasis added; first and second bracket set added; all other brackets in original; omitting internal citations, YouTube links, and parentheticals).

Similarly, in 2017, the Eleventh Circuit Court of Appeals explained that warrants directed to social media companies seeking “virtually every kind of data that could be found in a social media account” were overbroad. United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017). “And unnecessarily so.” Id.

Hard drive searches require time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant's home would be impractical, if not impossible. By contrast, when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data. That procedure does not appear to be impractical for Facebook or for the government. Facebook produced data in response to over 9500 search warrants in the six-month period between July and December 2015.

Id. (internal citations and website omitted). The Court recognizes that the Eleventh Circuit did not determine if there was a Fourth Amendment violation in that case due to the application of the good-faith exception. But the overbroad analysis still applies here.

Even when construing the Google warrant application in this case in its entirety, the affidavit could only be construed to describe with particularity the Video and notes SPD was specifically seeking this Video “to authenticate the date, time, and location of when the video was created.” See Ex. 2 at ¶ 10. However, the warrant application failed to explain how this Video could be related to Mr. Ziegler’s wallet, web history, contacts, credit card numbers, PINs or any of the non-relevant information sought and seized. The Court finds that the warrant authorizing the broad seizure of ESI contained in Mr. Ziegler’s Google Drive account was facially invalid and done in violation of his constitutional rights.

7.

## THE META/INSTAGRAM WARRANT

(DECEMBER 8, 2023)

As with the previous warrant, SPD obtained the Meta/Instagram warrant pursuant to 18 U.S.C. §§ 2701, et seq., and section 934.23(5), Florida Statutes. See Ex. 3 at p. 1. The affidavit in support of this warrant indicated SPD was investigating a charge of video voyeurism against Mr. Ziegler in violation of section 810.145(6)(b), Florida Statutes. The affidavit contained substantially the same facts as the phone and Google warrants. The Meta/Instagram warrant did reference the November 2nd meeting at Attorney Byrd's office:

On 11/02/23, Detectives interviewed Christian Ziegler and his attorney Derek Byrd's office. Ziegler stated he took a video of the sexual encounter with the victim on 10/02/23, the date of the alleged sexual battery. Ziegler stated the sexual encounter was consensual. Ziegler showed detectives the 2.5-minute-long video of the sexual encounter. He stated that the sexual encounter was consensual. Byrd made mention of a message (on Instagram vanish mode) between the victim and Ziegler where the victim asked him if he showed his wife the video.

See Ex. 3 at ¶ 13. The affidavit then indicated that SPD had spoken to both Ms. Doe and Mrs. Ziegler and "the victim did not give Ziegler consent to take this video of them having sex." Id. at ¶ 14. It further stated that neither Mrs. Ziegler nor Ms. Doe had seen nor knew anything about the Video. Id.

The affiant then affirmed that she had reason to believe that evidence of the crime would be found within Mr. Ziegler's Instagram account and that Mr. Ziegler utilized the program to commit the crime of video voyeurism. Id. at ¶ 15. The affiant further asserted that "valuable evidence will be located within the suspect's account which will provide additional information about his criminal activity." Id. at ¶ 18.

Similar to the previous Google warrants, this warrant required Meta to "seize as evidence any of the following:"

1. Any and all stored electronic communications or files associated with the user accounts identified as User Accounts Identified by User ID(s): [sic]

[https://www.instagram.com/\[redacted\]/](https://www.instagram.com/[redacted]/)

Username: [redacted]

and any related accounts concerning the same account subscribers or users, since the creation of such account until the present time of this affidavit, including the content and header information of email messages and any attachments, user contact information, group contact information, IP logs, and instant messages (Instagram Messenger) to include vanish mode messages, whether drafted, sent, received, opened or unopened, read or unread, and/or forwarded, and any buddy lists or contact lists,



calendars, transactional data, account passwords or identifiers, and/or any other files related to those accounts.

2. Any Neoprints linked to or associated with the above Instagram user account. A Neoprint is an expanded view of a given user profile. It contains their current profile information, and all wall postings and messages to and from the user that have not been deleted by the user.
3. Any Photoprints or videos linked to or associated with the above Instagram user account. A Photoprint is a compilation of all photos uploaded by the user that have not been deleted along with all photos uploaded by any user that has the user tagged in them.
4. Records concerning 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.
5. Journal entries, Neoprints, comments and the contents of private messages in the above-listed user's inbox, sent mail, and trash folders related to the above-listed user account(s)
6. Any images, videos, or chats within the vanish mode setting of the above account.

Ex. 3, pp. 2-3, ¶¶ 1-6.

Again, Detective Cox testified at trial that, in her opinion, the Meta/Instagram warrant failed to produce any evidence relevant to SPD's investigation.

The Court finds that the Meta/Instagram warrant's "seizure" of Mr. Ziegler's entire account history since its inception to be used as "evidence" again fails to provide either the necessary particularity or establish a nexus between the entire contents of this account to the crime being investigated. The only specific mention of Instagram linking this service to the crime is the affidavit's mention that Mr. Ziegler used it to communicate with Ms. Doe on and after October 2, 2023 (¶¶ 8, 10) and Mr. Byrd's comment that there was a vanishing message from Ms. Doe asking Mr. Ziegler if he showed the video to his wife. (¶ 13).

Even when construing the warrant application as a whole, the Court finds these references fail to provide the warrant with sufficient particularity to seize the entire contents of his account from its inception. Thus, even though no relevant evidence was located upon SPD's review of the seized information, the ESI seized by SPD was pursuant to a constitutionally invalid warrant and in violation of Mr. Ziegler's constitutionally protected rights.

## **8. REMEDIES**

Having concluded multiple and fundamental violations of Mr. Ziegler’s Fourth Amendment right, the Court must address what can be done about it in the present context.

**A.**

**The Constitutional Right of Return of a Person’s Property**

Implicit in the Fourth Amendment is the remedial obligation of courts to order the prompt return of illegally seized, non-contraband property. Weeks v. United States, 232 U.S. 383, 393 (1914), *overruled on other grounds by* Elkins v. United States, 364 U.S. 206 (1960); *see also* City of W. Covina v. Perkins, 525 U.S. 234, 240 (1999) (noting that when law enforcement seizes property pursuant to a warrant, the Fourteenth Amendment’s due process clause applies to the return of the property to its rightful owner); Bolden v. State, 875 So. 2d 780, 782 (Fla. 2d DCA 2004) (“that the party from whom materials are seized in the course of a criminal investigation retains a protectible property interest in seized materials”).

This is particularly important when the government determines that the investigation will not result in criminal charges which provide the individual a traditional criminal forum to challenge the seizure. Black Hills Inst. of Geological Research v. U.S. Dept. of Justice, 967 F.2d 1237, 1240 (8th Cir. 1992) (“Until criminal charges are brought, the property owner is to be considered an innocent bystander.”).

The government may not retain access to seized property which has been determined to be outside the scope of the warrant. *See* United States v. Matias, 836 F.2d 744, 747 (2d Cir. 1988) (“when items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items”); Doane v. United States, 2009 WL 1619642, at \*10–11 (S.D.N.Y. June 5, 2009) (ordering the return of “the originals and all copies” of seized item).

Intervenor Defendants during oral argument suggested that even if there were a “return” of Mr. Ziegler’s data, the government could keep a copy of it. The analogy used was if a stapler were seized, law enforcement could photograph and keep a picture of the stapler while returning the actual stapler. That contention, though, violates Mr. Ziegler’s property rights because it destroys his ability to control that property and exclude others from it.

Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. ***One of the main rights attaching to property is the right to exclude others . . .*** and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.

Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (emphasis added; internal citation omitted).

For these reasons, the Court finds that Defendants’ continued retention of the unlawfully seized ESI raises constitutional issues *distinct* from the lawfulness of the underlying warrants and their execution—not the least of which is Mr. Ziegler’s right to regain exclusive control over

his private information and to be free from a *de facto* forfeiture without due process or compensation. E.g., United States v. Premises Known as 608 Taylor Ave., Apartment 302, Pittsburgh, Pa., 584 F.2d 1297, 1302 (3d Cir. 1978) (noting that the government’s failure to return property seized pursuant to a search warrant in a timely manner may result in a *de facto* forfeiture); Lowther v. United States, 480 F.2d 1031 (10th Cir. 1973) (holding that the continued retention of evidence would constitute a taking without just compensation).

Absent Florida’s Public Record Law, there would be no credible argument to the main relief Mr. Ziegler seeks—the return of his property accomplished through the destruction of the electronic copies in the government’s possession.

## B.

### **Florida’s Public Record Law**

Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution.

Art. I, §24(a), Fla. Const.

Even before this constitutional provision was added to Florida’s Constitution in 1992, Florida maintained a robust statutory public records law. See ch. 119, Fla. Stat. That the people of Florida also added this right to our state’s constitution underscores the importance of access to public records.

And the Court acknowledges the constitutional importance of public records in Florida.

“‘Public records’ means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, *made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.*” §119.011(12), Fla. Stat. (emphasis added).

It is well established that the public records laws be liberally construed in favor of the state’s policy of open government. E.g., Board of Trustees v. Lee, 189 So. 3d 120, 125 (Fla. 2016).

## C.

### **The intersection of the Fourth Amendment and the Public Record Act**

Before proceeding further, the Court makes two observations derived from case law about Florida's public record law. *First*, physical presence on a governmental computer system does not automatically transform an individual's personal emails into a public record. State v. City of Clearwater, 863 So. 2d 149, 155 (Fla. 2003) (holding City of Clearwater employee's personal email on governmental server not public record). *Second*, an individual's private documents in the hands of a governmental entity received in the ordinary course of business are not automatically a public record. Kight v. Dugger, 574 So. 2d 1066, 1068 (Fla. 1990) (holding criminal defendant's file in the hands of the Office of Capital Collateral Representative are not governmental records subject to disclosure pursuant to chapter 119).

From these cases, the Court can conclude that a person's private property is not automatically transformed into a public record simply by being seized by the government and held in its file. That is not to say the seized items may not be public record—they may—but the simple fact of being seized and held by the government is not enough to qualify as a public record.

Otherwise, the return of every search warrant issued by a state court and returnable before a state judge in Florida would constitute a public record. And there would be nothing that the owner of the seized property could do to shield the contents of their property from public view. The ramifications of that holding would be sweeping—and outright scary.

Turning to the facts here, the Court has determined that the records at issue remain the private property of Mr. Ziegler. He has established ownership. And he has established that his property is not contraband, the fruit of criminal activity, or in need to be held as evidence for a future prosecution.

The question, then, is what, if anything, can be done by Mr. Ziegler (or Mrs. Ziegler, as it relates to marital communications) to shield his private property from public disclosure.

The Court is unaware of any published appellate court decision in Florida that directly addresses the public's right to disclosure of documents illegally seized by the government during an official investigation. The Court is aware, though, that despite Florida's public record law, the Palm Beach County Court ordered the destruction of a surveillance video obtained via a warrant but where the seizure occurred in violation of the defendant's Fourth Amendment rights. State of Florida v. Robert Kraft, 2019-MM-2346, 2019-MM-2348 (Fla. Palm Beach Cnty. Ct. order July 30, 2021).

The facts occurring before the trial court's destruction order were discussed in State v. Kraft, 301 So. 3d 981 (Fla. 4th DCA 2020). Law enforcement there was investigating massage parlors suspected of housing prostitution activity. Law enforcement sought, and obtained, a warrant to install a secret, non-audio video camera in places in the massage parlor where prostitution activities were believed to be occurring, including the massage room. There was no minimization in the warrant, and detectives were not given any instructions on how to minimize to avoid constitutional violation. Robert Kraft and many others were video recorded at the establishment, arrested, and prosecuted for soliciting prostitution. The trial court suppressed the

video surveillance based on the Fourth Amendment violation without any exception to the exclusionary rule applicable. The Fourth District affirmed.

There was a pretrial protective order in place preventing the video's release. After the evidence against him was suppressed, Mr. Kraft moved to modify the protective order seeking to prohibit the permanent release of the video. State v. Kraft, 2019-MM-2346, 2019-MM-2348 (Fla. Palm Beach Cnty. Ct. filing on May 13, 2021, pp. 2-4). A few months later, Mr. Kraft then moved to compel the destruction of the video, noting that it was unopposed by the State. Id. (Filing on July 29, 2021). (Previously, the State had opposed due to pending other litigation. Id. (Filing on Dec. 30, 2020). The trial court granted the motion and directed the State to "destroy the suppressed evidence forthwith and submit documentation to this Court outlining the steps it took to comply." Id. (order July 30, 2021). The Court found no appeal of that Order.

By separate Order entered today, the Court is taking judicial notice of the Kraft trial court filings. As noted in that order, because the Court is taking judicial notice, the Court is permitting the parties an opportunity to advise as to the propriety of the Court taking judicial notice.

The decision in Kraft establishes that a remedy can be the destruction of evidence obtained in violation of a person's Fourth Amendment rights. In Kraft the video never was Mr. Kraft's personal property; instead, it simply captured private moments in an area where he had an expectation of privacy. In this case, the facts are even more compelling because the government seized Mr. Ziegler's personal property.

Although not addressing the issue of improperly seized personal property, the Fourth District in Limbaugh v. State, 887 So. 2d 387 (Fla. 4th DCA 2004), did address medical records containing information of a criminal defendant, Rush Limbaugh. The main holding of that case was that Mr. Limbaugh's privacy rights to the content of his medical records was not implicated by the State's seizure and review of those medical records based on a valid warrant in an investigation of unlawful doctor shopping seeking to obtain controlled substances. The Fourth District though, explained its denial of certiorari was without prejudice to Mr. Limbaugh seeking "review by the issuing Judge to insure that all the records produced fall within the scope of the warrants, **and to seek other protective relief to prevent improper disclosures to third parties of records irrelevant to this prosecution.**" Id. at 398 (footnote citing to the statute allowing return of seized items omitted).

This last sentence suggests two things important here. *First*, there could be a remedy relating to documents seized in violation of the warrant. *Second*, Mr. Limbaugh retained a level of control to prevent disclosure to others of records not relevant to the prosecution. These suggestions would seem to apply here—especially the second—because almost all data SPD seized from Mr. Ziegler based on the three warrants is entirely irrelevant to the investigation.

Additionally, the Court notes there are Florida cases that have peripherally implied that, under facts like those here, an individual's constitutional rights prevail over the public's right to disclosure. These cases, though, are not directly relevant, are not as strong as Kraft, and to a lesser extent, Limbaugh, and could support either the Zieglers' or Intervenor's position.

- Florida Freedom Newspapers, Inc., 520 So. 2d 32, 34 (Fla. 1988) (noting prior to trial that there may be instances where court records should remain sealed out of respect for an individual’s constitutional rights).
- Shevin v. Byron, Harless, Schaffer, Reid & Associates, Inc., 379 So. 2d 633, 638 (Fla. 1980) (holding that under the facts of that case, a violation of an individual’s “disclosural privacy interest” *standing alone*, does not present a constitutionally protected interest sufficient to prevent public disclosure);
- National Collegiate Athletic Association v. Associated Press, 18 So. 3d 1201, 1214 (Fla. 1st DCA 2009) (holding that the application of the Florida public record law did not violate any constitutional right under the facts of that case and, therefore, the public records could be released);
- Roberts v. News-Press Publishing Co., Inc., 409 So. 2d 1089, 1094 (Fla. 2d DCA 1982) (analyzing the post Shevin case law and noting that "it seems clear that there is a potential federal constitutional right of disclosural privacy for employees that may exist in addition to the limited statutory exemptions in regard to the contents of personnel files").

Having concluded that each of the three warrants violated Mr. Ziegler’s constitutional rights, the Court concludes that Mr. Ziegler has the right to the return of his personal property. This right-of-return includes the right to exclusive possession of his property and the right to prevent disclosure to, or review by, others of his data. Failure to do so would result in further constitutional injury to Mr. Ziegler.

Mr. Ziegler’s request to destroy the contents of the data seized from those three warrants is a permissible remedy he has regardless of the existence of Florida’s broad public record provisions. And the Court will allow it.

There are two limitations to this ruling. *First*, the Court reminds that Mr. Ziegler voluntarily produced the Video to law enforcement and the 14 photographs taken by Specialist Yang, and therefore, those items were not seized unconstitutionally. *Second*, because Mr. Ziegler conceded that the data previously publicly produced is already in the public domain, there is no need to destroy that data. Thus, those items will not be part of the Court’s destruction order.

Before leaving this section, the Court notes several items touching on today’s analysis. The data seized in violation of Mr. Ziegler’s constitutional rights does not qualify as a public record. Recall the definition of public record requires it to be “made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.” §119.011(12), Fla. Stat. The seized ESI here cannot be made pursuant to a law or ordinance when it was seized *in violation* of Mr. Ziegler’s constitutional rights. Further, as SPD’s actions *exceeded* their lawful authority, the ESI was not received during the transaction of “official business.” Gentile v. Bauder, 718 So. 2d 781, 784 (Fla. 1998) (holding that government officials act in an official capacity only to the extent their conduct does not violate a clearly established

statutory or constitutional right which a reasonable person should have known); O'Boyle v. Town of Gulf Stream, 257 So. 3d 1036, 1040–41 (Fla 4th DCA 2018) (for information to be considered a public record, an official or employee must have prepared, owned, used, or retained it within the scope of his or her employment or agency).

Additionally, the Court is aware that article I, section 23, of Florida's Constitution, textually provides that Florida's privacy right provision "shall not be construed to limit the public's right of access to public records and meetings as provided by law." That exclusion simply does not apply to an individual's right to be secure from unreasonable searches and seizures and against the "unreasonable interception of private communication" nor his right to due process. Indeed, these individual rights have been in existence long before the adoption of the Public Record Act and are basic to the foundations of freedom guaranteed by both the United States and Florida Constitution.

To rule otherwise would be to elevate Florida's public record law over the Fourth, Fifth, and Fourteenth Amendments to the United States Constitution. The Supremacy Clause, see art. VI, U.S. Const., forecloses that construction.

**D.**  
**Alternate Holding – Criminal Investigative Records**

The Court provides this analysis if an appellate or reviewing court ultimately disagrees with the Court's conclusions that Mr. Ziegler's data was seized unconstitutionally.

Assuming *arguendo* that the Mr. Ziegler's ESI were not seized in violation of his constitutional rights, the Court alternatively holds that all ESI deemed irrelevant to SPD's investigation was not received or held "with the intent of perpetuating or formalizing knowledge' in connection with the transaction of official agency business" and is not subject to public disclosure. State v. City of Clearwater, 863 So. 2d 149, 154 (Fla. 2003).

As applied to this case, especially in the light of Detective Cox's testimony, this includes without limitation to: (1) the entirety of ESI seized pursuant to the Google and Meta/Instagram warrants as they contained no information relevant to SPD's investigation; (2) all 250,000+ photographs and 30,000+ videos from Mr. Ziegler's cell phone, specifically including those marked with the F7 as Detective Cox's testimony established none revealed any criminal conduct or implicated the sexual battery investigation; (3) the "List" as the testimony demonstrated it was not relevant to the potential criminal charge (Exhibit Q, paragraph 15i); and (4) all data not marked F7. This information plainly is not public record.

As it pertains to the information seized based on the cellphone warrant identified on Exhibit Q, the evidence established that Paragraphs 1-14 previously have been publicly produced and no longer addressed by this case. The Court found that Mr. Ziegler voluntarily produced the Video to law enforcement (Paragraph 16 of Exhibit Q).

That leaves the remainder of the items identified in Paragraph 15 of Exhibit Q as the only potential items that *may* qualify as public records: (1) those records between Mr. Ziegler and Ms.

Doe (Exhibit Q, paragraph 15e, 15f, 15g and 15k); (2) Mr. Ziegler's web browsing history (Exhibit Q, paragraph 15j); (3) the Cellebrite extraction report (Exhibit Q, paragraph 15h); and (4) depending on the resolution of the spousal privilege issue, certain communications between Mr. and Mrs. Ziegler (Exhibit Q, paragraph 15a, 15b, 15c, and 15d).

The Court hastens to note that it is *not* making an alternative finding that each of the items within these subparagraphs does or does not constitute a public record. The Court would need to adjudicate the Intervenor Defendants' crossclaims to make that determination, and it is not necessary to do so here. And the Court certainly is not adjudicating the existence or nonexistence of a statutory exemption from disclosure in this case. In other words, if the Court erred in its main analysis in this Final Judgment, the custodian will need to make the determination in the first instance if a record is a public record, and if so, whether it is confidential or subject to a statutory exemption.

The Court just noted "depending on the resolution of the spousal privilege issue," which the Court addresses below.

**E.**  
**Mrs. Ziegler's spousal privilege**

The Court's conclusion that Mr. Ziegler is entitled to the return of all data seized by the cellphone warrant (except as specifically exempted) eliminates the need for the Court to address Mrs. Ziegler's spousal privilege claim as all spousal communications are included in the scope of the return/destroy order in Mr. Ziegler's favor.

If, however, an appellate or any reviewing court ultimately disagrees with the Court's conclusions concerning the constitutional violations, the Court provides additional analysis addressing the spousal communications, which are located at Exhibit Q, Paragraphs 15a-15d. The Court first provides its primary analysis and then, its alternative analysis.

*First*, the Court in Section 3-B of this Order concluded that Mrs. Ziegler had standing to raise spousal privilege. The Court held that Mrs. Ziegler has a statutory right to prevent disclosure of spousal communications that were intended to be made in confidence between spouses while married.

As it pertains to the more than 1,200 text messages between Mr. and Mrs. Ziegler (Exhibit Q, paragraphs 15a-15d) seized by SPD under authority of the cellphone warrant, the Court undertook an *in camera* inspection of these communications consistent with the procedure established in Times Publishing Co. v. City of Clearwater, 830 So. 2d 844 (Fla. 2d DCA 2002), *approved by* State v. City of Clearwater, 863 So. 2d 149 (Fla. 2003), where there is a contest whether a document constitutes a public record.

Based on that *in camera* inspection of those communications, the Court finds that each was made by one spouse to the other spouse during the existence of their continuous marriage, and there was no other recipient of those communications. Further, the Court finds that these



communications were intended to be made in confidence between spouses. There has been no waiver.

These communications qualify for protection under section 90.504. As such, both Mr. and Mrs. Ziegler have a protected spousal privilege to prevent another from disclosing these recorded spousal communications pursuant to section 90.504. *Pagan v. State*, 29 So. 3d 938, 958 (Fla. 2009) (holding that either spouse can invoke the privilege and prevent another from disclosing spousal communications). This includes agents of the government.

As previously noted, the statutory adoption of section 90.504 (spousal privilege) occurred *prior* to July 1, 1993. Thus, even assuming the search warrant permitted the seizure of the communication between Mr. and Mrs. Ziegler, and assuming some of them otherwise would qualify as a public record, the substance of those communications would be exempt from disclosure pursuant to article I, section 24(d), Florida Constitution, and section 90.504.

Putting that more directly, none of these 1,200+ communications between the Zieglers may be publicly released.

*Second*, assuming the Court's conclusion that Mrs. Ziegler may prevent disclosure pursuant to section 90.504 is erroneous, almost none of those communications qualify as a public record. Almost none of them have any nexus to the sexual battery charge being investigated by the cellphone warrant. And that is not surprising, as almost all of them were exchanged by the Zieglers more than two years before the alleged crime.

The only communications that may arguably have some tangential nexus that could conceivably be a criminal investigative record would be:

<b>All messages from beginning message to ending message, inclusive</b>	
<b>Beginning message</b>	<b>Ending message</b>
2/5/2021 at 12:40:54 p.m.	2/5/2021 at 3:36:42 p.m.
2/19/2021 at 2:18:12 p.m.	2/19/2021 at 2:21:40 p.m.
2/19/2021 at 8:48:20 p.m.	2/19/2021 at 8:39:46 p.m.
2/19/2021 at 11:00:33 p.m.	2/19/2021 at 11:34:29 p.m.
2/19/2021 at 11:37:16 p.m.	2/19/2021 at 11:43:26 p.m.
2/25/2021 at 10:13:49 p.m.	2/25/2021 at 10:22:37 p.m.
3/10/2021 at 11:22:56 p.m.	3/10/2021 at 11:22:56 p.m.
3/10/2021 at 11:32:27 p.m.	3/10/2021 at 11:36:24 p.m.
6/20/2021 at 5:49:15 p.m.	6/20/2021 at 5:49:15 p.m.

Again, this is not a finding that these qualify as a public record. It is only an alternative finding that this is the universe of spousal communications that may constitute public record. Other than those communications, though, none could qualify as a public record.

**9.**  
**PUBLIC RECORD RETENTION AFFIRMATIVE DEFENSE**

The State Attorney's Office has also raised the affirmative defense that they are required to retain felony files for one year in accordance with records retention requirements set by Rule 1B-24.003(1)(b), Fla. Admin. Code. However, the Court notes that this rule was adopted pursuant to section 119.021(2)(a)-(d), Fla. Stat. as it applies to "public records." To the extent that this ruling has found that the records at issue are the private records of Mr. Ziegler, the Court also finds that this provision does not apply.

## **10. CONCLUSION**

Each of the three warrants in this case violated Mr. Ziegler's Fourth Amendment rights. Those warrants were vastly overbroad. They did not describe with particularity the items to seize. There was no search protocol included.

Instead, these warrants were "general warrants" that allowed unreasonable searches and seizures. Since the inception of our country, the Fourth Amendment has guarded against general warrants like those in this case. Law enforcement's actions with respect to these three warrants were patently erroneous and constitutionally intolerable. Mr. Ziegler's property was searched and seized in violation of his constitutional rights.

Mr. Ziegler was not arrested, and all criminal investigations of him are complete. No criminal charges were brought or contemplated. There is no need for law enforcement or the State Attorney's Office to retain the contents of Mr. Ziegler's cellphone, Google Drive, or Meta/Instagram accounts for purposes as evidence against Mr. Ziegler or others for future prosecution. None of the data constitutes contraband or the fruit of criminal activity.

In these circumstances, Mr. Ziegler has the legal right to the return of his property. This right includes exclusive possession and control of his property. A corollary right is the ability to preclude others from reviewing his property. These rights derive from the Fourth, Fifth, and Fourteenth Amendments to the United States Constitution.

Article 1, section 24, Florida Constitution, gives every person the right to inspect and copy any public record unless it is confidential or exempt from disclosure. Mr. Ziegler's property was not converted to public record by law enforcement's search and seizure. Further, Mr. Ziegler's property cannot be considered public record because violating a person's constitutional rights forecloses a finding it was "made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency." Florida's public record law does not apply to this situation.

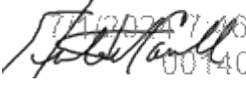
There is precedent in Florida for a court to order law enforcement to destroy illegally seized material in violation of a person's Fourth Amendment rights. And that is what Mr. Ziegler requests, and the Court grants that request.

**IT IS ORDERED AND ADJUDGED:**

1. The Court grants judgment in favor of Christian Ziegler as to each of Counts 1, 2, 3, and 4 as discussed in this Order.
2. Plaintiff Bridget Ziegler has standing to advance her spousal privilege claim. Based on the Court's resolution of Mr. Ziegler's claims, there is no need to award Mrs. Ziegler relief because her relief is accomplished by Mr. Ziegler's relief.
3. Each of the three search warrants to seize Mr. Ziegler's cellphone, Google Drive, and Instagram accounts violated Mr. Ziegler's constitutional rights.
4. Except as discussed in this decretal paragraph 4, the entirety of the data seized by the Sarasota Police Department based on the cellphone warrant belongs to Mr. Ziegler, and he is entitled to its return regardless of whether it is in the possession of the City of Sarasota/Sarasota Police Department or the State Attorney's Office for the Twelfth Judicial Circuit or both. The only exceptions are:
  - a. The Video Mr. Ziegler voluntarily provided to the Sarasota Police Department (also referenced at Exhibit Q, paragraph 16);
  - b. The 14 photographs Specialist Yang took on December 1, 2023, of Mr. Ziegler's cellphone and screens during the Video turnover; and
  - c. Any of Mr. Ziegler's data previously publicly produced by the Sarasota Police Department or State Attorney's Office.
5. The entirety of the data seized by the Sarasota Police Department based on the Google warrant belongs to Mr. Ziegler, and he is entitled to its return regardless of whether it is in the possession of the City of Sarasota/Sarasota Police Department or the State Attorney's Office for the Twelfth Judicial Circuit or both.
6. The entirety of the data seized by the Sarasota Police Department based on the Meta/Instagram warrant belongs to Mr. Ziegler, and he is entitled to its return regardless of whether it is in the possession of the City of Sarasota/Sarasota Police Department or the State Attorney's Office for the Twelfth Judicial Circuit or both.
7. The entitlement to the return of Mr. Ziegler's property addressed in this Final Judgment specifically grants Mr. Ziegler the right to the exclusive possession and control of his property and the ability to exclude others from obtaining that property.
8. Each of the City of Sarasota/Sarasota Police Department and the State Attorney's Office for the Twelfth Judicial Circuit is permanently enjoined from publicly disclosing the contents of Mr. Ziegler's property seized by any of the three warrants, except as specifically identified in decretal paragraph 4a-4c. The Court's temporary injunction merges into this Final Judgment.

9. Each of the City of Sarasota/Sarasota Police Department and the State Attorney's Office for the Twelfth Judicial Circuit shall destroy the original and all copies of the data seized by any of the three warrants, except as specifically identified in decretal paragraph 4a-4c. The requirement to destroy shall not begin until the later of: (1) the expiration of the time to appeal this Final Judgment; or if there is an appeal (2) the issuance of the mandate. Once the requirement to destroy becomes effective, the City of Sarasota/Sarasota Police Department and the State Attorney's Office for the Twelfth Judicial Circuit will comply promptly and without delay.
10. Within 10 days of executing the destruction requirement, each of City of Sarasota/Sarasota Police Department and the State Attorney's Office for the Twelfth Judicial Circuit will submit an affidavit that is filed in the Court file documenting the steps that it took the comply with the destruction of the data and affirming that it no longer possesses any data covered by this destruction requirement.
11. The Zieglers are entitled to the return of the posted bond. The Clerk shall not return that bond to the Zieglers until further Order of the Court or, if no such Order, the later of: (1) the expiration of the time to appeal this Final Judgment; or if there is an appeal (2) the issuance of the mandate.
12. Nothing in this Final Judgment impacts the status of any public record previously created that referenced or quoted information obtained from the data seized by the three warrants. This includes law enforcement's reports in this matter.
13. The Court did not address the Intervenor Defendants' crossclaims, which were not at issue at the time of trial. Those are severed. Nothing about those pending crossclaims impacts the finality of this Final Judgment. All judicial labor is complete with respect to the Verified Amended Complaint except for collateral matters. This Final Judgment is final.
14. The Court reserves jurisdiction to address enforcement matters as well as any timely filed motion for attorney fees or costs or both.

DONE AND ORDERED in Sarasota, Sarasota County, Florida, on July 01, 2024.

  
7/1/2024 7:46 AM 2024 CA  
001409 NC  
e-Signed 7/1/2024 7:46 AM 2024 CA 001409 NC

**HUNTER W CARROLL**  
Circuit Judge

**SERVICE CERTIFICATE**

On July 01, 2024, the Court caused the foregoing document to be served via the Clerk of Court's case management system, which served the following individuals via email (where indicated). On the same date, the Court also served a copy of the foregoing document via First Class U.S. Mail on the individuals who do not have an email address on file with the Clerk of Court.

JAMES BURGESS LAKE  
THOMAS & LOCICERO PL  
400 NORTH ASHLEY DRIVE STE 1100  
TAMPA, FL 33602

JOSEPH C MLADINICH  
FOURNIER ,CONNOLLY, WARREN & SHAMSEY PA  
1 S SCHOOL AVENUE SUITE 700  
SARASOTA, FL 34237

CRAIG JARETT SCHAEFFER  
2071 RINGLING BLVD  
SARASOTA, FL 34237

MORGAN R BENTLEY  
783 S ORANGE AVE STE 300  
SARASOTA, FL 34236

KAYLIN MARIE HUMERICKHOUSE  
783 S ORANGE AVE STE 300  
SARASOTA, FL 34236

JOSEPH C MLADINICH  
FOURNIER ,CONNOLLY, WARREN & SHAMSEY PA  
1 S SCHOOL AVENUE SUITE 700  
SARASOTA, FL 34237

MATTHEW SETH SARELSON  
3801 PGA BLVD, SUITE 600  
PALM BEACH GARDENS, FL 33410

MICHAEL BARFIELD  
1668 OAK STREET #1  
SARASOTA, FL 34236

SARELSON, MATTHEW SETH  
SCHAEFFER, CRAIG JARETT  
SCHAEFFER, CRAIG JARETT  
BENTLEY, MORGAN R  
SARELSON, MATTHEW SETH  
LAKE, JAMES BURGES  
MLADINICH, JOSEPH C  
MLADINICH, JOSEPH C

HUMERICKHOUSE, KAYLIN MARIE  
SCHAEFFER, CRAIG JARETT  
BENTLEY, MORGAN R  
BARFIELD, MICHAEL  
SARELSON, MATTHEW SETH  
HUMERICKHOUSE, KAYLIN MARIE  
SCHAEFFER, CRAIG JARETT  
LAKE, JAMES BURGES  
Joseph Polzak  
Mark R. Caramanica  
Mark R. Caramanica  
Zachary Stoner  
Michael Barfield  
Robert Fournier  
Joseph Mladinich

alfrancis@dhillonlaw.com  
CSCHAEFF@SAO12.ORG  
EBRODSKY@SAO12.ORG  
ESERVE@BGK.LAW  
haguillard@dhillonlaw.com  
jlake@tlolawfirm.com  
JOE.MLADINICH@SARASOTAFL.GOV  
KATHERINE.CORDERO@SARASOTAFL.  
GOV  
KHUMERICKHOUSE@BGK.LAW  
LPARCELS@SAO12.ORG  
MBENTLEY@BGK.LAW  
MICHAEL@DENOVLAWFL.COM  
msarelson@dhillonlaw.com  
saorounds@sao12.org  
SSHIFFLET@SAO12.ORG  
TGILLEY@TLOLAWFIRM.COM  
Joe.Polzak@sarasotafl.gov  
mcaramanica@tlolawfirm.com  
jvanderhorst@tlolawfirm.com  
zstoner@dhillonlaw.com  
mbar62@gmail.com  
robert.fournier@sarasotafl.gov  
jmladinich@fournierconnolly.com