LAW OFFICES OF
RICHARD G. WHITING
A PROFESSIONAL ASSOCIATION
1515 LADY STREET
POST OFFICE BOX 7877
COLUMBIA, SOUTH CAROLINA 29202

TELEPHONE (803) 256-9067
FACSIMILE (803) 256-0223
dick.whiting@whitinglawsc.com

RECEIVED
May 08 2024
SC Court of Appeals

May 7, 2024

VIA EMAIL AND US MAIL:
THE HONORABLE H. BRUCE WILLIAMS
Chief Judge of South Carolina Court of Appeals
South Carolina Court of Appeals
1220 Senate Street
Columbia, SC 29201

RE: McGee v. McGee
Civil Action No. 2023-001376

Dear Judge Williams :

By the Court of Appeals Orders filed December 5, 2023 its certification to the Charleston County Family Court was issued requiring the Family Court to supervise additional Discovery related to Petitioners Motion to Suppress certain communication pursuant to the South Carolina Homeland Security Act and to issue a report with proposed findings as to what, if any, of Respondent's actions constitution violations under the Homeland Security Act. On May 3, 2024, The Honorable Spiros S. Ferderigos issued his report to the Court of Appeals. One thing that was not forwarded on to the Court of Appeals was a 7th Affidavit by one of the Petitioners' experts, John Bumgarner. I have inquired of Judge Ferderigos if this was simply an error and had been advised by his Honor that he had intentionally left that affidavit out of his report believing it was not necessary for the proposed findings to be made. It is the opinion of Ms. McGee, the expert, Pete Currence and myself, that this 7th affidavit by Mr. Bumgarner is imperative to be included and reviewed by the Court of Appeals. I have attached a copy of this affidavit for your Honor's review.

I am uncertain how to supplement the lower court's report giving that this is not an Order. I am happy to file a Motion to Supplement the "Report" or any other Motion that the court deems necessary to get this matter included in the record for your review. I am also happy to provide additional argument as to why this affidavit is not only appropriate but critical to addressing whether or not an illegal interception took place.

CERTIFIED FAMILY COURT MEDIATOR

I would appreciate receiving a response from the Court as to how I am to proceed to get this urgently needed information included for consideration.

Thank you in advance for your time and consideration.

I am very truly yours

With highest and kindest regards,

Sincerely,

Richard G. Whiting

cc: The Honorable Spiros S. Ferderigos
sferderigosj@sccourts.org

Pete Currence
pete@mscmlaw.com

Jerry Theos
jerry@theoslaw.com

Matt Abee
matt.abee@nelsonmullins.com

Brittany Point
brittany@theoslaw.com

Elizabeth Stringer
liz@stringerlaw.us

Marie-Louise Ramsdale
ml@ramsdalelaw.com

RECEIVED
May 08 2024
SC Court of Appeals

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY
Family Court

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

Lindsay F. McGee Petitioner

v.

Justin McGee Respondent

SEVENTH SUPPLEMENTAL AFFIDAVIT OF JOHN BUMGARNER

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

Background

1. My name is John Bumgarner. I am a retired member of the US Armed Forces, where I specialized in intelligence and special operations. I have performed work for the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency and the United States Special Operations Command. My current fields of concentration are cybersecurity and network forensics. I have a Master Degree in Information Systems and one in Security Management. I have been a Certified Information Systems Security Professional (CISSP) for 24 years and a Systems Security Certified Practitioner (SSCP) for 22 years. I have assisted in the exam development for both of these internationally recognized cybersecurity certifications. I was one of the first GIAC Incident Handler (GCIH) certified worldwide. I have published dozens of articles on cybersecurity and cyberwar. And I have lectured on these topics at the Naval Postgraduate School, King's College London, Queen's University Belfast and other institutions. Some of my research in my fields of expertise have been used by multiple organizations, including the Atlantic Council, the Department of Defense, and the North Atlantic Treaty Organization (NATO). This research has also been used in hundreds of articles, books and studies that have been published. Additionally, I have consulted on various projects with the Federal Bureau of Investigation, the United States Secret Service and the Department of Homeland Security. I am currently based out of an office in Asheville, North Carolina. My full credentials are included in my CV which is appended to this affidavit.

2. On July 10, 2023, the law firm McDougall Self Currence McLeod headquartered in Columbia, South Carolina retained my consulting services to investigate alleged cyber intrusions into various accounts owned by their client Lindsay McGee. My role has now become that of a testifying expert.

3. My investigation into the alleged cyber intrusions and spying allegations required a detailed analysis of multiple pieces of technical data and non-technical information spanning back to January 2021. This current affidavit is in response to *Husband's Response to Wife's Proposed Findings of Fact* filed on April 05, 2024 in the Family Court Case No. 2022-DR-10-3072. This is my Seventh Supplemental Affidavit and my eighth affidavit overall since August 2023 for this case. Like many of my previous affidavits this one will cover much of the same documentary evidence and technical evidence that has been written about at length for the last 8 months. The Respondent's previous expert has not written a counter argument to the bulk of the evidence that has been discussed at nauseam across all my affidavits. The Respondent and his legal counsel continue to operate in the gray in many of their responses about the overwhelming amount of documentary evidence and technical evidence related to spy cameras that were placed in the Petitioner's private residence by the Respondent. Some of the evidence that we have attempted to obtain from the Respondent related to this case has been conveniently spoliated and is not available for analysis or interpretation. Even without this evidence the facts in this case are simple:

    a. The Respondent purchased over 2 dozen spy cameras between December 2020 and July 2022. (documentary evidence)

    b. The Respondent purchased at least 9 cameras with audio recording capabilities. (documentary evidence and technical evidence)

    c. The Respondent installed the software to remotely manage these cameras on his Apple iPhone XS Max. (documentary evidence)

    d. Thirteen spy cameras were flagged in the Petitioner's log files. (technical evidence)

    e. Two spy cameras (WF-113 and CamDuck) purchased by the Respondent were discovered in the Petitioner's residence. (physical evidence and documentary evidence)
    f. One (CamDuck) of these spy cameras recorded both audio and video in the Petitioner's master bedroom for approximately 8 months. (technical evidence)

g. CamDuck was connected to Petitioner's Wi-Fi network on May 15, 2022 by someone with the CIXICM application installed on a mobile device. The Respondent had this application installed on his Apple iPhone XS Max and was at the Petitioner's residence on May 15, 2022. (technical evidence)

h. Petitioner's Internet bandwidth shows major abnormalities for multiple months in 2022. The abnormalities are consistent with large amounts of data being transmitted out of her residence. Multiple spy cameras being remotely monitored would cause these bandwidth abnormalities. (technical evidence)

i. CamDuck recorded for approximately 8 months from mid February 2022 through October 3, 2022. The camera was never turned off in August 2022 and stored in a box unplugged as the Respondent claims. (technical evidence)

j. At least 6 spy cameras with the capability to record audio were once installed in the Petitioner's residence by the Respondent. (documentary evidence, physical evidence and technical evidence)

k. The Respondent spoliated at least 8 spy cameras with the capability to record audio. (documentary evidence and technical evidence)

Respondent's Lack of Technical Expert

4. The Respondent stated that he has not been able to retain an expert to verify the technical evidence in this case. (Husband's Response to Wife's Proposed Findings of Fact (hereinafter "Husband's Response") ¶ 10.3.3 p. 8 and ¶ 24.1 p. 13) This statement is false and misleading. The Respondent previously retained the services of Sean Leonard, who is a forensic expert with multiple certifications. Mr. Leonard wrote 2 affidavits related to Family Court Case No. 2022-DR-10-3072 for the Respondent. Mr. Leonard's first affidavit was submitted in June 2023, which was prior to my involvement in this case. His second affidavit was submitted in September 2023. His second affidavit was directly related to the Motion to Suppress Evidence in the Family Court Case No. 2022-DR-10-3072. Over the last 6 months the Respondent has had ample time to re-engage Mr. Leonard or another expert to refute the overwhelming amount of technical evidence that I have provided in my last six supplemental affidavits. During these six months, the Respondent has acted as his own expert and has attempted to refute the forensic evidence in this case without the expertise to do so. Additionally, the Respondent claims that he has not been afforded the opportunity to evaluate the facts or data that had been used in my affidavits. (Husband's Response ¶ II p. 28) This

statement is a fallacious argument. I have continually submitted multiple exhibits in my affidavits based on the data that I used in my analysis. The Respondent has had all this data at this disposal to evaluate with any expert of his choosing.

Respondent Questions the Validity of Log Evidence

5. The Respondent has questioned the validity and authenticity of the evidence related to the router logs obtained from the Petitioner's Arris BGW210-700 (DSL modem) within her residence. (Husband's Response ¶ 9.1 p. 5 and ¶ 9.3-4 p. 6) This statement is false and misleading, because the Respondent failed to mention his own expert's affidavit about the router logs. That affidavit was filed in September 2023. In that affidavit Mr. Leonard confirmed that the router logs were highly accurate as a method to identify devices that had been connected to Ms. McGee home network. (Leonard Aff. ¶ 22 p. 10.) Additionally, the Respondent had Daniel Walden, his step-father, submit an affidavit in September 2023, which confirmed that his two Apple devices (Daniels-IPad-2 and Dans-IPhone) had once connected to Petitioner's Wi-Fi network during one of his visits. (Walden Aff. ¶ 10 p. 2) The Respondent also confirmed that these 2 Apple devices that are listed in Petitioner's router logs belonged to his step-father. (McGee in Opposition to Petitioner's Amended Motion to Suppress (hereinafter "Husband in Opposition") ¶ 55 b-c, p. 10) The Respondent also confirmed that the device named "madisens-Air" listed in the Petitioner's router logs belonged to Manisen Lamp, who was a babysitter that the Respondent had previously hired to watch the children at the Petitioner's residence. (Husband in Opposition ¶ 55 a p. 10) The Respondent also confirmed that the device named "Bonnies-MBP" listed in the router logs belonged to another babysitter that stayed at the Petitioner's residence. (Husband in Opposition ¶ 55 d p. 10) The Respondent also confirmed that the device named "Charlies-iPad" listed in the router logs belonged to his oldest son. (Husband in Opposition ¶ 55 f p. 11) And finally, the Respondent confirmed that the devices named "Iphone-10-X" and "Justin's iPhone" listed in the Petitioner's router logs were his iPhones. (Husband in Opposition ¶ 55 g-h p. 11) The Respondent himself, his step-father Daniel Walden and the Respondent's expert, Sean Leonard have confirmed beyond a shadow of a doubt that the devices listed in the Petitioner's router logs were once connected to her Wi-Fi network. By confirming these devices the Respondent has shown that the router logs obtained from Petitioner's residence are valid from an evidentiary standpoint.

Respondent Questions the MAC Addresses within the Log Evidence

6. The Respondent cites that there is discrepancy between the 13 spy cameras mentioned in my Sixth Supplemental Affidavit filed in March 2024 and the 12 devices that I annotated in Exhibit B. (Husband's Response ¶ II A p. 31) Exhibit B was the device list obtained from the Petitioner's Arris BGW210-700 (DSL modem) on July 29, 2023. The Respondent is correct that only 12 devices in Exhibit B have been annotated. These 12 annotations are for the devices that either have device names (e.g., GF-PH130) linked to known spy cameras or use Wi-Fi components consistent with those embedded in spy cameras. The Respondent failed to mention Exhibit C, which was also attached to my Sixth Supplemental Affidavit. (Figure 1) Exhibit C was obtained from the AT&T Smart Home Manager service, which can be used to remotely configure the Arris BGW210-700 (DSL modem) within the Petitioner's residence. Exhibit C clearly lists the 13th device that was not listed in Exhibit B. I mentioned both these exhibits in my Sixth Supplemental Affidavit as shown below.

*"There is unquestionable technical evidence that shows at least 13 spy cameras were once connected to the Wi-Fi network in the Petitioner's private residence. (Exhibit B and Exhibit C)" (*Bumgarner 6th Suppl Aff. ¶ 4 p. 2)

Figure 1 - AT&T Smart Home Manager data

Date Collected: July 22, 2024

These devices were listed in the AT&T Smart Home Manager application used to remotely control the Wi-Fi network in Hayley McGee's House. Seven of the devices are cameras manufactured by SCS Enterprises. The other unknown devices have linked to vendors that also manufacture spy cameras.

0C:CF:89:22:5F:47	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
0C:CF:89:23:BE:4C	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
30:7B:C9:26:1C:9C	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:33:52:24	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:3C:30:18	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:6F:15:A0	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:32:E8:5F	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
0C:CF:89:50:51:F8	Shenzhen Dev.ce	Shenzhen Bilian Electronic Co Ltd	Unknown
0C:CF:89:A4:02:8A	Shenzhen Device	Shenzhen Bilian Electronic Co Ltd	CAMDUCK
0C:CF:89:B1:CB:93	Shenzhen Device	Shenzhen Bilian Electronic Co Ltd	Unknown
54:EF:33:45:D4:B0	Shenzhen Device	Shenzhen Bilian Electronic Co Ltd	Unknown
44:B2:95:75:B4:FE	SichuanA Device	Sichuan AI-Link Technology Co., Ltd.	Unknown
54:F1:5F:E6:9E:3E	SichuanA Dev.ce	Sichuan AI-Link Technology Co., Ltd.	Unknown

My initial affidavit was filed on August 30, 2023, which referenced these 13 spy cameras. Additionally, I have included the AT&T Smart Home Manager data as an Exhibit in multiple supplemental affidavits that I have submitted for the Family Court Case No. 2022-DR-10-3072. Neither the Respondent nor Matt Abee, his legal representative have raised this alleged discrepancy related to the number of spy

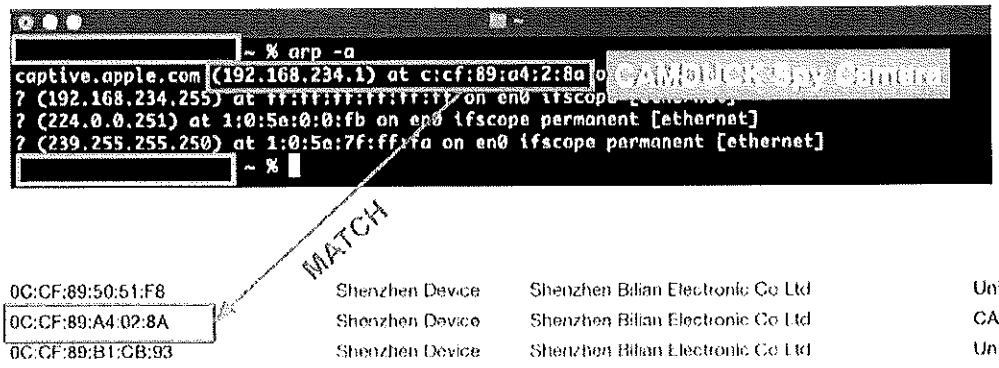
cameras prior to submitting the *Husband's Response to Wife's Proposed Findings of Fact* filed on April 05, 2024. In this filing the Respondent and his legal representation cherry picked the router log evidence to fit their narrative, which was clearly an attempt by them to befuddled the court by not mentioning the companion evidence that I have submitted multiple times to the court.

Respondent Questions the 13 Recording Devices in the Log Evidence

7. The Respondent cites that Petitioner failed to show that the "thirteen covert recording devices" shown in Figure 1 were capable of "recording audio, contemporaneously or otherwise." (Husband's Response ¶ 9 p. 5). Prior to November 01, 2023, the device with the MAC Address 0c:cf:89:a4:02:8a listed in Figure 1, was only identified as a device that used Wi-Fi components consistent with those embedded in spy cameras. On this date the Petitioner discovered an unknown spy camera in her master bedroom. During my investigation, I identified this device as a CAMDUCK-5U-BLACK on November 02, 2023. Documentary evidence later provided by the Respondent showed that he purchased the Camduck from Amazon on January 30, 2022. (Exhibit B) It is worth noting that I successfully identified an unknown covert recording device with the MAC Address 0c:cf:89:a4:02:8a in the AT&T Smart Home Manager application on July 22, 2023. (Figure 1) Three months later I proved beyond a shadow that this MAC Address was the one assigned to the CamDuck spy camera discovered in the Petitioner's master bedroom on November 01, 2023. (Figure 2) There is indisputable forensic evidence, which shows that the Camduck spy camera recorded video with embedded audio in the Petitioner's master bedroom for approximately 8 months beginning in mid February 2022 through October 3, 2022. (Bumgarner 5th Suppl Aff. - Exhibit D Exhibit E and Exhibit F and Bumgarner 6th Suppl Aff. - Exhibit E, Exhibit F and Exhibit G)

Figure 2 - Definitive match of CamDuck MAC address in the Petitioner's Wi-Fi log

MAC Address of CamDuck (post forensic image) - audio capable



Petitioner AT&T Wi-Fi log collected on 07.22.2023

8. The documentary evidence provided by the Respondent shows that he purchased nine WF-113 spy cameras manufactured by SCS Enterprises between July 2021 and July 2022. (Combined Device Purchase-McGee(HSA)_02011-2151) The Respondent purchased five WF-113 spy cameras directly from SCS Enterprises. (Exhibit C) The documentary evidence shows that these five WF-113 spy cameras all ***had audio recording capabilities.*** The other four WF-113 spy cameras were purchased from Amazon and ***had no audio recording capabilities***. (Exhibit D) The Respondent has confirmed that he only purchased four WF-113 cameras that did not have the capability to record audio. (Husband's Response ¶ 27 p. 13).

9. The default name for SCS Enterprises' spy cameras is GF-PH130. The AT&T Smart Home Manager records collected on July 22, 2023 lists seven unique devices with the name GF-PH130. (Figure 1) The Respondent claims that he used more than two of the four WF-113 spy cameras that ***did not have the capability to record audio*** in the Petitioner's residence. (Husband's Response ¶ 29 p. 14). The Respondent's claim is untrue and deceptive. The technical evidence collected in this case does not support the Respondent's claim. The technical evidence related to the GF-PH130 devices comes from multiple sources:

    a. AT&T Smart Home Manager application on July 22, 2023 (Figure 1)
    b. Arris BGW210-700 (DSL modem) device logs on July 29, 2023 (Exhibit A)
    c. First Revised Chart of Physical Devices and ID Markers - McGee(HSA)_002271A
    d. WF-113 spy camera discovered in Petitioner's residence on July 22, 2023

10. A SCS Enterprises' WF-113 spy camera was discovered in the Petitioner's residence on July 22, 2023. This device was one of the four WF-113 spy cameras that the Respondent purchased from Amazon that ***did not*** have the capability to record audio.

(Exhibit D) The device was relinquished to the Charleston County Sheriff's Office on August 02. 2023. The Respondent's *First Revised Chart of Physical Devices and ID Markers* lists two of the four WF-113 that he purchased from Amazon ***without audio recording capabilities.*** This chart and the camera discovered in the Petitioner's residence allowed us to positively identify three of the four WF-113 spy cameras that the Respondent purchased without audio recording capabilities. The MAC Addresses for the two WF-113 spy cameras listed in the Respondent's *First Revised Chart of Physical Devices and ID Markers* ***do not match*** any of the MAC addresses listed in either Figure 1 for devices with the name GF-PH130 or in the Arris BGW210-700 (DSL modem) logs collected on July 29, 2023. The Respondent's step-father Daniel Walden has confirmed that the logs were accurate by stating that he connected his Apple devices to the Petitioner's Wi-Fi network in June 2021. (Walden Aff. ¶ 10 p. 2) The June 2021 date is highly significant, because the Respondent ***did not*** purchase any of the SCS Enterprises' WF-113 spy cameras without audio recording capabilities until July 2021. Even the Respondent himself confirmed that the log files were accurate as of August 2021. (Husband in Opposition ¶ 55 h p. 11-12). There is one missing WF-113 spy camera ***without audio recording capabilities***. This missing spy camera is not listed in the Respondent's *First Revised Chart of Physical Devices and ID Markers.* Based on the evidence obtained from the AT&T Smart Home Manager we can speculate with a high degree of certainty that the missing WF-113 spy camera without audio recording capabilities is one of the seven identified with the name GF-PH130. (Figure 1) The Respondent claims that he installed more than two WF-113 spy cameras without audio recording capabilities on the Petitioner's Wi-Fi network after June 2021 is mendacious in nature. The evidence only supports that two of the four WF-113 spy cameras without audio recording capabilities were on the Petitioner's Wi-Fi network between July 2021 and July 2023.

11. Paragraph 10 showed that two of the four WF-113 SCS Enterprises spy cameras purchased by the Respondent ***without audio recording capabilities*** were connected to the Petitioner's Wi-Fi network between July 2021 and July 2023. The AT&T Smart Home Manager application records collected on July 22, 2023 lists five other spy cameras with the name GF-PH130, which is the default naming for cameras manufactured by SCS Enterprises. The documentary evidence provided by the Respondent shows that he purchased five WF-113 spy cameras manufactured by SCS Enterprises ***that had audio recording capabilities*** in 2022. (Exhibit C) Based on the preponderance of evidence we can confirm beyond a shadow of a doubt ***that the five WF-113 spy cameras with audio recording capabilities*** were installed on the Petitioner's Wi-Fi network between February 2022 and July 2023. The evidence that support this claim is (1) Respondent's documentary evidence, (2) the AT&T Smart Home Manager application records collected on on July 22, 2023, (3) the Respondent's *First*

Revised Chart of Physical Devices and ID Markers and (4) the SCS Enterprises WF-113 spy camera discovered in Petitioner's residence on July 22, 2023. The evidence clearly shows that the Respondent connected at least six spy cameras with the ***capability to record video with embedded audio*** on the Petitioner's Wi-Fi network between January 2022 and July 2023. It is important to note that the Respondent's ***failed to produce*** any of WF-113 spy cameras with ***audio recording capabilities.*** The Respondent's stories related to the spoliation of the five WF-113 spy cameras manufactured by SCS Enterprises ***that had audio recording capabilities*** has major inconsistencies. The Respondent has stated that three of these five cameras were unboxed at the Petitioner's sometime between the end of January 2022 and April 25, 2022. (First Revised Chart for Production - McGee(HSA)_00002A). The Respondent states that ***only one*** of these three spy cameras with ***audio recording capabilities*** was ever connected to the Petitioner's Wi-Fi network. (First Revised Chart for Production - McGee(HSA)_00002A). The Respondent also states that the two additional WF-113 spy cameras with ***audio recording capabilities*** that he purchased on July 26, 2022 were never connected to the Petitioner's Wi-Fi network. (First Revised Chart for Production - McGee(HSA)_00003A) The Respondent's supposition is that he immediately disposed of the latter spy cameras soon after the purchased them. (First Revised Chart for Production-McGee(HSA)_00003A) The Respondent's statements about not connecting the other four WF-113 spy cameras ***with audio recording capabilities*** to the Petitioner's Wi-Fi network is not supported by the evidence that I have submitted in multiple affidavits in this case. It is abundantly clear that the Respondent is being deceptive and misleading in his written statements to the court related to the WF-113 spy cameras ***with audio recording capabilities*** that were historically connected to the Petitioner's Wi-Fi network. Figure 1 above clearly shows that seven WF-113 spy cameras with the default name GF-PH130 were previously connected to the Petitioner's Wi-Fi network. Based on the ponderance of the evidence we can state with extreme certainty that the ***Respondent connected all five of the WF-113 spy cameras with audio recording capabilities*** to the Petitioner's Wi-Fi network between the end of January 2022 and prior to July 22, 2023.

Respondent and CIXICM Mobile Application

12. The Respondent has admitted to installing the CIXICM mobile application on his Apple iPhone XS Max on February 08, 2022. (Husband's Response ¶ 11 p. 8) In my Sixth Supplemental Affidavit, I discussed the functionality of the CIXICM mobile application. I also highlighted that the CIXICM application in the Apple App Store had been rebranded as CAMDUCK management application. (Bumgarner 6th Suppl Aff. ¶ 4 p. 2) The Respondent claims that the application that I discussed in my Sixth Supplemental Affidavit is not the CIXICM application. (Husband's Response ¶ 11.1 p. 9) Figure 3 is a

screenshot that I took in February 2024 and was included on page 5 of my Sixth Supplemental Affidavit. (Bumgarner 6th Suppl Aff. ¶ 12 p. 5) Figure 4 is a screenshot of the same application on the Apple App Store that I took on April 9, 2024. The only difference between these 2 screenshots is the application name on the first line. Based on these screenshots the Respondent's claim that the CIXICM application and CAMDUCK application are not the same is both misleading and mendacious. (Husband's Response ¶ 11.1 p. 9)

Figure 3 - CIXICM Application Apple App Store - February 2024

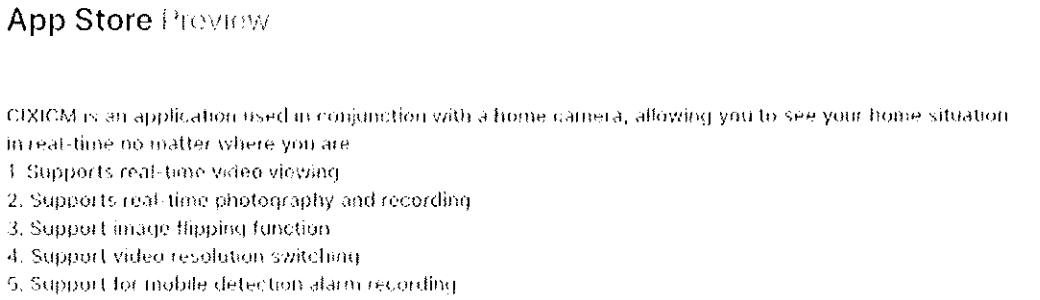
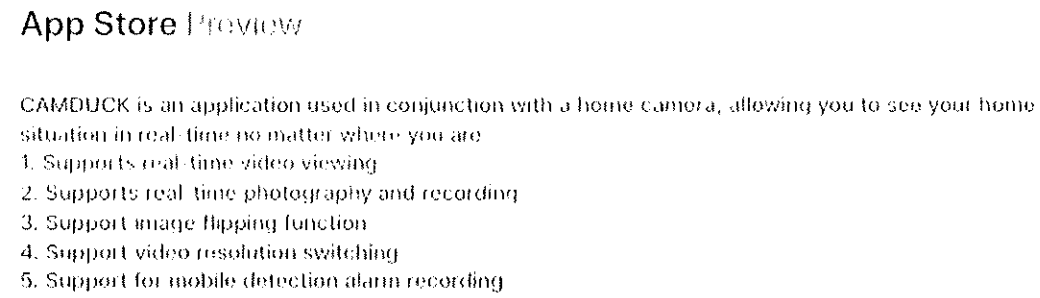


Figure 4 - CamDuck (rebranded) Application Apple App Store - April 2024



13. The Respondent has admitted to installing the CIXICM mobile application on his Apple iPhone XS Max on February 08, 2022. (McGee Aff. About Apple Application Records p. 2 ¶ 3) The CAMDUCK application (previously named CIXICM) on the Apple App Store has a release history, which starts in May 2021.[1] So based on this release history we know that the Respondent installed a version of the CAMDUCK application (previously named CIXICM) on his Apple iPhone XS Max. It is worth mentioning that the copyright for the CAMDUCK application on the Apple App Store is CIXICM. The Respondent or

[1] Release History - https://apps.apple.com/us/app/camduck/id1568241852

his legal counsel Matt Abee could have conducted a cursory search of the Apple App Store for details on the CIXICM mobile application and its basic name rebranding to CAMDUCK. Instead they decided to sow unwarranted doubt in their legal filings that the CIXICM application and CAMDUCK application were different even though they are the same. (Husband's Response ¶ 11.1 p. 9)

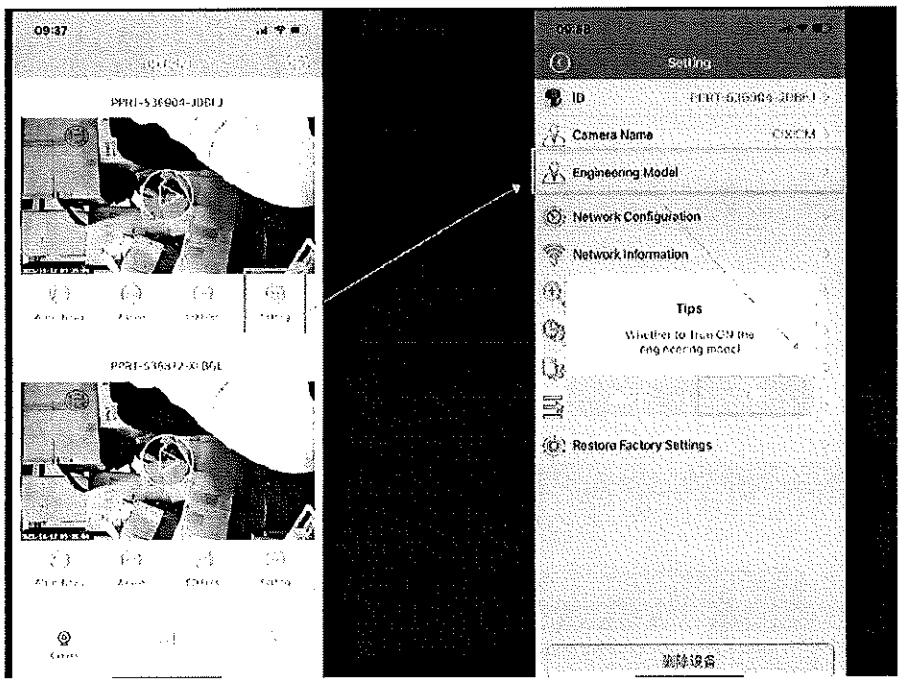
Respondent Questions that the CamDuck Recorded Audio

14. The Respondent has admitted that he purchased the CamDuck (LUOHE TY-BK/ CAMDUCK-5U-BLACK) spy camera on January 30, 2022. (Husband's Response ¶ 10 p. 6). The Respondent has admitted to taking the CamDuck spy camera to the Petitioner's residence in 2022. (First Revised Chart for Production-McGee(HSA)_00002A and Husband's Response ¶ 13 p. 9) This CamDuck was discovered in the Petitioner's master bedroom on November 01, 2023. The MAC address for the CamDuck was positively matched to a MAC address that I flagged on July 22, 2023 as belonging to an unknown spy camera. (Figure 1) The Respondent admitted to downloading the CIXICM mobile application, which is used to manage and control CamDuck spy cameras. (Husband's Response ¶ 11 p. 8) The Respondent did not deny ever using the CIXICM mobile application to manage the CamDuck (LUOHE TY-BK/CAMDUCK-5U-BLACK) spy camera discovered in the Petitioner's master bedroom on November 01, 2023.

15. In my Sixth Supplemental Affidavit I provided specific details on how the CIXICM mobile application would have been used to enable audio on the CamDuck spy camera that was discovered in the Petitioner's master bedroom on November 01, 2023. (Bumgarner 6th Suppl Aff. ¶ 8-22 p. 3-13) Within these details I showed a snippet, which is shown below from LUOHE (Amazon CamDuck reseller) that informed me how to enable the audio on the same model of CamDuck purchased by the Respondent. Figure 5 is the image that the vendor attached to their email.

"this is a picture of how to open the audio. You can turn on engineering model if sound is allowed in your state. Please don't tell the other one it has audio." (Bumgarner 6th Suppl Aff. ¶ 22 p. 13)

Figure 5 - LUOHE Directions for Enabling Audio on CamDuck using the CIXICM Application



16. The vendor's direction in Figure 5 allowed me to enable the internal microphone on the same model of CamDuck that was purchased by the Respondent from Amazon. The vendor disables the internal microphones of their cameras sold through Amazon, which allows them to be in compliance with Amazon's guidelines. In my Fifth Supplemental Affidavit I included Exhibit R, which was an email that LUOHE (Amazon CamDuck reseller) sent to McDougall Self Currence McLeod after they purchased the same model of CamDuck that the Respondent had purchased from Amazon. This email provided details on contacting LUOHE to enable sound on the camera they sold McDougall Self Currence McLeod from their Amazon store. The vendor made it crystal clear that the recording function on their cameras had to be manually enabled using the CIXICM mobile application. The CamDuck spy camera that was discovered in the Petitioner's master bedroom on November 01, 2023 was purchased by the Respondent on January 30, 2022. (Exhibit B) This spy camera had its internal microphone enabled, which allowed it to record audio in the Petitioner's master bedroom. The only individual that had the CIXICM mobile application installed on a mobile device and was in direct proximity to this camera was the Respondent. Based on the ponderance of evidence we can assert with extreme certainty that the Respondent is the only person that could have enabled the microphone. Any ludicrous claims made by the Respondent that he did not access the CamDuck spy camera that recorded audio for approximately 8 months in the Petitioner's master bedroom are preposterous.

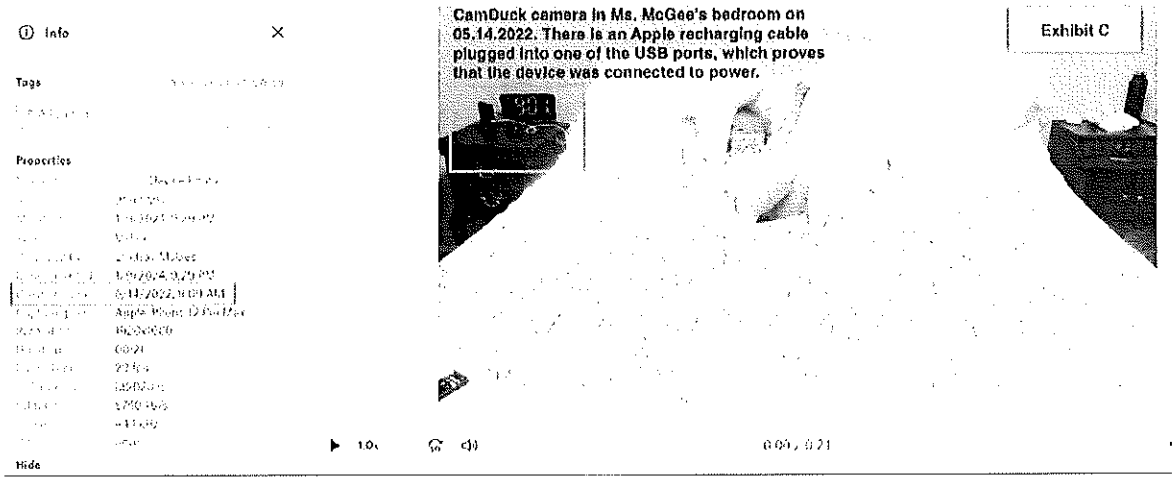
17. The technical evidence listed in Exhibit E, Exhibit F and Exhibit G that I submitted with my Fifth Supplemental Affidavit showed that the CamDuck recorded 20,452 files over approximately 8 months beginning in mid February 2022 through October 3, 2022. (Bumgarner 5th Suppl Aff. - Exhibit D Exhibit E and Exhibit F and Bumgarner 6th Suppl Aff. - Exhibit E, Exhibit F and Exhibit G) This evidence also showed that there were still 4962 undeleted files on the CamDuck's microSD Card. The Cellebrite Inspector and Magent Forensic applications, which were Exhibit F and Exhibit G in my Fifth Supplemental Affidavit showed that these files had embedded audio tracks. Based on the evidence any conjectures made by the Respondent that he never watched any videos on the CamDuck in Petitioner's master bedroom that contained audio are not supported by the physical and technical evidence in this case.

18. The Respondent also purchased 2 other CamDuck cameras on January 30, 2022. (Exhibit B) The Respondent has spoliated these devices. We purchased and tested the exact model of CamDuck camera that the Respondent purchased from Amazon. Based on my analysis we know beyond a shadow of a doubt that these additional CamDuck cameras also had ***embedded microphones to record audio.***

Respondent's Questions the Photograph of the CamDuck

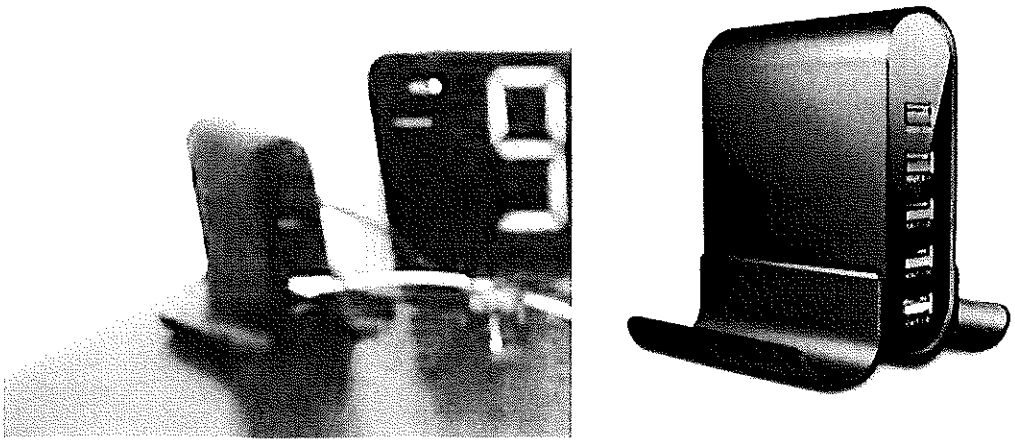
19. The Respondent claims that the photograph of the CamDuck that I submitted as Exhibit C in my Fifth Supplemental Affidavit could be another USB tower that the parties owned. (Husband's Response ¶ 15.1 p. 10) The photo in question is shown below in Figure 6 and was extracted from a video taken by the Petitioner's on May 14, 2022. In this still frame you can clearly see the CamDuck on the Petitioner's nightstand.

Figure 6 - CamDuck in Petitioner's master bedroom on 05.14.2022



20. Figure 7 is a comparison between the CamDuck on the Petitioner's nightstand and the CamDuck from the manufacturer's website. Both CamDucks in these images have the same distinct rounded top and winged base. Based on this photographic comparison it is clear that the Respondent's claim that this is just "another USB tower" is erroneous and deceptive. The Respondent could hire an expert that specializes in photogrammetry or computer vision to counter my analysis in these similarities of the devices in the images.

Figure 7 - CamDuck from Petitioner's video and CamDuck from vendor's website



Respondent's Denies Connecting CamDuck to Petitioner's Wi-Fi Network

21. The Respondent denies connecting the CamDuck spy camera discovered in the Petitioner's master bedroom to her private Wi-Fi network on May 15, 2022. (Husband's Response ¶ 16 p. 10) Based on the technical evidence the Respondent's claim is false. In my Fifth Supplemental Affidavit I provided multiple Exhibits that showed when the CamDuck spy camera was connected to the Petitioner's Wi-Fi network. I also discussed this in my Third Supplemental Affidavit and attached Exhibit N, which is shown in Figure 8 below.

Figure 8 - Date CamDuck was connected to the Petitioner's Wi-Fi network.

Exhibit N

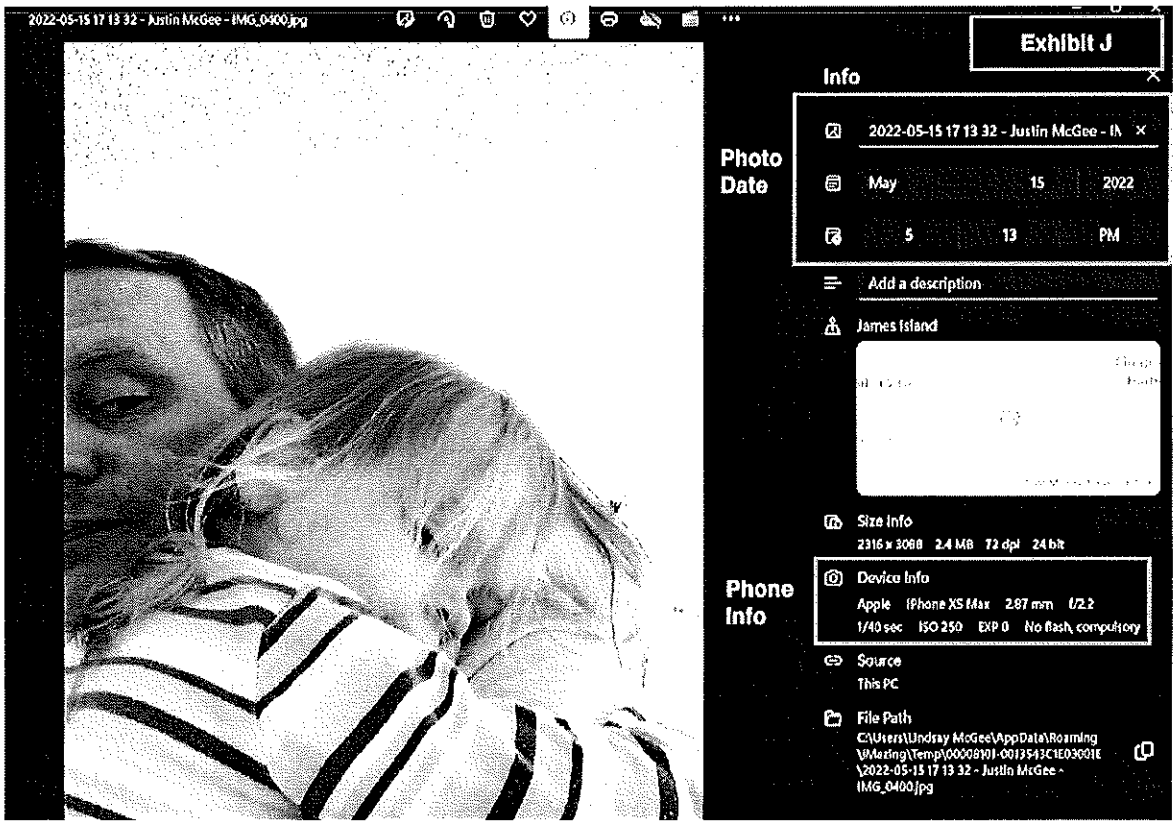
A snippet of the deleted files contained on the CAMDUCK spy camera

[illegible]	[illegible]	[illegible]	[illegible]
2020-03-30	3:11:09	351879680	/bin/vslocal/sd/record/20200329
[illegible]	[illegible]	[illegible]	[illegible]
2022-05-15	15:23:45	776929792	/bin/vslocal/sd/record/20220510/10
2022-05-15	16:10:28	740557312	/bin/vslocal/sd/record/20220510/11
2022-05-15	17:30:13	807567872	/bin/vslocal/sd/record/20220510/12
2022-05-15	19:17:04	733446656	/bin/vslocal/sd/record/20220510/13
2022-05-15	20:46:11	687849984	/bin/vslocal/sd/record/20220510/14
2022-05-15	21:54:30	692158976	/bin/vslocal/sd/record/20220510/15

22. Figure 8 above is a snippet from the CamDuck's Deletion Log, which is a hidden plaintext file that the spy camera writes data to. The complete Deletion Log was included in my Fifth Supplemental Affidavit as Exhibit G, Exhibit H and Exhibit I. Each one of these exhibits were annotated based on the evidence being discussed in that affidavit. The highlighted line above in red shows the date 2022-05-15. This is the date based on the evidence obtained from the CamDuck's internal files that the spy camera was connected to Petitioner's Wi-Fi network by someone using the CIXICM mobile application. Once the CamDuck was connected to Wi-Fi it was able to update its internal clock to the correct date stamp by querying the Internet. From 2022-05-15 forward the date stamps on the CamDuck were for the year 2022. Prior to 2022-05-15 the date stamps for the CamDuck were set to its internal default year of 2020. The date 2020-03-30 listed about 2022-05-15 is actually May 14, 2022. This was determined by counting the deleted file dates in reverse and correlating the first recording's date with the Respondent purchased date for this spy camera and the date that he installed the CIXICM mobile application on his Apple iPhone XS Max.

23. In my Fifth Supplemental Affidavit, I included Exhibit J, which was a photograph taken by the Respondent on May 15, 2022 at the Petitioner's residence. (Figure 9) The metadata within the Respondent's photograph shows that it was taken with an Apple iPhone XS Max. The Respondent's application purchase history indicates that the CIXICM software used to manage the CamDuck was installed on his Apple iPhone XS Max. (McGee Aff. About Apple Application Records p. 2 ¶ 3) Based on the vendor's documentation the only way to connect one of their spy cameras to a Wi-Fi network is by using their CIXICM management software. Based on the ponderance of the evidence we can infer with absolute reasonable certainty and beyond a reasonable doubt that the Respondent was the person that connected the CamDuck spy camera to the Petitioner's Wi-Fi network on May 15, 2022 using the CIXICM application installed on his Apple iPhone XS Max. The Respondent claims that we never provided any records showing that the CamDuck was connected to the Petitioner's Wi-Fi network on May 14, 2022. (Husband's Response ¶ 15 p. 10) This statement is erroneous, because at no time have I stated that the CamDuck was connected to the Petitioner's Wi-Fi network prior to May 15, 2022.

Figure 9 - Respondent's Apple iPhone XS Max at Petitioner's residence on May 15, 2022

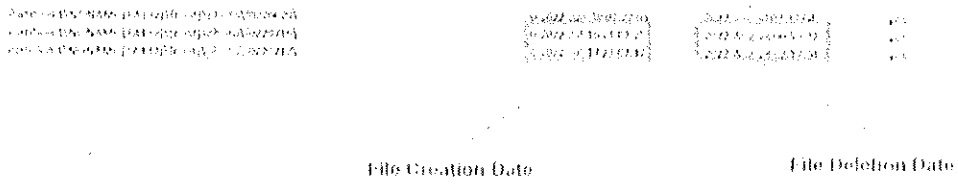


Respondent's Denies Remotely Managing CamDuck

24. The Respondent denies that he remotely accessed the CamDuck in the Petitioner's residence. (Husband's Response ¶ 21.2 p. 10) The Respondent's statement is fallacious and mendacious. There are several pieces of technical evidence that indicate that the CamDuck was being remotely managed by someone using the CIXICM application. The Respondent has confirmed that he had this application installed on his Apple iPhone XS Max. (McGee Aff. About Apple Application Records p. 2 ¶ 3)

25. The CamDuck maintains a hidden plaintext file that the device uses to write information about file deletion. Steve Abrams, another expert working on this case with me, used two industrial standard forensic tools (Cellebrite and Magent) to extract various records and videos from the CamDuck's microSD card. Figure 10 below is a snippet from the data that was extracted and analyzed from the CamDuck's microSD card. Figure 10 shows that 2 video files created in July 2022 were remotely deleted on August 27, 2022 (the date stamps below are in Coordinated Universal Time, which is +5 to Eastern Standard Time). During these deletions the CamDuck recorded a video that shows the Petitioner getting dressed. (Abrams 3rd Supp. Aff. ¶ 8; p. 3) And at no time did she have a device in her hands that would allow her to delete these recordings. (Abrams 3rd Supp. Aff. ¶ 8; p. 3) We know that the Respondent had the children for the weekend, so we can speculate that he was monitoring the CamDuck remotely since the Petitioner was alone for the weekend.

Figure 10 - CamDuck files being deleted remotely

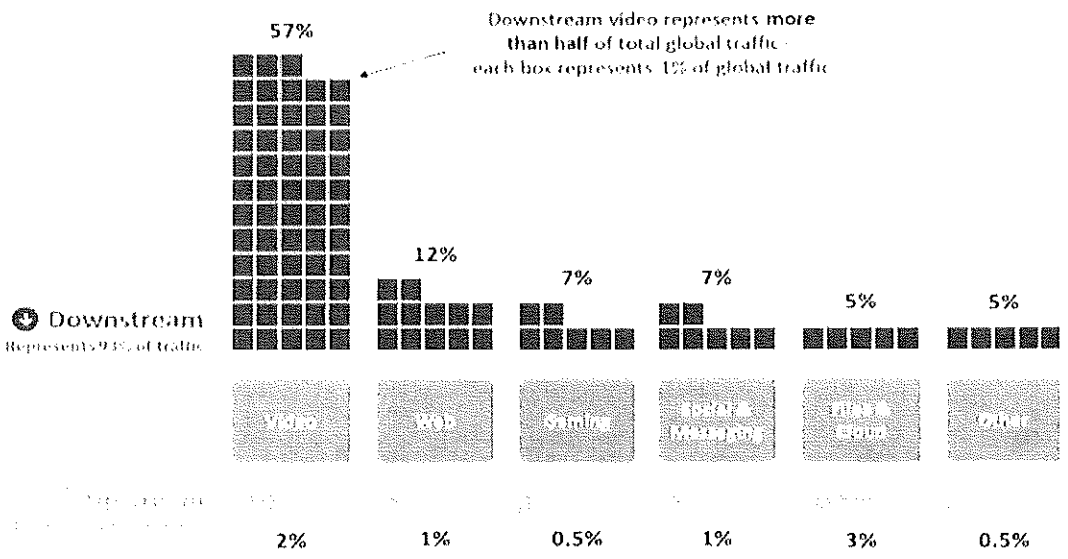


26. During this investigation, I pulled the Petitioner's bandwidth utilization logs from AT&T. These logs showed some anomalies related to the amount of data being transmitted out of her network. This type of outbound data is commonly called upstream bandwidth. A study was published in 2021 that showed that most households used more downstream bandwidth than upstream bandwidth.[2] The bulk of downstream bandwidth is largely used for video streaming services, such as Netflix or Disney. During 2022 the

[2] 2021 Bandwidth study - https://www.ncta.com/whats-new/new-study-examines-internet-traffic-patterns-and-bandwidth-requirements

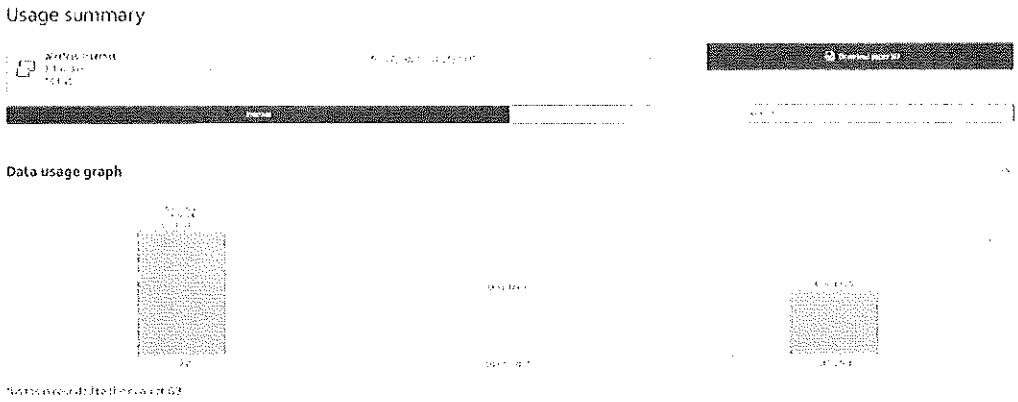
Petitioner was using Netflix, Disney and occasionally Amazon Prime video. The study indicated that over half of the global consumption of bandwidth is linked to video streaming services. Figure 11 below shows the types of services and their normal bandwidth utilization metrics. The metrics displayed in Figure 11 clearly show that downstream bandwidth is much higher than upstream bandwidth globally. These metrics are a strong indicator that the upstream bandwidth anomalies for the Petitioner's internet service are highly atypical for a standard household.

Figure 11 - Global Bandwidth Utilization Metrics



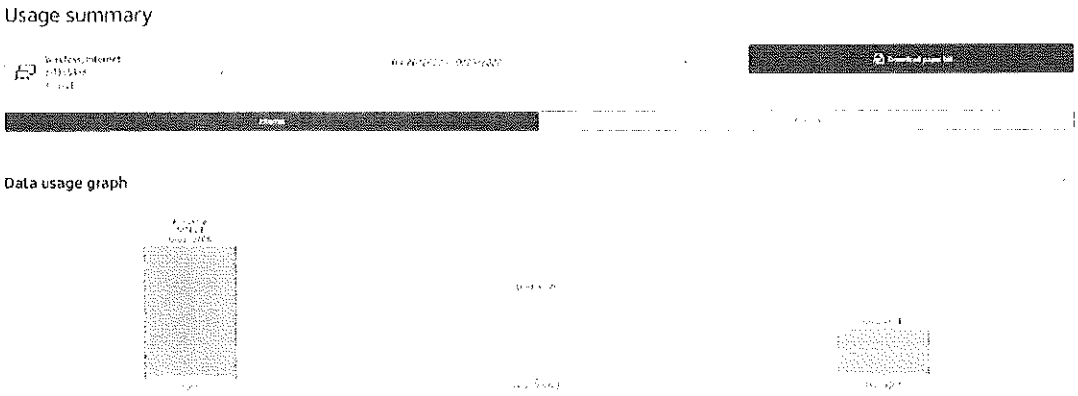
27. This study highlights that the service YouTube Live requires more upstream bandwidth than downstream bandwidth, because the service is streaming live video content out of the network. Spy cameras also stream live video content and recorded video content. The 13 spy cameras that I flagged in the Petitioner's Smart Home Manager Application had the capability to stream live video content and recorded video content to the Respondent's Apple iPhone XS Max, which had multiple camera management applications installed. Figure 12 below shows that the upstream bandwidth was greater than the upstream bandwidth in the Petitioner's home between August 26, 2022 and September 25, 2022. During this period of time we know that at least 2 spy cameras purchased by the Respondent were recording video and one of these was also recording audio. These cameras are currently in physical evidence.

Figure 12 - Petitioner AT&T Bandwidth Utilization for 08.26.2022 to 09.25.2022



28. Figure 13 shows the bandwidth utilization for the period of September 26, 2022 to October 25, 2022. The upstream bandwidth for this period was 58 percent of total bandwidth used at the Petitioner's residence. This is again a strong indication that spy cameras on the Petitioner's Wi-Fi network were being remotely monitored by someone external to the residence. There was a dramatic reduction in the upstream bandwidth utilization for the periods of October 26, 2022 to November 25, 2022, November 26, 2022 to December 25, 2022 and December 26, 2022 to January 25, 2023. Respectively the upstream bandwidth for these periods was 21 percent, 8 percent and 7 percent of the total bandwidth used by the Petitioner. The major reductions in upstream bandwidth between November 26, 2022 and January 25, 2023 are a strong indicator that the spy cameras in the Petitioner's residence were not able to communicate with her Wi-Fi network. These sharp declines in upstream bandwidth utilization are consistent with the Petitioner changing her Wi-Fi password in November 2022. (McGee Aff. ¶ 72; Ex. Q to McGee Aff.) After this password change the spy cameras installed in her residence by the Respondent could no longer be remotely monitored by the Respondent.

Figure 13 - Petitioner AT&T Bandwidth Utilization for 09.26.2022 to 10.25.2022



Respondent's Allegations related to Investigation

29. The Respondent makes some type of claim related to "allegations about the weather station or alarm clock that her experts were positive contained cameras." (Husband's Response ¶ II A p. 31) He continues these allegations about a RCA Alarm Clock and "black power adapter." (Husband's Response ¶ II A p. 31) The Respondent's argument is hard to follow and his logic is befuddling due to him leaving specific details. These unsupported allegations were another attempt by the Respondent to sprinkle doubt onto my findings and the overwhelming evidence in the case against him. Originally, we requested to inspect the weather station embedded with a spy camera that the Respondent purchased. After we obtained the MAC Address for the device in the Respondent's *First Revised Chart of Physical Devices and ID Markers* we abandoned our request, because the technical evidence indicated that this spy camera had never been connected to the Petitioner's Wi-Fi network. In February 2024, I received a RCA Alarm Clock and "black power adapter" from Nelson Mullins. The RCA Alarm Clock was purchased by the Respondent and provided to me by Nelson Mullins for inspection. I received this RCA Alarm Clock after Nelson Mullins inspected it. My inspection was to determine if the device had any type of management channel, through either Wi-Fi, Bluetooth, Infrared or Audio beacon. My investigation determined that the RCA Alarm Clock did not have the capability to be remotely controlled. And after disassembling the device I determined it had no internal microphone. The "black power adapter" was also sent to me by Nelson Mullins for inspection to determine if it had any type of management channel. Additionally, the Respondent's *First Revised Chart of Physical Devices and ID Markers* prepared by Nelson Mullins never mentioned if the MEE007 device listed on line 7 had a microSD card. Nelson Mullins only listed the device as a "power adapter". After receiving the device, I quickly determined that it

could not be remotely managed. After cross-referencing the device model number MEE007, I determined that the microSD card slot was hidden behind a sticker on the plug-side. I removed the sticker and discovered that the device's microSD card had been removed. It's unclear why Nelson Mullins never mentioned the empty microSD card slot in the *First Revised Chart of Physical Devices and ID Markers* that they prepared. Additionally, the Respondent failed to provide the actual purchased record for the MEE007 spy camera in the *Combined Device Purchase* document provided by Nelson Mullins. The Respondent only included the product page for the MEE007 in his *Combined Device Purchase* document. Without the actual purchase record we cannot determine if the Respondent purchased a microSD card with the device or potentially purchased undisclosed cameras.

30. The Respondent questions my alleged inconsistency in the number of spy cameras on the Petitioner's Wi-Fi. (Husband's Response ¶ II A p. 31) The Respondent's inconsistency claim is inaccurate, because he intentionally did not mention all the evidence. My initial affidavit was filed in August 2023. In that affidavit I highlighted that at least 13 spy cameras had been connected to her Wi-Fi network. The evidence that I relied on were obtained from AT&T Smart Home Manager application on July 22, 2023 and Arris BGW210-700 (DSL modem) device logs on July 29, 2023. The combined total of spy cameras is 13, which is the number that I have continually stated in my affidavits.

<u>Respondent's Raised Concerns About RXAMYDE Screenshot</u>

31. The Respondent raised concerns that the screenshot of the RXAMYDE features is from a third-party source outside the United States. (Husband's Response ¶ II A p. 30) The Respondent purchased the RXAMYDE spy camera from Amazon on May 28, 2021. (Combined Device Purchase-McGee(HSA)_02074) The seller of this spy camera is a Chinese company based on the purchase receipt. The Respondent's *First Revised Chart for Production* states that he cannot produce this device for inspection. (First Revised Chart for Production-McGee(HSA)_00001A) Since the Respondent spoliated the RXAMYDE spy camera we cannot physically inspect the device or check its MAC address against the 13 known spy cameras that had connected to the Petitioner's Wi-Fi network. McDougall Self Currence McLeod attempted to acquire the RXAMYDE spy camera from the Amazon website in the United States. The device is currently only sold on the Amazon website in the United Kingdom, which is where the screenshot showing the devices features was obtained. Based on the camera's features described on the Amazon product page in the United Kingdom we postulate that the RXAMYDE spy camera was removed from Amazon in the United States for a policy violation. A subpoena to Amazon targeting the RXAMYDE spy camera and specific details related to it being removed from the site would allow us to determine the camera's features.

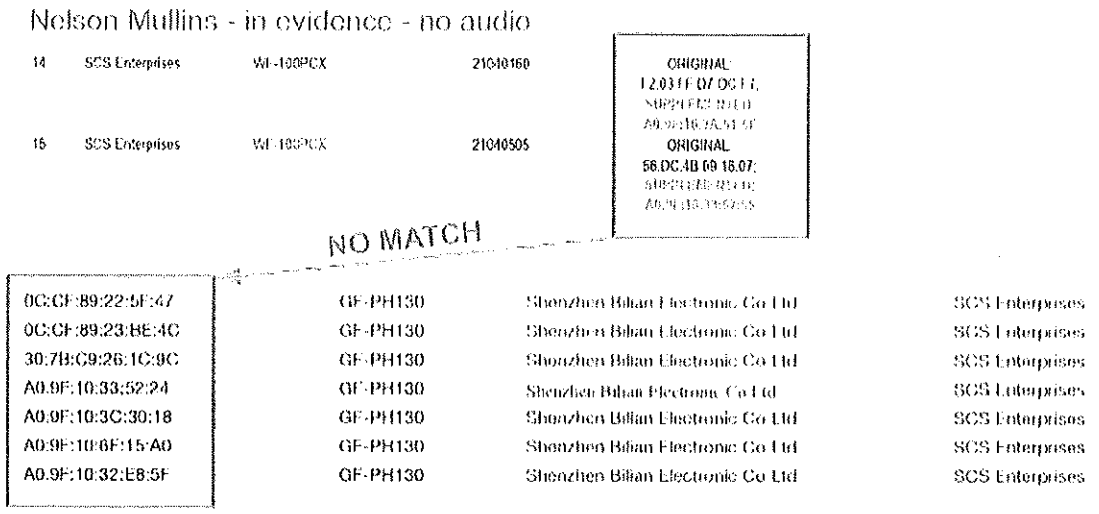
Based on the RXAMYDE features listed in the screenshot we can speculate that the device purchased by the Respondent had embedded audio recording capabilities. Currently, we strongly believe that the RXAMYDE spy camera that was spoliated by Respondent was one of the 13 spy cameras previously connected to the Petitioner's Wi-Fi network. There is indisputable documentary evidence, tangible physical evidence and strong technical evidence that shows that the Respondent still ***used at least 6 spy cameras with the capability to record audio i***n the Petitioner's residence. There is strong evidence that indicates that there were 2 additional CamDuck spy cameras, which were capable of recording audio in the Petitioner's residence. Unfortunately, the Respondent also spoliated these 2 CamDuck devices, which he purchased in January 2022 along with the CamDuck spy camera discovered in the Petitioner's master bedroom. These additional spoliated devices raised the number of spy cameras with audio recording capabilities to at least 9 devices. Based on the preponderance of evidence we know that the Respondent connected 6 of these devices to the Petitioner's Wi-Fi network. The technical evidence strongly indicates that the other 3 spoliated devices mentioned above were also connected to the Petitioner's Wi-Fi network by the Respondent.

Respondent's Spoliation of Spy Camera Evidence

32. The documentary evidence shows that the Respondent purchased 9 spy cameras that were manufactured by SCS Enterprises. The documentary evidence shows that 4 of these 9 spy cameras ***could not record audio.*** (Exhibit D) The documentary evidence also shows that 5 of these 9 spy cameras ***had the capability to record audio.*** (Exhibit C) The technical evidence shows that 7 of these 9 spy cameras were connected to the Petitioner's Wi-Fi network by the Respondent. (Figure 1) The Petitioner discovered 1 of the 4 cameras ***without the capability to record audio*** in her residence in July 2023. Nelson Mullins provided the MAC Addresses for 2 of the 4 cameras ***without the capability to record audio*** in the Respondent's *First Revised Chart for Production*. (First Revised Chart of Physical Devices and ID Markers - McGee(HSA)_002271A) Figure 14 shows beyond a shadow of a doubt that these 2 camera in evidence are not listed in the Petitioner's AT&T Smart Home Manager application logs that were collected on July 22, 2023. The last SCS Enterprises spy camera ***without the capability to record audio*** was spoliated by the Respondent. Based on the evidence we can make a logical conclusion that this spoliated camera is one of the 7 SCS Enterprises cameras shown in Figure 1. The technical evidence clearly shows that 2 of the 4 cameras w***ithout the capability to record audio*** were connected to the Petitioner's Wi-Fi network by the Respondent. Based on the preponderance of evidence, the other 5 SCS Enterprises cameras listed in Figure 1 are the 5 devices that ***had the capability to record audio,*** *which were* spoliated by the Respondent. There is no logical argument

that can be constructed to counter that these spoliated cameras were not connected to the Petitioner's Wi-Fi network in 2022 by the Respondent.

Figure 14 - MAC Addresses in Evidence do not Petitioner's Wi-Fi logs



Nelson Mullins - in evidence - no audio

14	SCS Enterprises	WI-100PCX	21040160	ORIGINAL
15	SCS Enterprises	WI-100PCX	21040505	ORIGINAL 56:0C:4B:09:16:07;

NO MATCH

0C:CF:89:22:5F:47	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
0C:CF:89:23:BE:4C	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
30:7B:C9:26:1C:9C	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:33:52:24	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:3C:30:18	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:6F:15:A0	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises
A0:9F:10:32:E8:5F	GF-PH130	Shenzhen Bilian Electronic Co Ltd	SCS Enterprises

Petitioner AT&T Wi-Fi log collected on 07.22.2023

33. The documentary evidence shows that the Respondent purchased 3 CamDuck cameras in January 2022 from Amazon. (Exhibit B) One of these cameras was discovered in the Petitioner's master bedroom on November 01, 2023. The MAC address for this camera positively matched an address that was on the log files that I collected from the Petitioner's Wi-Fi network on July 22, 2023. (Figure 2) There is indisputable forensic evidence, which shows that the Camduck spy camera ***recorded video with embedded audio*** in the Petitioner's master bedroom for approximately 8 months beginning in mid February 2022 through October 3, 2022. (Bumgarner 5th Suppl Aff. - Exhibit D Exhibit E and Exhibit F and Bumgarner 6th Suppl Aff. - Exhibit E, Exhibit F and Exhibit G) During this period the CamDuck recorded 20,452 files and 4962 of these files are still on the CamDuck's microSD Card. There is no logical argument that can be constructed to counter that this CamDuck was not connected to the Petitioner's Wi-Fi network in 2022 by the Respondent. As previously stated the Respondent purchased a total of 3 CamDuck cameras in January 2022. In my Fifth Supplemental Affidavit I outlined that these other 2 CamDuck cameras also ***had the capability to record audio.*** (Bumgarner 5th Suppl Aff. ¶ 31 p. 8-9) These additional CamDuck are conveniently missing from the Respondent's *First Revised Chart of Physical Devices and ID Markers and First Revised Chart for Production* that was provided by Nelson Mullins in February 2024. Their absence from these documents is a strong indicator that the Respondent spoliated these cameras, which ***had the***

capability to record audio. We assert that these spoliated devices were 2 of the 5 unidentified spy cameras that I flagged in the Petitioner's Wi-Fi logs on July 22, 2023.

34. The Respondent purchased a RXAMYDE spy camera from Amazon on May 28, 2021. (Combined Device Purchase-McGee(HSA)_02074). Strong circumstantial evidence indicates that the RXAMYDE spy camera ***had the capability to record audio.*** The Respondent has also spoliated this camera. We assert that this spoliated device was 1 of the 5 unidentified spy cameras that I flagged in the Petitioner's Wi-Fi logs on July 22, 2023.

Technical Evidence as of 04-18-2024

1. To date all the technical evidence obtained to develop this affidavit and all of my previous ones was obtained solely by McDougall Self Currence McLeod. To date Nelson Mullins, the law firm representing Justin McGee (Respondent), has provided limited data that has any forensic value.

Affidavit Status as of 04-18-2024

2. This Seventh Supplemental Affidavit was developed in response to *Husband's Response to Wife's Proposed Findings of Fact* filed on April 05, 2024 in the Family Court Case No. 2022-DR-10-3072. As additional questions need to be answered or as more data becomes available for analysis another supplemental affidavit will be created.

FURTHER THE AFFIANT SAYETH NOT!

John Bumgarner

SWORN TO AND SUBSCRIBED BEFORE ME THIS

18th, **DAY OF** April, **2024.**

NOTARY PUBLIC FOR NORTH CAROLINA

MY COMMISSION EXPIRES: 3 May 2025

Kirstin S Reimer Notary Public Buncombe County, North Carolina