RECEIVED
Aug 09 2024
SC Court of Appeals

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

MOTION FROM CHARLESTON COUNTY FAMILY COURT

Family Court Case No. 2022-DR-10-3072

Appellate Case No. 2023-001376

Justin McGee, ... Respondent,

v.

Lindsay F. McGee, ...Petitioner.

Reply to Court Order

The following is in response to this Courts Order July 22, 2024 which directed the parties to provide a return addressing: 1. How this court can rule on Petitioners Motion to suppress when the contents of alleged interception are unknown?; and 2. The feasibility of the parties' viewing copies of the communication and themselves and informing the family court what, if any, of the recording contained information which could be considered intercepted communication pursuant to the act?

As this Court has on several occasions has set out the South Carolina Home Land Security Act prohibits the intentional interception, attempt interception, or procedures or procure any other person to intercept or attempt to intercept any oral or electronic communication 17-30-20; (1) intentionally uses attempts to use or precures any other person to use or attempts to use any electronic mechanical other devices to intercept any oral communication (2) intentionally disclose or attempt to disclose. Or attempts to use the contents of any wire oral or electronic communication knowing or having reason to know that the information was obtained through the intercepts of wire or oral or electronic communication violation by the subsection … (see South Carolian Code section 17-30-20) et seq.

The Petitioner has submitted to this Court Affidavits of Mr. Steven Abrams and John Bumgardner, both highly trained and respected experts in the area of electronic communication, the contents of those Affidavits are set out herein as set forth verbatim.

If this Court has any concerns whether or not any actual interception took place certainly there cannot be any question that attempts to intercept occurred literally over months and months and months. Recall that the facts that set out in the experts Affidavits highlight that the respondent Justin McGee purchased numerous recording devices and even admitted to placing at least one of these devices in the home then occupied by the Petitioner Lindsey McGee and her children. Attached to this return is a Fifth Supplemental Affidavit by Mr. Abrams summarizing some of the contents of the intercepted communications based upon his review of these communications. There are literally hundreds of hours of additional recordings which have not been reviewed. Mr. Abrams highlights the work that he has done in reviewing a portion of the intercepted communications.

This Court asks how they can issue an order to suppress when the contents of the recordings are unknown. As pointed out in this Court's Order section 17-30-110 (A) grants this court the authority to "suppress the contents of any intercepted wire, oral, or electronic communication or evidence derived thereof. This court has the ability to issue a suppression order simply setting out that any evidence as contained in an intercepted wire or oral or electronic communication or any evidence derived from that communication should suppressed. The respondent may have the ability to argue that he has an independent source and that the evidence that he seeks to admit was not illegally intercepted or derived thereto.

It is absolutely not feasible for either of these parties to review all 833 hours of recordings or to pay their portion of the $249,900.00 as directed by the lower court.

The above suggested solution would allow this matter to go forward, thus shifting the burden on to the respondent (wrong doer) to show that any evidence which he seeks to present to the court was independently secured and not a result of an illegal interception or evidence derived there from. This suggested solution should result in each party has the ability to review copies of any communication themselves and inform the family court what if any of the communications were in fact illegally intercepted pursuant to the act.

Respectfully submitted,

s/Richard G. Whiting
Richard G. Whiting
Attorney for Plaintiff
1515 Lady Street (29201)
Post Office Box 7877
Columbia, SC 29202
803-256-9067
dick.whiting@whitinglawsc.com

s/Peter G. Currence
Peter G. Currence
Attorney for Plaintiff
791 Greenlawn Dr., Suite 4 (29209)
Post Office Box 90860 29290-1860
Columbia, SC 29209
803-776-3130
pete@mscmlaw.com

August 9, 2024

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY
Family Court

Family Court Case No. 2022-DR-10-3072

Appellate Case No. 2023-001376

Lindsay F. McGee, Petitioner,

v.

Justin McGee, Respondent.

FIFTH SUPPLEMENTAL

AFFIDAVIT OF STEVEN MARC ABRAMS, J.D., M.S.

PERSONALLY APPEARED BEFORE ME, the undersigned, who, being duly sworn, deposes and states the following:

Background

1. My Name is Steven Marc Abrams. I am a licensed Attorney and Counselor at Law, in good standing, in South Carolina, Washington, DC, and New York. I am a member of the South Carolina Bar, The Washington DC Bar, The New York State Bar Association, and the New York State Academy of Trial Lawyers. I am a retired South Carolina State Constable. My field of concentration is digital forensics. I have assisted municipal, county, state, and federal law enforcement agencies and the US Department of Defense and the Department of State with digital forensics investigations for over three decades. For 11 years, from 2008 until 2019, until

my retirement I held a law enforcement commission from the Governor of South Carolina at the request of the United States Secret Service. In all I have spent over 40 years in the field of digital forensics, and nearly two decades in the practice of law. My office address is 1154 Holly Bend Drive, Mount Pleasant, South Carolina 29466. My office phone number is (843) 813-1996. My full credentials are included in my CV which is appended to this affidavit.

2. For over a year, my colleague John Bumgarner, an expert in network forensics, and I have been working for attorneys Peter G. Currence and Richard G. Whiting to investigate allegations of cyber spying (eavesdropping and interceptions) on attorney Lindsay McGee ("Petitioner") which occurred in her McCutchen Street, James Island home for over nine months in 2022. Between the two of us, Mr. Bumgarner and I have filed thirteen affidavits in the family court and South Carolina Court of Appeals with our findings in this matter based on technical (forensic examination of recovered cameras, AT&T internet bandwidth logs, router logs) and documentary evidence (Respondent's camera purchase history and family court pleadings in this matter). The conclusion to be drawn from our investigation is that 1) There is no question but that Respondent attempted to intercept Petitioner's conversations (including attorney client privileged conversations) in her home; 2) It is very likely (beyond a preponderance standard) that actual interceptions did occur; and because all these interceptions occurred months before Respondent filed anything in the family court, 3) It is likely that Respondent's entire course of litigation in the family court against Petitioner is based directly upon or is derivative of his illegal aural interceptions of Petitioner.

3. We have documented to scientific certainty that illegal interceptions of Petitioner's aural communications occurred between at least February of 2022 and October of 2022. These

interceptions were accomplished using at least eight[1] different covert spy cameras with audio capabilities that after having been purchased by Respondent were placed simultaneously in Petitioner's home recording virtually every word spoken in the home. In total there were thirteen covert cameras purchased by Respondent placed simultaneously into Petitioner's 1500 square foot home, recording her every movement. At no time before their detection and removal was Petitioner aware of these covert spy cameras, nor did she ever consent to them being secreted in her home. This level of covert surveillance is unprecedented in any investigation that Mr. Bumgarner or I have seen in our more than 70 years of combined experience.

Technical Evidence

4. The technical evidence in this case consists of the forensic evidence extracted from the two covert cameras found in Petitioner's home, the router logs from Petitioner's home Internet router, and the bandwidth logs from Petitioner's AT&T Internet account.

5. From the router logs we learned that thirteen covert cameras were operating in Petitioner's home during much of 2022. As part of our investigation into possible cyber spying in Petitioner's residence, the network logs from Petitioner's home router were reviewed by Mr. Bumgarner. His review of the router logs indicated conclusively to a scientific certainty that there had been a total of thirteen covert cameras in Petitioner's residence.

6. Upon this revelation, Petitioner remembered that Respondent had been in her home prior to when she purchased it, having offered to install "outlet splitters" on some of her electric outlets. Searches conducted in the summer and fall of 2023 located two of these covert cameras

[1] Technical and documentary evidence strongly suggests that Respondent placed a ninth audio enabled camera into Petitioner's McCutchen home in addition to the eight devices that are known to a scientific certainty to have been secreted in the house and connected to Petitioner's Wi-Fi network.

remaining in Petitioner's home. The cameras were disguised to look like an outlet splitter and a USB hub. One of these cameras ("CamDuck") resembling a USB hub was initially set up by Respondent on Petitioner's bedside table but later placed in the cabinet under the bedside table by Petitioner where it was forgotten until she later discovered it in November 2023 while searching her home for covert cameras. The CamDuck had audio and video recordings from 2022 intact on the SD memory card within the device. There were over 5000 ten-minute video/audio segments recovered from the SD card. Forensic artifacts from the SD card indicated that these 5000 video segments, many from August and September 2022, were only a small fraction of the material that likely was captured by the camera. Most of the 20,000 recordings captured by the camera had been overwritten by subsequent use of the device and in some cases manually deleted. Upon consent of Petitioner, I reviewed the contents of the videos contained on the SD card. Below I will detail the most significant content that I observed from these audio/video files.

7. The other technical evidence consists of AT&T internet bandwidth records. Normally, home internet traffic is primarily inbound to the home. The majority of data flows into a home as a result of the consumption of content from the Internet such as Netflix and other TV streaming content, CNN and other news content, and web browsing. However, in Petitioner's home in August and September 2022 most of the data was flowing out of the home. We believe this is because of the data being streamed out from all the covert cameras hidden in Petitioner's home. We have no other plausible explanation for the high outbound traffic in this bandwidth report. This indicates that not only were the cameras connected to the Wi-Fi router, but they were actually streaming content, presumably to Respondent, who purchased them, and set them up. Respondent has admitted in responsive pleadings in the family court that he downloaded the

Apps to his iPhone needed to configure and monitor the CamDuck and SCS cameras. Mr. Bumgarner's testing of the CamDuck software and camera showed that the user must manually initiate audio recording using the App, and has to initiate streaming over the Internet using the App. The cameras remain nascent in a stealth mode until they are polled remotely by the user of the CamDuck App. The bandwidth records and our experiments with the App make it more likely than not that Respondent was remotely monitoring at least the CamDuck camera after having configured it to record audio.

8. The Internet bandwidth records indicate that multiple cameras were streaming out on the Internet because of the sheer volume of data reported by AT&T in these bandwidth reports. From the technical and documentary evidence, there is proof[2] that at least eight and very likely nine audio enabled cameras were installed on Petitioner's Wi-Fi router based on MAC addresses and network names, only one of which (CamDuck in bedroom) we were able to find and examine. Because we never had an opportunity to examine the other two CamDuck cameras we cannot determine with complete certainty that the other CamDuck MAC addresses seen in the logs are a precise match to the remaining two CamDuck cameras that Respondent purchased. Respondent's filing ("Chart of Devices", Bates McGee(HSA)_00001A, see attached) says nothing about the other two CamDuck devices, and they were never produced.

[2] SCS Enterprise cameras broadcast the network name of "GF-PH130". Seven of these SCS cameras were seen in the router logs. Five of the seven SCS cameras installed on Petitioner's Wi-Fi were equipped with audio. This is based on the evidence developed during discovery, including 1) Respondent's purchase records, 2) SCS MAC addresses in responsive pleadings by Nelson Mullins, 3) MAC address of the SCS camera we have analyzed, and 4) SCS MAC addresses the router logs.
"SHENZHEN" is the network name broadcast by CamDuck cameras. Based on this network name and three very similar MAC addresses seen in the router logs we are nearly certain that all three CamDuck cameras with audio purchased by Respondent were installed on Petitioner's Wi-Fi router.

Documentary Evidence

9. The documentary evidence used in our investigation consists of Respondent's purchase history[3] that showed in 2021 and 2022 he purchased cameras identical to the ones recovered from Petitioners' home and seen in her router logs.

10. Respondent's purchase records show that there were nine cameras with audio purchased in 2021 and 2022. Of these, three CamDuck cameras with audio were purchased on January 30, 2022, from Amazon. Five SCS Enterprises cameras with audio were purchased between January and July 2022. There was one RXAMYDE camera with audio purchased in 2021.

11. In Respondent's filings in the family court, he admitted to placing at least one of the cameras in Petitioner's home and admitted that he downloaded the software needed to configure and remotely monitor CamDuck cameras. This puts the CamDuck camera we found into Respondent's hands along with the software needed to enable audio recording, remote monitoring, and connection to Petitioner's Wi-Fi router prior to the camera being found with covert audio and video recorded on it in Petitioner's bedroom. The CamDuck we examined contained evidence that it had been connected to Petitioner's Wi-F network [4] and had been accessed remotely.

12. Based on the notes in Respondent's "Chart of Devices" (Bates "McGee(HSA)_0001A") and a comparison of the MAC addresses of the SCS cameras being held at Nelson Mullins with the MAC addresses recorded in Petitioner's router logs, we know to a scientific certainty that

[3] In total Respondent is known to have purchased thirty-two (32) covert cameras from December 2020 through July 2022. Respondent's "Chart of Devices" only lists 26 cameras, leaving eight cameras, including two CamDuck cameras, unaccounted for.

[4] The MAC address of the CamDuck in our possession precisely matches one of the MAC addresses identified in the Petitioner's router logs.

Respondent placed all five of the SCS Enterprises cameras with audio capabilities that he purchased into Petitioner's home and connected them on her Wi-Fi network so they could be remotely monitored in February 2022. In the note on item 11 of Respondent's Chart of Devices, cited above, he admits to taking multiple SCS cameras to the McCutchen home of Petitioner as early as July 2021. Respondent admits to connecting the SCS cameras at Petitioner's home to the App (on his phone). Respondent claims he removed some of the SCS devices from Petitioner's home but admits that "[t]wo likely remained at McCutchen House until August 2022 although one was left in the garage."

Figure 1 - Photo taken by Petitioner in her kitchen in August 2022 showing SCS covert camera installed to an outlet. She was unaware this was a camera attached to her Wi-Fi network and she was being spied on in her own home.

Spoilation

13. In March of 2023, Respondent came into Petitioner's home without her permission and took a golf cart from the garage[5] and the assumption is that he removed all the cameras that he could find in the home at that time. In reply to Petitioners' request that he produce the cameras for inspection, Respondent has stated in filings in this matter that he destroyed and discarded many of the cameras he purchased only months before[6], some because of alleged damage and others inexplicably. Regardless of why they were discarded during the course of litigation, they were not available to be produced to Petitioner per her Request for Production. This left Petitioner with only the two cameras found in her residence to search for evidence of interceptions, even though it is known from the router logs that there were thirteen covert video cameras secreted in Petitioner's home by Respondent, up to nine of which were capable of recording audio simultaneously.

Contents of the CamDuck SD card

14. The CamDuck camera can be placed in motion detection mode or continuous record mode. Because the CamDuck was placed in the cabinet under Petitioner's bedside table which has a door that is usually closed, there was seldom any motion seen by the camera to initiate recording. Therefore, at some point the CamDuck was changed to continuous recording. We know this because there are artifacts on the SD card from motion activated and continuous recording modes. The continuous recordings remaining on the camera span from 12:00AM August 24, 2022, through 8:38PM September 29, 2022. Hurricane Ian came through

[5] Respondent had a GPS tracking device on Petitioner's vehicle at this time and would have been aware of her location away from her home.

[6] Respondent claims he threw away a camera in August 2022 that his purchase records reflect he purchased on July 26, 2022, while he was having his Wife followed by a private investigator.

Charleston on September 28 and 29, 2022, and it is believed that power was lost to the CamDuck as a result of the Hurricane explaining the sudden cessation of recording observed in the videos found on the SD card. There was one final sequence of recording on October 3, 2022, that corresponded with Petitioner plugging in the power strip on which the CamDuck was attached after it had been removed from the wall during the storm.

Respondent's filings do not dispute the interception details that we determined from data on the SD card, nor has he identified an expert to refute the interception details that we determined from data on the SD card.

15. Moreover, Respondent filed an affidavit in the family court on September 29, 2023, in which he stated, "12. I have not installed, placed, accessed, removed, used, deleted files from, watched or listened to footage from, or otherwise had anything to do with any camera at McCutchen House *since the Summer of 2022.*" (*Emphasis added.*). Respondent's statement seems to be crafted so as not to challenge or contradict our findings based on the data from the CamDuck camera found in Petitioner's bedroom in the McCutchen house, that all of the intercepted audio and video ended at the close of Summer 2022.

How the video was examined

16. Given there are approximately 5000 ten-minute videos it would have been cost prohibitive to watch/listen to every segment. I developed two strategies to find the most important video segments. I requested that Petitioner provide me with a timeline of specific conversations that were likely heard in the bedroom (see exhibit 1). Based on this timeline, I reviewed the videos for intelligible audio. I found that when the cabinet door was closed, and Petitioner was not close to the cabinet the audio was muffled and hard to hear clearly. When the doors were open, or the person(s) speaking were on the bed or close to the cabinet the audio was clear and could

be understood. Besides the timeline approach, I also processed the videos using my Cellebrite Inspector software and was able to separate out the videos made while the cabinet door was open. I was able to see and hear the visual and audio content of these videos.

A comparison of Respondent's pleadings with the audio from CamDuck recordings supports the conclusion that the aural interception of Petitioner was the original source of Respondent's most inflammatory allegations

17. On June 12, 2023, Respondent filed a 34-page affidavit in Support of his Motion for Temporary Relief in which he makes several allegations. I have reviewed the videos recorded in Petitioner's bedroom nine months to a year earlier to see if the source of these allegations (many of which would be impossible to know about unless one was inside Petitioner's home) could be the covert video/audio cameras that Respondent secreted in Petitioner's house. These are the items where suppression seems most appropriate.

1. In reviewing this material, it is important to keep in mind that not only were these cameras recording to the SD card, but based on the router logs that proved these cameras were connected to the Internet, and the Internet bandwidth records that indicated that data was streaming out of the house, it is almost certain[7] that Respondent was viewing this video/audio remotely months before he made the allegations contained in his Complaint and June 12, 2023 affidavit.

[7] Complete scientific certainty cannot be obtained because Respondent has not produced any of his mobile devices on which the CamDuck App was installed in 2022. He claims to have done a factory reset on one of these iPhones, and another was allegedly damaged and discarded. Respondent stated in a filing that the iPhone 8 that was factory reset had been used to monitor the cameras. Respondent is still in possession of another iPhone XS that he stated had the CamDuck App installed on it, but he has never produced this device for examination.

18. The most striking example of an allegation in Respondent's affidavit that seems to have come directly from material overheard in Petitioner's bedroom is found on page 7, item q., of Respondent's affidavit,

> "On September 3, 2022, she invited a man she didn't know to her home and engaged in unprotected sex with him. She contracted a sexually transmitted infection and admitted it was from having sex with this person." (Respondent June 12, 2023, Affidavit in Support of Temporary Relief, pg. 7).

I located a video segment on the CamDuck SD card from the wee hours of September 4, 2022, in which Petitioner and a male visitor were in Petitioner's bed about to have sex and there ensues a brief discussion and search for condoms. At 4:39:36AM on September 4, 2022, male voice - "No, I got no, … you know." 4:39:45AM - Petitioner can be seen on video through open cabinet door looking inside her bedside cabinet, "Sorry, let me look…", She doesn't find anything, and they get back to what they were doing.

Petitioner has told me that she did not have a sexually transmitted infection from that encounter, but that she did discuss something like that with a friend within her house that Respondent may have overheard from all the cameras that were placed around her house. The exact date of the encounter may have been learned by a PI outside of Petitioner's house but the unprotected sex on that date could only be known to someone with eyes and/or ears inside of petitioner's house. This would seem to close the loop and confirm that Respondent was watching and listening to what was going on inside of Petitioner's bedroom. It should also be noted that while other allegations were footnoted with the source, there were curiously no sources attributed to these allegations.

19. In addition, Petitioner has reason to believe that there was more than one camera in her bedroom that morning, as Respondent later taunted Petitioner about the encounter with exact

details, suggesting Respondent could see Petitioner and her male companion, something not possible from inside the cabinet where the CamDuck was installed.

20. Further confirmation that item q was based on observations of Petitioner inside her home comes from manual annotations on the GPS tracking logs produced by Respondent. On October 1, 2022, Petitioner went to seek medical attention at the Premier Medical urgent care facility at 354 Folly Road on James Island. Respondent and his PI, John Clayton, had been tracking Petitioner's movements for months with a series of GPS transmitters affixed to her car. The GPS tracker logs were produced in discovery. These logs were extensive and contained over 20,000 entries, only a few of which were highlighted with manual entries. However, the GPS records on October 1, 2022, showing Petitioner went to the urgent care facility and then to the pharmacy were manually annotated by Respondent or his PI. This suggests that Respondent was keenly aware of Petitioner's conversation in her home regarding her medical complaint such that this visit to the urgent care facility and pharmacy was worth documenting in the GPS logs out of the 20,000 other entries.

21. Page 7, item r, of Respondent's affidavit also contains an allegation that could only have been learned from the covert cameras. "She repeatedly participated in virtual sex with a man who she knew had previously used or attempted to use nude photographs to extort a different female." In reviewing the videos when the cabinet door was open from my Cellebrite report I found a video that depicted Petitioner engaged in phone sex with the individual referenced in Respondent's affidavit. This is the only reasonably likely source of Respondent's knowledge of "virtual sex"; he watched it on the video/audio stream from Petitioner's bedroom. After reviewing the text messages referenced in Respondent's affidavit Exhibit C, Page 14, there

was no "attempt to use nude photographs to extort a different female", it was clearly a hypothetical presented as a bad joke among a group of friends.

Additional intercepted material on the CamDuck SD card

22. Other content observed in the videos from Petitioner's bedroom included marijuana use, and conversations with friends about Petitioner's marital strife and childhood traumas.

The sheer number of covert cameras secreted in Petitioner's small house ensured total coverage of the premises for monitoring of Petitioner's speech and actions.

23. In video from the SD card in the SCS camera recovered from Petitioner's garage, Petitioner can be observed pacing back and forth while in an intense phone conversation. While this camera had no audio, it is likely that one of the eight or nine cameras with audio may have recorded this and other conversations held throughout Petitioner's home.

24. Given there were at least eight cameras with audio capabilities installed in Petitioner's home, and we were given an opportunity to examine only one of them, it is likely that Respondent had access to every spoken word in Petitioner's home during the period during which the cameras were installed in her home. Therefore, given the spoliation that Respondent has admitted to, we will never be able to conclusively know what Respondent learned from his interceptions, but it should be assumed he learned much more than we were able to see on this one camera recovered from Petitioner's bedroom cabinet.

FURTHER THE AFFIANT SAYETH NOT!

Steven Marc Abrams, J.D., M.S.

SWORN TO AND SUBSCRIBED BEFORE ME THIS
07, **DAY OF** August, **2024.**

NOTARY PUBLIC FOR SOUTH CAROLINA
MY COMMISSION EXPIRES: 7/21/2033

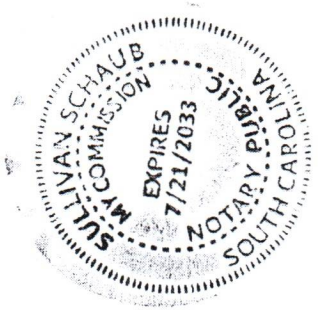

Chart of Devices
McGee v. McGee - No. 2022-DR-10-3072

No.	Device Name	Model Number	Vendor	Order Number	Purchase Date	Audio Capability	Software or Application	Current Location	Notes
1	Vtech Monitor	VM321-2	Amazon - Vtech Store	...4210	10/1/2020	Yes	Unknown	Ready to produce.	Baby monitor with two cameras. Wife regularly used these devices. No known specific date range of installation and use.
2	Weather Station	zweatherstation-500w	Zetronix	100049779	1/4/2021	Yes	Unknown	Ready to produce.	This device was never used and was only located at Eddie Farm.
3	Mini USB	SG-HC240w-128GB	Spy Gear Gadgets	71256	1/9/2021	Yes	Look Cam Pro	Unknown	Upon information and belief, this device was used exclusively at Eddie Farm.
4	Wireless Charger Alarm Clock	MAC-RWCRRIR	The Spy Store	16352	1/4/2021	No	HDLiveCam	Unknown	Upon information and belief, Wife disposed of this in August 2021. Wife brought this device to McCutchen House on or about February 18, 2021.
5	Router	DMY-RT-NVC	Home Security Superstore	391906	4/27/2021	No	Tiny Cam Pro	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	This device may have been set up at McCutchen House at approximately the end of April 2021, but it was never used to intercept video and/or audio.
6	Air Cleaner	AIRFRESH-WIFI	Big Security	778098	4/27/2021	No	Tuya Smart	Unknown	Upon information and belief, this device was thrown away after it stopped working in approximately fall 2021. Wife used it during approximately July 2021 when she smoked marijuana. It was replaced months later by the Palm Vid below.
7	RXAMYDE USB	B08YQYM6W9	Amazon	...5025	5/28/2021	No	HDLiveCam	Unknown	Husband lacks information about the use and location of this device.
8	SCS Fan	WF-422	Amazon - SCS Store	...3023	5/28/2021	No	iOT Living	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	This was exclusively used in the camper, though it may have been opened initially at McCutchen House.
9	SCS Outlet (Up)	WF-113U	Amazon - SCS Store	...7065	7/7/2021	No	iOT Living	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	Unknown whether this was used at McCutchen House or Eddy Farm: two were used at McCutchen House starting in July 2021, and two were taken to Eddy Farm. Initial connection of this device and the App likely occurred in July 2021 at McCutchen House. This or one of the other SCS cameras were removed almost immediately upon set up. Two likely remained at McCutchen House until August 2022, although one was left in the garage.
10	SCS Outlet (Up)	WF-113U	Amazon - SCS Store	...7065	7/7/2021	No	iOT Living	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	Unknown whether this was used at McCutchen House or Eddy Farm: two were used at 664 starting in July 2021, and two were taken to Eddy Farm. Initial connection of this device and the App likely occurred in July 2021 at McCutchen House. This or one of the other SCS cameras were removed almost immediately upon set up. Two likely remained at McCutchen House until August 2022, although one was left in the garage.
11	SCS Outlet (Down)	WF-113D	Amazon - SCS Store	...3467	7/15/2021	No	iOT Living	Unknown	Unknown whether this was used at McCutchen House or Eddy Farm: two were used at 664 starting in July 2021, and two were taken to Eddy Farm. Initial connection of this device and the App likely occurred in July 2021 at McCutchen House. This or one of the other SCS cameras were removed almost immediately upon set up. Two likely remained at McCutchen House until August 2022, although one was left in the garage.

Chart of Devices
McGee v. McGee - No. 2022-DR-10-3072

No.	Device Name	Model Number	Vendor	Order Number	Purchase Date	Audio Capability	Software or Application	Current Location	Notes
12	SCS Outlet (Down)	WF-113D	Amazon - SCS Store	...0627	7/28/2021	No	iOT Living	Unknown	Unknown whether this was used at McCutchen House or Eddy Farm: two were used at 664 starting in July 2021, and two were taken to Eddy Farm. Initial connection of this device and the App likely occurred in July 2021 at McCutchen House. This or one of the other SCS cameras were removed almost immediately upon set up. Two likely remained at McCutchen House until August 2022, although one was left in the garage.
13	5-Port USB Tower	5CGRWIFI	Know Your Nanny website	23054	1/24/2022	Unknown	Unknown	Ready to produce.	This device was never used and was supposed to be returned, but it remains in Husband's possession.
14	Power Hub	CWS-WiFi-HUB 3	Custom WiFi Spy Cameras	104015	1/25/2022	No	HDLiveCam	Unknown	Upon information and belief, this device was not purchased with audio capabilities. It was used in approximately February 2022, until it was thrown away in August 2022.
15	USB Tower	LH-5USB	Amazon - LUOHE Store	...7811	1/30/2022	No	CIXICM	Upon information and belief, Burngarner has possession of this device	This device was potentially used in April 2022 at the McGee Law Firm (125 Wappoo), and then taken to McCutchen during the summer of 2022 before being removed by Husband in August 2022. Husband stored the device unconnected in a box in his office. Upon information and belief, the device was removed from the McGee Law Firm by Wife in August 2022 and placed at McCutchen House. Husband has not used or accessed this device since it was removed from McCutchen House in the summer of 2022.
16	6 Port USB Tower	Unknown	Amazon - ZD Lopqmz	...7811	1/30/2022	No	TuyaSmart	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	To Husband's best recollection, this device was never used at McCutchen House. If at all, it would have been in April 2022, most likely, and was then removed the same month.
17	SCS Outlet (Audio)	WF-113D	SCS Enterprises	2536	1/31/2022	Yes	iOT Living	Unknown. Husband disposed of this device in May, June, or August 2022. Husband cannot be sure, but two of the three SCS Outlet devices were destroyed by an electrical surge and thrown away. The third was removed and thrown away in roughly August 2022.	To Husband's best recollection, these three SCS Outlet devices were opened at McCutchen House. Although one was used in McCutchen House beginning in approximately February 2022, the two remaining were used in the Loggia at Eddy Farm. Those two were destroyed by contractors due to water intrusion at the same time as the TV in the Loggia around May or June 2022.
18	SCS Outlet (Audio)	WF-113S	SCS Enterprises	2628	4/25/2022	Yes	iOT Living	Unknown. Husband disposed of this device in May, June, or August 2022. Husband cannot be sure, but two of the three SCS Outlet devices were destroyed by an electrical surge and thrown away. The third was removed and thrown away in roughly August 2022.	To Husband's best recollection, these three SCS Outlet devices were opened at McCutchen House. Although one was used in McCutchen House beginning in approximately February 2022, the two remaining were used in the Loggia at Eddy Farm. Those two were destroyed by contractors due to water intrusion at the same time as the TV in the Loggia around May or June 2022.
19	SCS Outlet (Audio)	WF-113D	SCS Enterprises	2628	4/25/2022	Yes	iOT Living	Unknown. Husband disposed of this device in May, June, or August 2022. Husband cannot be sure, but two of the three SCS Outlet devices were destroyed by an electrical surge and thrown away. The third was removed and thrown away in roughly August 2022.	To Husband's best recollection, these three SCS Outlet devices were opened at McCutchen House. Although one was used in McCutchen House beginning in approximately February 2022, the two remaining were used in the Loggia at Eddy Farm. Those two were destroyed by contractors due to water intrusion at the same time as the TV in the Loggia around May or June 2022.
20	Palm Vid Air Cleaner	PVAIRCLEAN-WIFI	Amazon	...2653	2/25/2022	No	TuyaSmart	Unknown	Upon information and belief, Wife used this device when she smoked marijuana at the McGee Law Firm (125 Wappoo). It was last seen when the law firm moved.

Chart of Devices
McGee v. McGee - No. 2022-DR-10-3072

No.	Device Name	Model Number	Vendor	Order Number	Purchase Date	Audio Capability	Software or Application	Current Location	Notes
21	Soundbar	BB4KWIFISOUNDBAR-01	Deluxe CCTV	33736	4/25/2022	Yes	Unknown	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	New in the box. Purchased for Loggia at Eddy Farm, but never installed.
22	SCS Outlet (Audio)	WF-113D	SCS Enterprises	2747	7/26/2022	Yes	iOT Living	Unknown	Husband purchased these two devices to replace the devices in the Loggia that were destroyed and never used them at McCutchen House. They were disposed of in August 2022.
23	SCS Outlet (Audio)	WF-113	SCS Enterprises	2747	7/26/2022	Yes	iOT Living	Unknown	Husband purchased these two devices to replace the devices in the Loggia that were destroyed and never used them at McCutchen House. They were disposed of in August 2022.
24	OUMEIOU Power Bank	OU-001	Amazon - OULJK Store	... 0231	12/20/2020	No	None	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	This device was only located at Eddie Farm. It was used with Wife's knowledge and consent to catch the contractor believed to be going through their belongings.
25	Divine Eagle USB	MEE007	Amazon - Divine Eagle Store	...0231	12/20/2020	No	None	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	This device was only located at Eddie Farm. It was used with Wife's knowledge and consent to catch the contractor believed to be going through their belongings.
26	OUMEIOU Power Bank	OU-001	Amazon - OULJK Store	...4650	12/28/2020	No	None	Ready to produce, but objection to being outside the scope of the Homeland Security Act.	This device was only located at Eddie Farm. It was used with Wife's knowledge and consent to catch the contractor believed to be going through their belongings.

Date	Notes
2/7/22 (9:40 am)	Work call via MS Teams
2/7/22 (12-5 pm)	Work call via MS Teams
2/16/22 (2pm)	Work call via MS Teams
2/24/22 (2pm?)	Work call via MS Teams
2/27/22	
4/1/22 (12:00 pm)	Work call via MS Teams
4/5/22 (10:15 am)	Phone call with mortgage broker
4/8/22 (10:12 am)	Work call via MS Teams
4/12/22 (9:30 am – 4pm)	Work call via MS Teams
9/4/2022 (3:00 am…)	Dan
9/22/22 (1:40 pm)	On phone with a friend
9/26/22 (8:45 am)	
9/26/22 (3:03 pm)	
9/26/22 (8:34 pm)	Phone call w/ Brittney (64 min)
9/27/22 (10:12 am)	
9/27/22 (10:37 am)	
9/27/22 (10:53am)	
9/27/22 (10:12 am)	
9/27/22 (10:37 am)	
9/27/22 (10:53am)	Call with attorney?
9/27/22 (12:24 pm)	Phone call w/ Emily (59 min)
9/28/22 (8:08 am)	
9/30/22 (8:00 pm-ish)	Dan at my house
10/1/22	Dan at my house

APPENDIX A.

Steven M. Abrams, J.D., M.S.
Curriculum Vitae

Steven M. Abrams, J.D., M.S.
Attorney, Digital Forensics Examiner and Instructor
1154 Holly Bend Drive
Mount Pleasant, SC 29466
843-216-1100
Steve@AbramsForensics.com

Curriculum Vitae

My key practice areas are Electronic Privacy, Digital Forensics and e-Discovery, and Computer Law.

Education

2023 -Magnet Forensics, AXIOM Cyber training, Webinar, August 2023
2023 -DataPilot, DataPilot 10 Training Class, live online, May 19, 2023

2021 -ADF Mobile Device Investigator Training, live 1 on 1 online, December 28, 2021

2016 -Techno Security 2016, Computer Forensics Training Seminar, Myrtle Beach, SC, June 5-8, 2016

2014 -Georgia Bureau of Investigations, Internet Evidence Finder Forensics Training, Decatur, Georgia, February 2014

2013 -Techno Security 2013, Computer Forensics Training Seminar, Myrtle Beach, SC, June 2-5, 2013

2012 -Techno Security 2012, Computer Forensics Training Seminar, Myrtle Beach, SC, June 3-6, 2012

2011 -November 9-12: EnCase 7 Training, Salt Lake City, UT
-November 6 – 9: Paraben Forensics Innovations Conference, Park City, UT
- South Carolina Assoc. of Legal Investigators (SCALI) Annual Training Seminar, May 2011
- April 7, 2011: SC Electronic Crime Task Force Quarterly Meeting and Training

2010 -Techno Security 2010, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2010

2009 - Cellebrite Mobile Device Forensics Certification (CCMDE), SEMAR, Mexico City, Mexico
-SCALI Annual Training Seminar, May 2009

2008 - South Carolina Basic Constable Training, Tri-County Technical College / SC Criminal Justice Academy, October – November 2008
- Commissioned as a South Carolina State Constable (LEO) on November 20, 2008.
- Techno Security 2008, Computer Forensics Training Seminar, Myrtle Beach, SC, June
2007 - Charleston School of Law, Charleston, SC, Juris Doctor (J.D. - Magna Cum Laude)

- GMU2007 Computer Forensics Symposium, Regional Computer Forensic Group

of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2007 (40 CEU HTCIA)
- Techno Security 2007, Computer Forensics Training Seminar, Myrtle Beach, SC, June

2006 - University of Aberdeen, School of Law, Kings College, Old Aberdeen, Scotland in collaboration with the University of Baltimore Law School Summer Law Program in Comparative Criminal Procedure and UK Business Entities & Taxation
- Techno Security 2006, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2006

2005 - SCALI Annual Training Seminar, May 2005
- SCALI Fall Training Seminar, October 2005

2004 - Access Data Advanced Windows Forensics, June 23-25, 2004, New York City. (24 Credit Hours)
- SCALI Annual Training Seminar, May 2004 (10 CEU)

2003 - GMU2003 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, George Mason University, Fairfax, VA. Aug.2003, (40 CEU HTCIA)
- Techno Security 2003, Computer Forensics and Security Conference (24 CEU)
- SCALI Annual Training Seminar & PI Training Seminar (16 CEU SLED)

2002 - SCALI Annual & Fall Training Seminars (16 CEU SLED)
- GMU2002 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2002, (40 CEU HTCIA)
- Access Data Computer Forensic Boot Camp, North Carolina Justice Academy, Edneyville, NC (24 CEU)

1992-1994 Microsoft Internet Developer Workshops NY, NY

1992-1993 Novell NetWare CNE Training, IBM Skills Discovery, Jericho NY

1984-1985 Microcomputer and Electronics Engineering, Hofstra University, Hempstead NY

1982-1983 Ph.D. Studies, Faculty Fellowship, Columbia University, Graduate School of Arts & Sciences

1981-1982 Columbia University, College of Physicians & Surgeons, Master of Science (M.S.)

1977-1981 Allegheny College, Meadville PA, Bachelor of Arts (B.A.) (Psychology - Computer Science)

Professional Licenses

Current

Licensed Attorney in South Carolina
Licensed Attorney and Counselor at Law in New York

Amateur Radio License

FCC Licensed General Class Radio Operator 2011 – current "KK4JNU"

Previous Licenses & Commissions
Licensed as a Private Investigator in South Carolina and New York (2002-2008), South Carolina State Constable (Sworn, 2008-2019).

Experience (Selected)

2016 – Present, Senior Attorney, Abrams Cyber Law & Forensics, LLC. Mount Pleasant, SC 29466. Concentration on Electronic Privacy and Defamation Cases, Electronic Discovery, and Digital Forensics.

2018 - Continuing Legal Education Instructor, ***Electronic Privacy Violations during Divorce: Legal and Ethical Guidelines for Family Law Practitioners,*** SC Bar, Columbia SC (February 21, 2018).

2016 – Continuing Legal Education Instructor, ***Smartphones as evidence for Personal Injury Cases***, NBI, Charleston SC (December 8, 2016).

2011 – 2016 Sole Practitioner Abrams Law Firm, PC. Mount Pleasant, SC 29466

2011 - Digital Forensics Instructor / Investigator, H-11 Digital Forensics / United States Embassy, Tirane, Albania.

2010 – Facilitator, Instructor, Annual In-Service Legals and CDV Training (SLED), Lowcountry Constable Association.

2009 – Speaker, South Carolina Association for Justice, Hilton Head, SC (August 6, 2009) Topic: Civil Discovery of E-mails after *O'Grady*

2009 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Faculty, SC Bar Convention – Family Law Section CLE

2008 – 2011 Shareholder, Abrams Millonzi Law Firm, P.C., Mount Pleasant, SC 29464

2007 - Presenter, "E-Discovery: Definition, FRCP Changes and Application CLE",NBI, Charlotte, NC, December 19, 2007

2007 - Digital Forensics Instructor/Investigator, H-11 Digital Forensics, United States Embassy, Mexico City, Mexico

2007 - Presenter, "Civil to Criminal: Collaborative Computer Forensics Investigations between PIs and Law Enforcement",GMU2007, August 9th & 10th, 2007

2007 - Presenter – "A South Carolina Lawyer's Roadmap to Navigating the New Federal E-Discovery Rules," The South Carolina Bar (CLE Division), April 13, 2007.

2006 - Presenter – "Typical Internet Sexual Activity and its Detection", Family Law CLE, The

South Carolina Bar (CLE Division), November 2006.

2006 - Instructor, "3-day Hands-on Computer Forensics Workshop", Trident Technical College, N. Charleston, SC, CLE accredited by The South Carolina Bar, January 2006.

2005 - Lecturer, "Computer Forensic Introduction", Trident Technical College, CLE accredited by South Carolina Bar and CEU / In-Service hours for PIs / LE by SLED.

2001 - Present Steve Abrams & Company, Ltd. (dba Abrams Computer Forensics)
Licensed Private Investigator, Computer Forensics Examiner

1998 - 2001 Steve Abrams & Company, Ltd. Mt. Pleasant, SC, President

1996 - Democratic National Committee, Instructor - Southeast and Northeast Regional Schools for Congressional Campaign Managers.

1995 – 1999 Direct Marketers of Charleston Mt Pleasant, SC, Partner
Co-owner of Political Database Marketing Company and full service political print shop.

1994 - 1995 The Software Studio Mt Pleasant, SC, Owner
Owner of software development company that developed database applications for the Newspaper publishing industry.

1992-1993 Town of North Hempstead, Manhasset, NY, Deputy Commissioner of Finance

1986 - 1992 Digitron Telecommunications, Inc., Huntington, NY, Director of R&D

1984 - 1986 Computer Associates International., Islandia, NY, Senior Systems Programmer

1983 Contel Information Systems Division. Great Neck NY, Software Engineer
(Developed the first Network Forensics Applications for the DoD

Recent Publications

Steven M. Abrams, Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age, 75 N.Y. St. B. Assn. J. 8, 15 (Feb. 2003).

Steven M. Abrams, Knowledge of Computer Forensics, Essential for 21st Century Private Investigators, 16 PI Mag. 46, 59 (October 2003).

Professional Awards & Honors

2008 – Member, SLED Ad Hoc Committee on Computer Forensics

2007 – CALI Excellence for the Future Award, Aviation Law, Charleston School of Law, Fall 2006

– CALI Excellence for the Future Award, Interviewing, Counseling & Negotiation, Charleston School of Law, Fall 2006

– CALI Excellence for the Future Award, Insurance Law, Charleston School of Law, Fall 2006

_ Dean's List, Charleston School of Law, Fall 2006, Spring 2007.

2004 - "2004 SCALI Investigator of the Year"

2003 - Member, SLED Private Investigations Business Advisory Committee

Professional Associations

Member, Institute of Electrical and Electronics Engineers - IEEE
Member, Lowcountry Constables Association - LCA

Bar Association Memberships

Admitted to practice in **South Carolina, District of Columbia, and New York**.

Compensation

I receive $425 per hour, plus mileage, travel and lodging expenses, for all Computer Forensics services and for depositions and trial testimony.

Previous Expert Testimony

I have completed over 1250 computer forensics investigations; the overwhelming majority of cases were settled and did not require me to testify.

South Carolina cases in which I was qualified in court as an expert are:

Hillburn v. Hillburn, (2001-DR-08-2354);
Smith v. Smith, (2001-DR-22-212);
Natale v. Natale, (2003-DR-10-775)
Berda v. Berda, (2003-DR-10-1899);
Murphy v. Murphy (2004-DR-10-1510) and
Overstolz v. Fountain of Youth Wellness Centers LLC (2003-CP-10-000761).
Gitter v. Gitter (2008-DR-10-2865)
Ricigliano v. Ricigliano, (2009-DR-18-0102)
Edwards v Junevicus, (2010-DR-10-4736)
BTM Machinery Inc. v. Michael J. Finley *(2013-CP-10-4366)*
Cherry v Cherry (2014-DR-10-95)
Whitfield v. Schimpf and Sweetgrass Plastic Surgery, *LLC (Case No. 2017-CP-10-2758)*

I was qualified as a testifying expert on digital forensics in federal court in the South Carolina Federal District Court

UHLIG, LLC, V JOHN ADAM SHIRLEY, *(CIVIL ACTION NO.. 6:08-1208-HFF) GREENVILLE DIVISION*

UNITED STATES OF AMERICA v. BRANDON DANIELS *(CRIMINAL, 2021) CHARLESTON DIVISION*

I have also prepared expert's reports under Federal Rule 26(a)(2)(B) for the following federal civil suits filed in the United States District Court for the District of South Carolina:

Lumpkin v. Bennani, (Civil Action No. 2:03-2904-23), and
Miller v. American LaFrance Corp. (Civil Action No. 2:04-1668-23)
***Microsoft v.* BWC Products Inc.** (Civil Action No. 2:06-CV-2023-CWH)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)

And in the United States District Court for the Southern District of New York:
UNITED STATES OF AMERICA v. KEITH RANIERE (also known as "VANGUARD") and ALLISON MACK (Case 1:18-cr-00204-NGG-VMS)

I was appointed the Court's Expert in United States District Court, District of South Carolina, Rock Hill Division:

The Travelers Home and Marine Ins. Co. v. Pope, C/A No.: 0:10-cv-1688-JFA

I was qualified as a testifying computer forensics expert in North Carolina courts in: ***Hollins v. Lightfoot.***

In addition, I have been deposed in the following matters over the past ten years:

Thomas & Assoc. v. Christopher Humphreys *(Case No. 2018-CP-10-0455)*
Catherine Cope v. Wells Fargo Bank N.A., Century 21 Properties Plus, and Jim Bailey, individually; *(Case No.: 2018-CP-18-00112)*
Rick Gray v. Church Mutual *(2017)*
Calandra v. Calandra *(2004-DR-10-2675)*
McLernon v. McLernon *(2003-DR-10-3090)*
White v. Cassidy *(*2004-DR-08-256)
Khoury v. Noce (2006-CP-10-001830)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)
Beard v. Dunn & Dixon-Hughes et al, (Case No. 2010-CP-08-0776)
UHLIG, LLC, V JOHN ADAM SHIRLEY, *(CIVIL ACTION NO.6:08-1208-HFF)*
ALTMAN, ET AL. V. FIRST CITIZENS BANK AND TRUST COMPANY *(2012-CP-34-0124)*

Machine Transcript of audio track from CamDuck Video

9/22/2022 1:22:00PM to 1:23:40PM (excerpt)

Lindsay: We have to forgive them. You know? Like or meaning don't forgive them.

You know what I mean by that? Like, I can't ...

Friend: I have had trouble with the whole well, like you did, because I have, my husband carried on and he cheated on me, and then I got pregnant with [ ]. Well, and I found out about the cheating. Well, right after the miscarriage, well, I was, like, devastated with my miscarriage because I thought, like, God was punishing me, you know, I was never gonna be able to push through all this. So I really still struggle with, trusting him.

And then like that, like, there, I've told before. Again, I have, like, very sensitive, like, heart to heart conversation that's

[ ] have trust issues with him [ ] but because of some of the decisions that have been made since I have been together with him...

Lindsay: You don't have to itemize it

Friend: Right. I said, like, you have made decisions in our relationship that were not honest decisions that have affected me and that it is very hard for me to trust you.

Lindsay: Um... You know, I hope, you know I'm like not to someone who...

(Audio fades out and in)

You're still in my phone right now.

Maybe, like, this is what I'll say about Justin. It's not just about the adultery. It's that you fucking lie about everything in your law practice. Like, you're the most unethical person I've ever met. And so, yeah, it, like, translates across.

...

... (part 2)

9/22/2022 1:32:00PM to 1:33:51 PM (excerpt)

Friend: ... is a good alternate Easter, but, like...

Lindsay: I'm surprised [unintelligible] still goes up there. Meaning, like, yeah. Like, meaning he still has that loyalty bind of...

Friend: And he loves it, like, now he can't, I mean, his mom is the one of, like, [ ] siblings. So, yeah. A lot of aunts, like,

Joe and I went to his aunt's house that was closest to her. She was 45 minutes away one day, during the day.

Lindsay: Mhmm

Friend: ... just because it was something to do and her...

Lindsay: okay.

Friend: Her husband is, like, the Baker automotive of that area.

Lindsay: Mhmm.

Friend: They live in a freaking beautiful, beautiful neighborhood, beautiful home, like, gorgeous. Like, indoor jacuzzi...

Lindsay: Remind me...

Friend: [ ] in her basement, like, you know, like that house.

Lindsay: Remind me of a Katie Baker story after it.

Friend: Okay. And while we were there, like, I didn't

Lindsay: Yeah.

Friend: ... know. Like, can we just stay with you please, please?

Lindsay: Yeah. Oh...

....