

SEARCH WARRANT

G.L.c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS

SUFFOLK COUNTY

SUPERIOR DIVISION

NAME OF APPLICANT

Amy Erlandson-LaPointe

POSITION OF APPLICANT

Boston Police Sergeant Detective

SEARCH WARRANT DOCKET NUMBER

TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:

Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is **PROBABLE CAUSE** to believe that the property described below

- has been stolen, embezzled, or obtained by false pretenses
- is intended for use or has been used as a means of committing a crime.
- has been concealed to prevent a crime from being discovered.
- is unlawfully possessed or concealed for an unlawful purpose.
- is evidence of a crime or is evidence of criminal activity.
- other (specify)

YOU ARE THEREFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property:

1. Directs the Custodian of Records for **Apple** to search for, collect, and return to the affiant, if they are found, iCloud records as specified in this affidavit associated with Apple ID / email address and alternative identifying information (one or any combination of the following details):

FOR THE PERIOD OF 2/1/2015 TO 1/8/2020.

Apple ID / email address: [REDACTED]

IMEI (International Mobile Equipment Identity): 354390066243657

Telephone Number: [REDACTED]

Specified ICCID/SIM Card number: 8901260312754658271

Full name, DOB, address: Alvin Campbell DOB 08/02/1980 555 Worcester RD, Framingham, MA 01701 USA

- a. Device registration information, including but not limited to, customer information, names, addresses, email addresses, and telephone numbers, date of registration, purchase date and device type.
- b. Customer service records, including but not limited to, contacts that the customer has had with Apple customer service regarding a device or service, records of support interactions with the customer regarding a particular Apple device or service, and information regarding the device, warranty, and repair.
- c. iTunes information, including but not limited to, basic subscriber information such as names, physical addresses, email addresses, telephone numbers, information regarding iTunes purchase/download content, transactional records, and connections, update/re-download connections, and iTunes Match connections.

- d. iCloud data, including but not limited to:
 - i. Subscriber information, including but not limited to, basic subscriber information such as names, physical addresses, email addresses, telephone numbers, and information regarding iCloud feature connections.
 - ii. Mail logs, including but not limited to, records of incoming and outgoing communications such as times, dates, sender email addresses, and recipient email addresses.
 - iii. Email content, including but not limited to, iCloud email content in the customer's mailbox.
 - iv. Other iCloud content, including but not limited to, PhotoStream, documents, contacts, calendars, bookmarks, and iOS device backups.
 - e. Find My iPhone data, including but not limited to, Find My iPhone connection logs, and Find My iPhone transactional activity for requests to remotely lock or erase a device.
 - f. All records, data, and information, including but not limited to, text messages, Instant Messages, voicemails, documents, images/photographs, videos, data documenting the device location, and the date and time that any digital images were taken.
 - g. All records, data, and information, including but not limited to, credit card information, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information.
 - h. Your Affiant has probable cause that the data sought in this search warrant is being secured, kept, or used in violation of the laws of the Commonwealth of Massachusetts, at *Apple Inc., 1 Infinite Loop, Cupertino, CA 95014*, to wit: crimes of Rape, in violation of Massachusetts General Law, c. 265 § 22, Kidnapping, in violation of Massachusetts General Law c. 265 § 26 and Secret Sexual Surveillance, in violation of Massachusetts General Law c. 272 § 105.
 - i. I also seek the authority of this Court to take custody of the items contained in Section 2 (a) as described above, and to search those items for evidence relating to the crimes of Rape, in violation of Massachusetts General Law, c. 265 § 22, Kidnapping, in violation of Massachusetts General Law c. 265 § 26 and Secret Sexual Surveillance, in violation of Massachusetts General Law c. 272 § 105.
2. As stated above, this search warrant is requested under the authority of M.G.L. Ch. 276 § 1B. This statute, in part, provides courts in the Commonwealth with the authority to issue search warrants to electronic communication and remote computing service providers outside Massachusetts in accord with applicable provisions of the Federal Stored Communications Act (18 USC § 2703). Generally, however, the providers are not familiar with the facts of the investigation. Thus, the provider has no reasonable means to distinguish evidence of the crimes under investigation from any other records contained within the records of the account. Further, it would be improper to disclose the particular facts known to the affiant, to the provider. Therefore the provider should not be in the position of determining which records are, or are not, relevant or responsive to the demand or the investigation. Thus, I respectfully request that this Court order that the provider produce all records and items identified in Section 2(a) above in their entirety. Upon receipt, the items will be subject to further

review by law enforcement officers assigned to this investigation for the items detailed in Section 2(b). If any privileged information should be discovered during the course of the officers' search, the officers assigned will immediately halt their search and bring the matter to the authorizing judge's attention before taking further action. The authorizing judge will then be in a position to inform the assigned officers of their preferred protocol for further evidence review (i.e. special magistrate or taint team, etc.).

3. In the event that the services of an expert to complete the examination become necessary, a special request is made of this Court to authorize the use of civilian or law enforcement experts to complete this examination. In any event, the use of a civilian expert or experts in the execution of this warrant will be limited to the tasks for which the respective individual's expertise is necessary. At all times, any work performed by a civilian expert will be supervised by a sworn law enforcement forensic examiner, or the affiant.
4. Any and all information sought in this warrant shall be returned to Sgt. Det. Amy Erlandson-LaPointe via email at amy.erlandson@pd.boston.gov.

at: *Apple Inc., 1 Infinite Loop, Cupertino, CA 95014*

which is occupied by and/or in the possession of:
Apple Inc., 1 Infinite Loop, Cupertino, CA 95014

on the person or in the possession of :

You are are not also authorized to conduct the search at any time during the night.
You are are not also authorized to enter the premises without announcement.
You are are not also commanded to search any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.
YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the Superior Division of the Suffolk County Court Department.

DATE ISSUED <i>7/27/20 1:32 PM</i>	SIGNATURE OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK <input checked="" type="checkbox"/> <i>MDR RICCIUTTI, J</i>
FIRST OR ADMINISTRATIVE JUSTICE WITNESS: <i>J FABRICANT</i>	PRINTED NAME OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK <i>MD RICCIUTTI</i>

I, Sergeant Detective Amy Erlandson-LaPointe, being duly sworn, do depose and say under the pains and penalties of perjury that the following is true to the best of my knowledge:

PLACE TO BE SEARCHED:

I am seeking the issuance of a warrant, under authority of M.G.L. Ch. 276 § 1B authorizing the search of the Custodian of Records Office for the electronic service provider Apple, Inc. The official business address is detailed more particularly as:

Apple Inc.
Attention: Privacy and Law Enforcement Compliance
1 Infinite Loop
Cupertino, CA 95014

ITEMS TO BE SEARCHED FOR:

1. I respectfully seek the issuance of a warrant directing the Custodian of Records for **Apple** to search for, collect, and return to the affiant, if they are found, iCloud records as specified in this affidavit associated with Apple ID / email address and alternative identifying information (one or any combination of the following details):

Apple ID / email address: [REDACTED]

IMEI (International Mobile Equipment Identity): 354390066243657

Telephone Number: 617-380-9991

Specified ICCID/SIM Card number: 8901260312754658271

Full name, DOB, address: Alvin Campbell DOB 08/02/1980 555 Worcester RD,
Framingham, MA 01701 USA

- a. Device registration information, including but not limited to, customer information, names, addresses, email addresses, and telephone numbers, date of registration, purchase date and device type.
- b. Customer service records, including but not limited to, contacts that the customer has had with Apple customer service regarding a device or service, records of support

- interactions with the customer regarding a particular Apple device or service, and information regarding the device, warranty, and repair.
- c. iTunes information, including but not limited to, basic subscriber information such as names, physical addresses, email addresses, telephone numbers, information regarding iTunes purchase/download content, transactional records, and connections, update/re-download connections, and iTunes Match connections.
 - d. iCloud data, including but not limited to:
 - i. Subscriber information, including but not limited to, basic subscriber information such as names, physical addresses, email addresses, telephone numbers, and information regarding iCloud feature connections.
 - ii. Mail logs, including but not limited to, records of incoming and outgoing communications such as times, dates, sender email addresses, and recipient email addresses.
 - iii. Email content, including but not limited to, iCloud email content in the customer's mailbox.
 - iv. Other iCloud content, including but not limited to, PhotoStream, documents, contacts, calendars, bookmarks, and iOS device backups.
 - e. Find My iPhone data, including but not limited to, Find My iPhone connection logs, and Find My iPhone transactional activity for requests to remotely lock or erase a device.
 - f. All records, data, and information, including but not limited to, text messages, Instant Messages, voicemails, documents, images/photographs, videos, data documenting the device location, and the date and time that any digital images were taken.
 - g. All records, data, and information, including but not limited to, credit card information, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information.
 - h. Your Affiant has probable cause that the data sought in this search warrant is being secured, kept, or used in violation of the laws of the Commonwealth of Massachusetts, at *Apple Inc., 1 Infinite Loop, Cupertino, CA 95014*, to wit: crimes of Rape, in violation of Massachusetts General Law, c. 265 § 22, Kidnapping, in violation of Massachusetts General Law c. 265 § 26 and Secret Sexual Surveillance, in violation of Massachusetts General Law c. 272 § 105.
 - i. I also seek the authority of this Court to take custody of the items contained in Section 2 (a) as described above, and to search those items for evidence relating to the crimes of

Rape, in violation of Massachusetts General Law, c. 265 § 22, Kidnapping, in violation of Massachusetts General Law c. 265 § 26 and Secret Sexual Surveillance, in violation of Massachusetts General Law c. 272 § 105.

2. As stated above, this search warrant is requested under the authority of M.G.L. Ch. 276 § 1B. This statute, in part, provides courts in the Commonwealth with the authority to issue search warrants to electronic communication and remote computing service providers outside Massachusetts in accord with applicable provisions of the Federal Stored Communications Act (18 USC § 2703). Generally, however, the providers are not familiar with the facts of the investigation. Thus, the provider has no reasonable means to distinguish evidence of the crimes under investigation from any other records contained within the records of the account. Further, it would be improper to disclose the particular facts known to the affiant, to the provider. Therefore the provider should not be in the position of determining which records are, or are not, relevant or responsive to the demand or the investigation. Thus, I respectfully request that this Court order that the provider produce all records and items identified in Section 2(a) above in their entirety. Upon receipt, the items will be subject to further review by law enforcement officers assigned to this investigation for the items detailed in Section 2(b). If any privileged information should be discovered during the course of the officers' search, the officers assigned will immediately halt their search and bring the matter to the authorizing judge's attention before taking further action. The authorizing judge will then be in a position to inform the assigned officers of their preferred protocol for further evidence review (i.e. special magistrate or taint team, etc.).
3. In the event that the services of an expert to complete the examination become necessary, a special request is made of this Court to authorize the use of civilian or law enforcement experts to complete this examination. In any event, the use of a civilian expert or experts in the execution of this warrant will be limited to the tasks for which the respective individual's expertise is necessary. At all times, any work performed by a civilian expert will be supervised by a sworn law enforcement forensic examiner, or the affiant.

AFFIANTS KNOWLEDGE, TRAINING, EDUCATION AND EXPERIENCE:

1. I have been employed by the Boston Police Department for the last fourteen years. I joined the Boston Police Department in April of 2006. In March of 2020, I was promoted to the rank of Sergeant Detective. Since September 2019 I have been assigned to the Sexual Assault Unit as a detective supervisor. Prior to this assignment I worked at District C-11 as a patrol supervisor.
2. I spent the prior five years in the Bureau of Investigative Services as a detective where I worked at both the Family Justice Center and the Drug Control Unit (DCU). The majority of this time was

at the Family Justice Center (FJC) where I worked in both the Sexual Assault Unit and Crimes Against Children Unit. Before that I was assigned as a detective to the District E-18 Drug Control Unit covering areas of Hyde Park and Mattapan. I was also a member of the Firearms Discharge Investigation Team (FDIT).

3. In my assignment as an investigator, I have completed several training programs including but not limited to the 40 hour Commonwealth of Massachusetts Sexual Assault Investigator course in 2013, a 36 hour Internet Crimes Against Children Investigative Techniques Training Program and 15 hours of BitTorrent Investigations sponsored by ICAC and the US Department of Justice, NYPD's Special Victim's training, 18 hours of training by the Massachusetts Attorney General's Office at the 2014, 2015, and 2016 National Cyber Crime Conference, and eight hours of training in Cyber Crime Investigations, CIT Training, as well as trauma related trainings. I have also received certification in Mobile Phone Seizure. Throughout my career as a Police Officer and Detective and Sergeant, I have participated in numerous arrests, search warrants, and been the affiant on many search warrants.

STATEMENT OF FACTS:

1. This affidavit is submitted for the limited purpose of establishing probable cause for issuing a search warrant. This affidavit contains only that information sufficient to establish probable cause for the search warrant being sought and does not reflect the entirety of the information gathered during the investigation. Accordingly, I have not included each and every fact known to myself and other law enforcement officers involved with this investigation.
2. The victims' identities are known to this detective but will not be revealed in this affidavit pursuant to M.G.L. c.41, § 97D and c.265§ 24C. However, they will be referred to by the initials of those victims will be used when needed to describe facts of their specific cases.
3. On Sunday December 08, 2019 a report was filed by VR which explained that she had ordered a ride share from the Harp Bar located at 85 Causeway Street on December 06, 2019. VR explained that she was intoxicated and unaware of where the driver of the vehicle she had got into had taken her. VR explained when she woke up the next morning she was in a bed with a male who she believed was the driver that picked her up at the Harp. VR explained that she was somewhere in Rhode Island when she awoke. VR reported to the responding officer that she was unsure if she was raped or drugged so she had a sexual assault evidence collection kit conducted on 12/7/2019.
4. On Tuesday, December 11, 2019, Detective Sullivan and Detective Waldrip conducted an audio-recorded interview with the victim VR, during which time she reported that on the evening of

December 06, 2019, she was a work holiday party at the Harp located at 85 Causeway Street in the City of Boston.

5. The victim reported that she arrived at the Harp sometime around 9:00 or 9:30 PM. VR explained she was drinking vodka sodas and bud light during her time at the party. VR estimated that she drank about six or seven alcoholic beverages during her time at the party and stated that she had a lot to drink.
6. VR explained to detectives that she left the Harp around 11:50 PM. VR stated that she summoned a ride-share through her Uber app. VR explained she walked outside and saw a vehicle that did not match the description of the Uber that she had ordered. VR stated that the driver called her name and she then proceeded to get into the backseat of the vehicle. Through the course of this investigation detectives were made aware by witness Joe Piedmonte that he followed VR out of the Harp and observed her on her phone while approaching the SUV. The driver of that SUV appeared to be on his phone. VR went on to explain to detectives that it is about a five to ten-minute car ride from the Harp to her residence. VR advised detectives that she talked to her friend, ██████████ for a little over one minute about fifteen to twenty minutes after she got in the vehicle. Through looking at her phone history VR was able to inform detectives that ██████████ called her at 12:08 am on December 07, 2019. VR explained that ██████████ asked her if she had made it home to which VR told ██████████ that she was not home yet. It should be noted that VR does not have an independent memory of receiving a call from ██████████; she only knows that she did because she looked at her call log and saw the call and also spoke with ██████████ the next day about it.
7. VR explained to detectives that the next memory that she had was waking up naked in a bed. VR stated that she did have one memory from the middle of the night where she stated: "I just have like a vision of him on top of me, but it was a very quick memory." VR stated that she was in the bed with the same person who had picked her up from the Harp and that he too was naked in the bed when she awoke. VR explained that when she woke up, she was trying to find her keys. The person who was in the bed with VR got out of bed, got dressed and stated he wanted to get a breakfast sandwich before heading to work. After getting dressed VR and the male party went outside and got into his vehicle. VR reported that her keys were located in the back seat of the vehicle. VR explained the area where the house as being houses that were closely situated together, neutral in color. VR believed the house to be small and possibly a single-family. VR stated to detectives that the male parked the car on the street and the street appeared to be a main road.
8. VR described her assailant as bald, had a goatee, black male, "quite tall," medium complexion, no accent, "not thin, not very heavy but the heavier side." Black button-down, black pants black trench coat, long black coat.

9. The two parties then got into the vehicle with VR sitting in the front passenger's seat of the vehicle. The male operator drove the vehicle to a Dunkin Donuts located at 20 Ann and Hope Way, Cumberland Rhode Island. VR stated that the drive to get to the Dunkin Donuts took less than ten minutes. VR was able to tell detectives that they went through the drive-thru where the driver of the car ordered a breakfast sandwich and she got a cup of water. After leaving the Dunkin Donuts the driver of the vehicle drove to CVS located at 311 Broad Street, Cumberland Rhode Island. The driver of the vehicle explained to VR that he had to go to work and would drop her off at the CVS so she did not have to wait in the cold to order an Uber.
10. Once at the CVS, the driver of the vehicle left the area and VR ordered an Uber to her residence in Boston, MA. During the interview with detectives Detective Sullivan asked VR when she woke up in the morning and looked at the man she was in bed and drove with to Dunkin Donuts and CVS if that was the same man as the Uber ride, she ordered. VR was unsure if it was the same person and stated "It matches the description. I wasn't overly looking at him but the majority of the features check out." Detective Sullivan asked VR why she called the person "Stephen." VR explained that she got the name from the Uber app but never addressed him by name.
11. VR, during her interview, stated the last sexual intercourse she had happened on 10/31/2019. Boston Police Detectives did collect a Sexual Assault Evidence Collection Kit 55819 from MGH on 12/10/19 and delivered this to the Boston Police Crime Lab for review. Boston Police Crime Lab Serology forwarded their findings to the Boston Police Forensic Unit, DNA Section for further analysis. VR also disclosed that, while getting a Sexual Assault Evidence Collection Kit done, medical personnel observed a cut her breast, a cut that was very irritated on the nipple that was not there before the incident. This was corroborated by medical records.
12. Detectives reviewed camera footage from the area of the Harp which showed a large dark-colored SUV parked in front of the area of the Harp. The video appears to show that there is some interaction between the driver of the SUV and VR before she gets into the car. On video, an individual believed to be VR can be seen walking up to the vehicle, opening the door and getting into the vehicle. The vehicle is then observed on multiple cameras throughout the Boston Police network traveling on Causeway Street, across North Washington Street, and onto Commercial Street.
13. Detectives also recovered video from the 7-Eleven located at 91-99 Causeway Street that showed a black colored Chevrolet Suburban with a silver trailer hitch attached to it. Detectives also believed the vehicle to be around a 2013 or 2014 model due to the style of the headlight, grill, and bumper that was on the vehicle. The vehicle also had what appeared to be an object on the front dashboard of the vehicle in front of the steering wheel which appeared from the video to be a notebook or paper-like item.

14. Detective Morrissey responded to Cumberland, Rhode Island, where he recovered video from the Dunkin Donuts located on Ann and Hope Way as well as from an Auto Body shop located at Carr's Collision Center 396 Broad Street Cumberland, RI. At the Dunkin Donuts, the Suburban in question can be seen coming through the drive-thru at approximately 7:55 AM. The vehicle is then observed minutes later driving by Carr's Collision Center towards the CVS.
15. On Saturday, December 14, 2019, Detectives Waldrip and Sullivan responded to Cumberland Rhode Island and canvassed the area for cars similar to the one described in this document to no avail.
16. Detective Sullivan arranged for the victim's phone to be forensically examined by the Electronic Crimes Task Force. On January 2, 2020, Sergeant Amy Erlandson-LaPointe and Detective Waldrip met with Cambridge Detective Daniel Marshall who went over the results of the examination with them. Detectives were able to receive multiple data points (over one-hundred) showing the whereabouts of VR's travels between midnight and 9:55:59 AM on 12/7/19. Detectives were able to corroborate the GPS data points by looking at the point representing VR's time at Dunkin Donuts which coincided with the video recovered of her there.
17. Detectives observed one GPS data point stating the phone of VR was stationary in the area of Commercial Street in the North End from approximately 12:20am – after 1am. Her phone was turned off for a period of time and her phone began pinging again at various towers in downtown Boston at approximately 2:56:22 AM, 03:09:23 AM, 03:18:50 AM, 3:26 AM on 12/7/2019. Detectives conducted a query of a traffic camera (Genetec Camera 252 Clinton/North) near where the victim's phone was pinging. Detectives located video of a black suburban with no lights on driving down Clinton Street at approximately 3:26 AM. As the vehicle proceeds near the end of the camera frame, it is observed putting on its headlights.
18. Detectives also analyzed the activity on VR's phone. At 12:08 AM VR received a phone call that lasted seventy two seconds. The call originated from [REDACTED] After that phone call, two more messages at 12:26 AM are sent to the VR's phone. It is unknown if VR read those messages. At 7:43 AM is the next activity on the phone where VR actively used her phone. After using the phone at 7:43 AM the phone is again used frequently. According to a fitness application on VR's phone, she does not appear to take any steps while in the presence of the defendant.
19. Detectives learned from the forensic analysis of VR's phone, that after 3:30am, it begins to travel out of Massachusetts and into Rhode Island. Specifically, detectives observed data points that placed VR's phone in the area near the intersection of Broad Street and Pleasant Street in Cumberland Rhode Island from 4:24:08 AM - 7:43:07 AM.
20. Detectives armed with this information informed members of the Cumberland Rhode Island Police Department that they were interested in the area of Broad and Pleasant Street in their

community and believed the black Chevrolet Suburban with the trailer hitch may be located in that area.

21. At 10:45 PM on 01/02/2020, Detective Waldrip received a phone call from Cumberland Police Department Lieutenant Michael Ride stating that they had observed the car in the driveway of 3 Pleasant Street. The vehicle had since left the area when the phone call to Detective Waldrip was made. Lieutenant Ride reported to Detective Waldrip that the vehicle observed parked there was a 2013 Chevrolet Suburban bearing Massachusetts Registration [REDACTED]. Lieutenant Ride also reported the vehicle had a silver trailer hitch attached to the back of the vehicle. The officer who observed the vehicle was Officer Andrew Dutra of the Cumberland Police Department. After conducting a query of the vehicle it was learned the owner of that vehicle is Alvin Campbell DOB 08/02/1980 Massachusetts driver's license number: [REDACTED].
22. On 01/07/2020 the Boston Police Crime Lab confirmed that the DNA Sample located in the SAECK was a mixture, with the dominant contributor being a match to Alvin Campbell. Alvin Campbell was confirmed to have a DNA sample in CODIS due to a prior conviction in the state of Massachusetts. Alvin Campbell's DNA was also a match to two prior Boston Police Sexual Assault investigations in 2016 and 2017 as well as a CODIS match to a 2018 Medford Police Sexual Assault investigation.
23. An arrest warrant was sought for Campbell and he was arrested on January 7, 2020. Upon his arrest a white Apple iPhone cell phone with IMEI Number 354390066243657 was recovered from his hand. Campbell was actively using the cell phone when detectives approached him to place him under arrest.
24. Detectives looked into Campbell's prior criminal involvement. Campbell's recent criminal engagement is outlined below:
25. On December 08, 2019, one day after the alleged rape and kidnapping of VR, Alvin Campbell was arrested while driving the Suburban in question (MA REG [REDACTED] by the Lexington Police Department for an unrelated charge. Boston Police were provided with the Lexington Police Department Booking image of Campbell and observed Campbell's physical description and clothing (black button-down shirt) to match the description of the male given by the victim. During the incident, the defendant allegedly purported to be an UBER driver and ultimately got into a dispute with the male passenger in his car. The passenger reported to police that the driver of the vehicle that evening (Campbell) had propositioned him to have sexual relations with the two females in the vehicle. The reporting party declined the proposition and reported to police that the driver of that vehicle "became angry." According to the Lexington, MA Police report, the defendant's motor vehicle was stopped later that night and the defendant was the operator of the motor vehicle. He was arrested for an outstanding warrant on an unrelated charge.

26. Campbell has also been linked through DNA to three other rapes that were linked in the Combined DNA Index System (CODIS): two of which were committed in the City of Boston, in 2016 and 2017, respectively, and another committed in the City of Medford, Massachusetts in 2018.
27. In a 2018 Medford incident, the female victim reported she became heavily intoxicated at the Howl at the Moon Saloon in the City of Boston and got into a black colored SUV which takes her to Medford. During the trip the driver kissed the victim against her will and without her permission and touched her "pubic area". The female returned home without her underwear and believed she may have been sexually assaulted. DNA from that incident was entered into CODIS where a match was located in the database which revealed that the DNA was from Alvin Campbell.
28. In an incident that occurred in Boston on 2/9/17, the victim reported that she met the suspect at the Harp Bar near the TD Garden in the City of Boston and exchanged phone numbers with him. Later that same night the victim ordered a vehicle through the Uber application on her cell phone but the ride never materialized, so the suspect drove the victim home, where he sexually assaulted her and attempted to sexually assault her roommate. Again in that case, DNA evidence was collected and entered into CODIS which resulted in a positive match to Alvin Campbell.
29. In an incident that occurred in Boston on July 30, 2016, the victim and a group of her friends were at a downtown bar when they ordered a ride using the Uber application. The suspect picked up and drove them back to their hotel. The victim, however, separated from the group after an argument erupted and the suspect offered to drive her around so she could collect herself. When the victim asked to be taken back to her hotel the suspect refused to do so and took her instead to his apartment in the Dorchester section of the City of Boston where he sexually assaulted her. DNA collected in that incident also matched Alvin Campbell in CODIS.
30. On February 15, 2019, Campbell got into an altercation with a female known to the Commonwealth outside of a nightclub known as "Tunnel." The following is directly from the police report number I192011931 which documented the incident. "[The victim] stated that as she exited the night club "Tunnel", Campbell approached her and asked her for her number. [The victim] stated she politely declined but Campbell would not take no for an answer. Campbell then began yelling at her and shouting profanities. [The victim] further stated that she believed Campbell threw money at her then grabbed her friend [a witness known to the Commonwealth] by the hair, picked her up and slammed her to the ground. [The victim] then attempted to intervene and Campbell then picked her up and also slammed her onto the ground. [The victim] then stood up and Campbell grabbed her right hand and proceeded to twist her hand. [The victim] sustained broken nails and pain in her ring and pinky fingers. [The witness known to the Commonwealth] sustained a bump on the back of her head. [The victim and witness] refused

medical attention. Officers also spoke with [an additional eye witness] who corroborated their version of the events.”

31. On January 10th, 2020, Detective Waldrip received a phone call from two women known to the Commonwealth who explained to Detective Waldrip that on the evening of November 26, 2019, Alvin Campbell encountered them in the Seaport District of Boston. The two women informed Detective Waldrip that Campbell first asked if he could get in their car because it was cold out, he was told no. He then asked if they wanted to go to his house in Rhode Island with him which they told him no again. He then asked if they wanted to smoke marijuana and he would follow them in his vehicle to a 7-Eleven in order to buy rolling papers. Campbell took one of the women’s phones and either placed his number in it or called his phone in order to obtain their phone number. The women reported that once they were driving, Campbell began following them towards the store. The women texted Campbell that they no longer wanted to meet up, but Campbell continued to follow them for several miles onto the highway. Campbell continued to text them and over the next few weeks until about mid-December.
32. Uber provided information, pursuant to a search warrant, that Alvin Campbell was an active Uber driver until August 1, 2016.
33. A search warrant was conducted on his car MA Reg- [REDACTED] on January 9, 2020, and UBER stickers were located on the windshield and front passenger floor. Additionally, business cards in the name of Alvin Campbell with UBER codes written on the back were located during the search of the car.
34. Detectives on February 12, 2020 were able to obtain a search warrant (**2084sw26 issued 2/12/20 by Judge Tochka for the period of December 6, 2019 – January 8, 2020**) for the cell phone of Alvin Campbell bearing IMEI 354390066243657 Model A1522 which was and is still in the custody of the Boston Police Department. That search warrant provided detectives with additional information which is detailed as follows:
35. Videos of VR, the victim from the incident that occurred on 12/6/2019 into 12/7/2019, being sexually assaulted while unconscious on the backseat of a vehicle which appears to be the Black Chevrolet Suburban owned by Alvin Campbell. Eleven videos are recorded during the time VR is unconscious inside the vehicle. Eight additional videos were taken by Campbell with the victim in the early morning hours at his home in Cumberland, RI and his vehicle the next morning. The male makes several comments on the video and can be observed on video placing his finger inside the vagina of a woman whom detectives believe to be VR.
36. Another video is taken where Campbell is in the backseat of his car and is calling VR by her first name asking is she OK and can be heard in attempting to help her get dressed after the sexual assault by explaining to VR that her arm needs to go into the sleeve of her upper garment. VR

remains unresponsive during this video. He acknowledges her physical state by instructing her to raise an eyebrow if she is OK.

37. In one of the recovered videos from that evening VR is filmed clothed, unconscious and appeared to be sleeping in the back bench seat of Campbell's vehicle. In this particular video you can clearly see the victim's entire body including her face.
38. Also found in the photographs section of Campbell's phone was a picture of VR's driver's license.
39. Also found in the phone from the original search warrant was a phone message conversation with phone number [REDACTED]. In that text conversation there is a text message from [REDACTED] dated 12/12/2019 at 3:08:37 PM (UTC -5) where the person texted Campbell's phone stating "I think of you as nothing more than a rapist. And I seen you in Boston about a year ago outside the garden...don't ever harass me like that and yell out for me. What were you doing waiting for more belligerently girls you can scoop up? Don't text me again."
40. The text conversation continues with another message from the above number to Campbell stating "I was drunk! I don't remember a thing from that night, but I have a voice recording of myself in your car and there's no fucking way you didn't know I was drunk that night" Another message dated 12/12/2019 at 3:12:21 PM (UTC-5) from [REDACTED] to Campbell's phone stated "You picked me up with piss down my legs, you knew I was drunk, just by my voice you knew I was drunk. And I'm not blaming anyone I'm grown but your still a rapist in my eyes. Disgusting" The conversation continues on, at 3:18:18 PM (UTC-5) the phone number [REDACTED] text Campbell's phone "Yeah because you know you're the piece of shit who took full advantage of the situation. I could barely speak straight and you decided it was ok to fuck me..idc if I threw myself at you, you could have said hell no this young girl is so drunk but you didn't. you're gross. I hope you never have a daughter because karma will come around to you. Now have a good day and don't text my phone anymore."
41. It should be noted through the course of this text conversation Campbell denied raping the accuser.
42. A review of Campbell's publicly available Facebook account offers further evidence of the suspect's proclivity for making videos. By way of example, working backward from the day the suspect was arrested for the kidnapping and rape of VR, January 8th, 2020, through June of 2019, the suspect posted approximately 153 videos on Facebook. These videos are mundane in content and depict no criminal activity, but certainly confirm that the suspect is a person who documents his life via video-recordings and other forms of social media.
43. Based on Campbell's affinity for memorializing his life through video, the discovery of videos in which Campbell is raping VR, the linkage to three prior incident via DNA, and the texts between an unknown female who accuses Campbell of raping her, Detective Waldrip sought and was

granted a second warrant for Campbell's iPhone (issued on 3/12/20 by Judge Tochka for the period January 1, 2016 – January 8, 2020).

44. During a review of data from the second search warrant, detectives discovered video and photographic evidence of Campbell committing multiple sexual assaults on intoxicated females. Specifically, video and/or photographic evidence of approximately eight assaults, occurring from February 2017 to December 2019 were located on this cell phone.
45. The crimes documented by Campbell include Rape, Indecent Assault and Battery, and a variety of instances where Campbell secretly video and audio records these victim's in various states of undress without their knowledge or consent.
46. Based on these videos and photographs, Boston Police Detectives had identified and interviewed eight additional women who were assaulted by Campbell on various dates. Of the eight women interviewed, all but one has agreed to cooperate in further police investigations.
47. Videos of the 2017 rape in Boston and the 2018 rape in Medford were also recovered from Campbell's phone.

48. Campbell was employed by UBER from 2/20/2015 to 8/1/2016.

BACKGROUND REGARDING APPLE ID AND ICLOUD:

1. Apple is a United States company that produces the iPhone, iPad, iPod Touch and Apple Watch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing texts, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
2. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud

Tabs enables iCloud to be used to synchronize web pages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

3. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through the App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.
4. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.
5. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

6. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.
7. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.
8. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.
9. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store, such as apps for financial institutions, apps for money transfers, and apps for text messaging, may reveal

services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, contacts, and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's users.


CONCLUSION:

1. Based on the above mentioned facts, there is probable cause to believe that the crime of Rape, in violation of MGL c.265:s.22b, and Kidnapping a violation of MGL c. 265: s.26, and Secret Sexual Surveillance, in violation of Massachusetts General Law c. 272 § 105, occurred on the evening of 12/6/2019 into the early morning hours of 12/7/2019.
2. Campbell has been linked by DNA to three additional sexual assaults from July 31, 2016, to as recently as December 2018.
3. Alvin Campbell has displayed a pattern of sexual predatory behavior where he targets women coming out of licensed premises establishments who appear to be intoxicated.
4. In the most recent assault known to law enforcement that occurred on 12/6/2019 into the early morning hours of 12/7/2019 Campbell memorialized his crime by videotaping it, taking photographs of the victim's personal information and held those digital documents in his possession up until the time of arrest one month after the aggravated rape.
5. After forensic review of Campbell's cell phone, eight more victims of sexual assault and other crimes have been identified by Boston Police Detectives.
6. Campbell is shown to have a habit of memorializing these assaults by taking secret video recordings and photographs of these women, as well as pictures of prescription bottles, medical records, and other items containing, including the contact information of some of these women.
7. Campbell has shown a habit of later making contact with these victims via text messages.
8. It is also likely that detectives may become aware of more potential victims of Campbell that had encountered him.

9. Investigators are aware that electronic device utilization is one of the most common activities today. Behavioral characteristics often become routine. A person's preferences, hobbies, desires, and other behavioral characteristics can often be determined by examining digital evidence, similar to identifying what types of magazines a person chooses to read.
10. Based on my training and experience we know that electronic devices such as cellular phones are capable of being used for a number of multimedia purposes, to include, but not be limited to, the ability to send and receive phone calls, text messages, photographs, short videos, as well as other electronic data and voice communication. We also know that cellular phones contain internal memory, which can store records of received, dialed, and missed calls on that particular phone, as well as records regarding text messages. Cellular phone memory also stores downloaded ringtones, data downloaded from the internet, pictures, text messages, phone books, date books, address books call logs, subscriber information, and other data.
11. Based on training and experience I know that modern mobile devices, such as an iPhone, are capable of storing an abundance of data. Additionally, most modern mobile devices are capable of taking pictures and videos, communicating with others including suspects, victims and co-conspirators, surfing and searching the Internet.
12. Your Affiant knows that modern mobile devices, such as an iPhone or iPads, have the ability to be used for sending and receiving messages. Your Affiant knows from her training and experience that individuals who communicate using a modern mobile device often do not clean out their message folders including but not limited to the sent and received messages.
13. Your Affiant knows from experience that iCloud is Apple's cloud service that allows customers to access music, photos, applications, contacts, calendars, and documents from their iOS devices and Mac or Windows personal computers. It also enables customers to back up their iOS devices to iCloud, which as a result, information and data from the customer's iOS device is stored by Apple off the device. With the iCloud service, customers can get an iCloud.com email account or utilize their own email account.
14. Your Affiant knows from experience that depending on one's settings, iCloud will sync and store information to the cloud numerous times throughout the day almost in real time, when the device is connected to Wi-Fi. It is possible that a photograph or other items may be synced up to the iCloud and then later deleted off the iOS device, but remain on the iCloud.
15. Your Affiant knows that a person's iCloud may contain information and data from prior iOS back-ups, which is no longer contained on the actual mobile device. Therefore extracting this information from Campbell's iCloud may be the only avenue to retrieve this information.

16. Your Affiant requests that this search be unrestricted and unlimited. Campbell has a documented history of taking secret videos, photographs, and audio recordings of these unsuspecting victims. Investigators are aware of this behavior spanning the last four years and involving at least eleven women. It is more probable than not that this behavior was established prior to the first reported incident in 2016. *and specifically began when Campbell started working for Uber in 2015.*
17. Based on the foregoing facts and on-going investigation, as well as my law enforcement training and experience, your Affiant requests that a search warrant be issued. *For the periods of 2/1/2015 To 1/8/2020.*
18. Your Affiant also requests to be exempt from the mandatory seven day return period for warrants and return the warrant upon receipt of requested information from Apple.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY, this 27 day of ~~June~~ ^{July} 2020.


Sergeant Detective Amy Erlandson-LaPointe
Boston Police Department
Sexual Assault Unit

Then, personally appeared the above Sergeant Detective Amy Erlandson-LaPointe and made oath that the foregoing affidavit by his subscribed is true, on this 27th day of ~~June~~ ^{July} 2020. *132AM*

Before me,



Superior Court Justice
Suffolk Superior Court