Snap Chat: Investigating the 'Self-Destructing' App

POLICE TECHNICAL
Technical. Training. Solutions.

Aaron Edens, POLICE TECHNICAL

…Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos. Referred to as 'snaps', the company processes approximately 700 million of them every day on Apple's iOS and Google's Android operating systems. Snapchat users access the application frequently. According to marketing material provided by the company the average Snapchat user checks their account 14 times a day.

Introduction

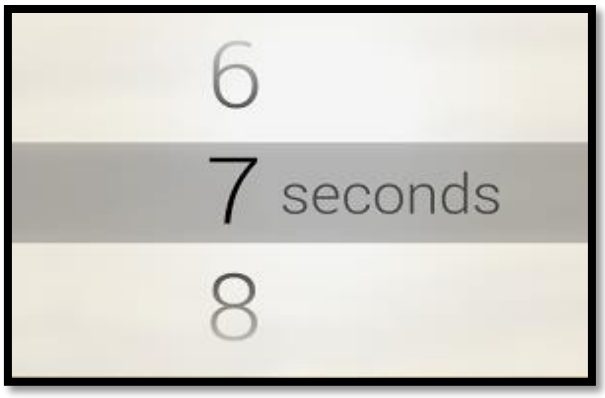
Snapchat is one of the most popular applications for sending and receiving 'self-destructing' messages, pictures, and videos. Referred to as 'snaps', the company processes approximately 700 million of them every day on Apple's iOS and Google's Android operating systems. Snapchat users access the application frequently. According to marketing material provided by the company the average Snapchat user checks their account 14 times a day.

The feeling of anonymity may reduce the inhibition of users of the Snapchat application. In one academic study 14.2% of Snapchat users admitted to having sent sexual content via Snapchat. A significant portion of those sending sexual content are likely minors. Half of Snapchat users are between the ages of 13-17. These children are sending and receiving sexual content and it is likely they are doing so in your jurisdiction. More than half of all Snapchat users are located in North America.

Investigating cases involving Snapchat can be difficult. The application is designed to destroy the very evidence law enforcement officers need to investigate and prove a criminal case. But are the images actually gone? Is it possible to retrieve them? Even if they are gone, are there other types and sources of information that can be used in a criminal investigation? Before answering those questions it is helpful to understand the language and services of Snapchat. The company offers more than just the ability to send pictures and videos.

Snaps

A snap is a picture or video message taken and shared with other Snapchat users in rea;-time. The sender of a snap has the option of setting a timer for how long the snap can be viewed. This timer has a minimum of one second and a maximum of ten seconds. Once a snap has been viewed it is deleted from the company's system and is no longer visible to the recipient.



Chat

Snapchat users can send text messages to others using the Chat feature. Once a user leaves the Chat screen, messages viewed by both the sender and the receiver will no longer visible. The application notifies other users when they are online so they can begin messaging each other.

Photos

Snapchat users can send pictures to other users by taking pictures with the front or rear facing cameras on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device.

Our Stories

Our Stories is a collection of user submitted snaps from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a rave could all contribute to the same Our Stories collection by sharing their snaps, even if they do not know each other. Users can also view Our Stories events if they are not actually present at the event by subscribing to the story.

Stories

A Snapchat user can keep a sort of photo/video diary using the Story feature. Each snap is a Story documents the user's experience. Based on the user's privacy settings, the photos and videos added to a Story can be viewed either by everyone on Snapchat or just the user's friend. Stories are visible to other users for up to 24 hours.

Snapcash

Snapcash is an online money transfer service offered by Snapchat. The actual business platform is run by SquareUp, the distributor of a mobile credit card reader and application Square Register. Snapcash can be used to transfer money between Snapchat users using a linked, U.S. issued Visa or Mastercard debit card only; using credit cards is not permitted. Snapcash can only be sent to other users who have a linked debit card.

Snapcash has a $250 weekly limit but can be upgraded to a $2,500 weekly limit. Users who upgrade have to provide their full name, date of birth, and Social Security number.

Snapcash is not supposed to be used as payment or compensation for snaps, like those involving nudity, or illegal items. It's not exactly clear how Snapchat intends to monitor potential illegal activity using Snapcash if the messages involving the transaction are automatically deleted by the company.

Law enforcement investigations involving the inevitable use of Snapcash to pay for illegal goods and services will rely heavily on information collected and retained by both Snapchat and Squareup.

Discover

Discover is a news feed from Snapchat partners such as ESPN, CNN, and the Food Network.

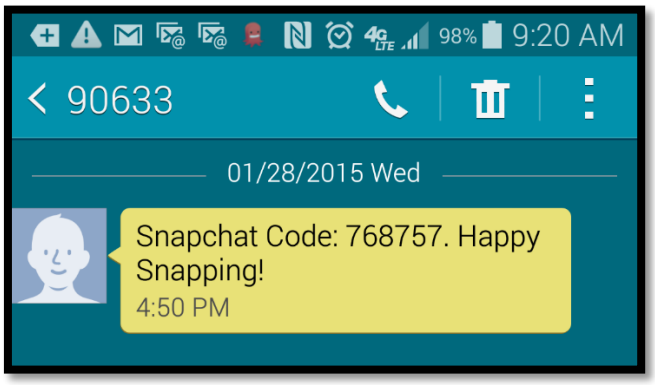
What Information Does Snapchat have?

Snapchat users may feel anonymous but the reality is the company collects and retains a considerable amount of information regarding their customers. This information is available with appropriate legal process such as a search warrant, court order, or subpoena.

When a Snapchat user creates and uses an account they have to information useful to criminal investigators, such as:

Personally Identifying Information

When a user creates an account they make a unique Snapchat username. This is the name visible to other Snapchat users. A user also enters a data of birth. This is supposed to prevent anyone under the age of 13 from using Snapchat but there is no way to verify the actual age of a user. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.



Usage Information

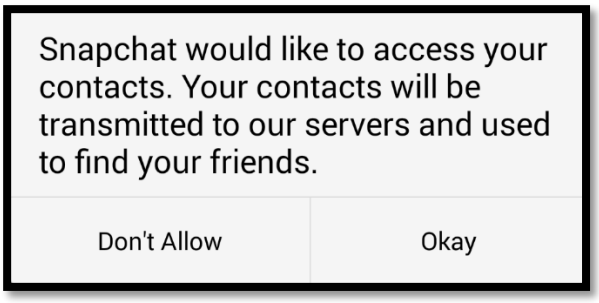
While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

Device Information

Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

Device Phonebook and Photos

If a user consents, Snapchat can access from their device's electronic phonebook or contacts list and images. It is unclear if the company stores phonebook information for any extended period of time or if they simply use it to assist with identifying any other Snapchat users among the contacts.



Financial information

Snapchat retains information about the method and source of payment of customers who use the Snapcash service. This includes i debit card information such as the card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and social security number of those involved in money transfers.

Snapcash generate a receipt for any transaction. The receipts are programmed to automatically delete after the sender and recipient have seen the message and swiped out of the Chat screen, unless either taps to save the message. Snapchat maintains transactional records for ten days. These records include information about the sender and receiver, the transaction amount, and date/time stamps of when the message was sent, received, and opened.

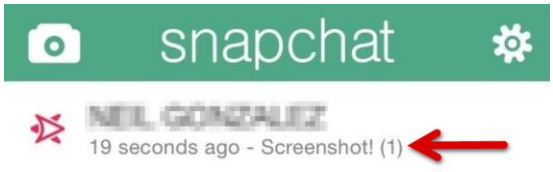
To obtain financial information it may be necessary to serve both Snapchat and Squareup with legal demands.

Message Content

Snapchat's moto is 'delete is our default.' Snapchat deletes a snap once it has been viewed. If the message is not read, because the user has not opened up the application, the message is stored for 30 days before being deleted. However, just because the snap no longer appear to the user, doesn't necessarily mean they are gone. Recovering Snapchat Messages From The Application

There are multiple avenues to explore when attempting to recover Snapchat messages. In most cases this will require actually seizing and searching the device used to send or receive the messages.

- Certain elements of chat communications within the application can be downloaded and saved by the receiver.
- Snaps can be saved by the user to the image gallery on the device. This means the image taken with the Snapchat application may exist on the mobile device that took it.
- Snapchat is programmed to automatically delete a chat after the recipient has seen it. However, a user can tap the message and saves it within the application.
- Snapchat has a feature called Replay. This allows users to view a previously viewed snap once per day. This feature is disabled by default and the user must opt-in to use Replay.
- If a Snapchat user posts an image or video to the My Story feature it can be viewed by their friends for 24 hours. If the user posted to the Our Stories feature the snaps are archived and can be viewed through Snapchat.
- Screen capture is a popular method for those receiving Snapchat messages to keep a duplicate of the image. Snapchat "attempts" to notify a user when the recipient activates the screen capture feature on their device. This feature does not always work. Alternately, Snapchat users can also take an image of their screen with a separate device or camera.



Third party apps

The 'self-destructing' aspect of Snapchat has led to an explosion of free and paid third-party apps specifically designed to save snaps. These applications use variations of the Snapchat name and sometimes are only differentiated by capitalization such as: Snapsaved, Snapsave, SnapSave, Snapchat Save Pic, Snap Save, Snapkeep, SnapBox, SnapSpy, KeepSnap, Snapchat Saver, and Save My Snaps. Use of these applications violates Snapchat's terms of service and the company works with Apple's iTunes and Google's Play Store to have them removed almost as quickly as they appear. Additionally, one of these third party apps was responsible for the data breach known as 'the Snappening' where 100,000 pictures and videos were released by hackers onto the internet. Despite these drawbacks third party apps for saving snaps continue to be popular. Unfortunately, many of these application developers are not part of a company or institution where a legal demand could be sent. Instead, it will be necessary to forensically examine a mobile device with the application installed to recover snaps from a third part application.

Forensics

In 2013 a private forensics company announced they had discovered Snapchat messages were not actually deleted. Instead, the application changed the file extension to something forensic software and examiners had not encountered before.

After the revelation that snaps were no actually deleted, the company added low level encryption to the messages to make it difficult to view these images even if they were located. Fortunately, there are solution for both locating the 'deleted' files and decrypting them. But it depends largely on the type of device, operating system, and the version of Snapchat.

Due to the structure of Apple's iOS operating system the amount of data that can be recovered during a forensic examination is limited. By design the operating system writes over recently deleted files when new data is received. Criminals using an Android device aren't so lucky. Using forensic tools, such as Internet Evidence Finder from Magnet Forensics, the following data can be recovered from Snapchat:

- Chat messages
- Even logs
- Friends
- Received images
- Received videos
- Sent snaps

While it is not always possible to recover the images and videos, it is possible to recover log data includes message content, timestamp, sender, receiver, delivery options and statuses for the messages.

Court Order

Is it possible to compel Snapchat to store messages for longer than 1-10 seconds? According to the Snapchat privacy policy it is.

"*We also sometimes receive requests from law enforcement requiring us by law to suspend our ordinary server-deletion practices for specific information*."

Prospective collection of Snapchat messages would require the use of a Federal electronic surveillance order under Title 18 United States Code 2516, also known as a Title III wiretap, or a state wiretap order. Why a wiretap order? Because no other legal mechanism available to law enforcement investigators would likely apply to the unique circumstances involving Snapchat. Collection of Snapchat messages would not be covered under the provisions of a preservation order pursuant to Title 18 United States Code Section 2703(f) as the message would be deleted from the company's servers before a law enforcement officer was even aware of the need to preserve it. Additionally, a preservation order applies retroactively, not prospectively, so future snaps could not be preserved using the technique. Similarly, legal process, such as a search warrant, would be ineffective when served on Snapchat because the messages to be seized no longer exist. A dialed number recorder/trap trace device, also known as a pen register, would conceivably collect metadata associated with the snap, provided the manufacturers of the equipment needed to do so could make the necessary configuration to capture the data. However, a pen register would not capture the content of the snaps. The remaining mechanism for collection of snaps in real-time, or near real-time, is the adaptation of an electronic surveillance order. Modification of the server-deletion practices is likely the only method for Snapchat to comply with the legal demand. Law enforcement wiretap equipment is not configured to intercept this type of communication and the company is not likely to have the capabilities or willingness to modify their equipment to comply.

The use of state wiretap laws to compel Snapchat to "suspend our ordinary server-deletion practices" could be problematic depending on the elements of the respective laws. For example, in California, Snapchat's services meets the definition of "wire communication" required to apply for a wiretap. However, the statute limits wiretaps to cases involving importation or distribution of controlled substances, murder, gang crimes, weapons of mass destruction, kidnapping, and human trafficking. Crimes commonly associated with Snapchat, such as distribution or possession of child pornography, are not covered under the state wiretap statute.

For jurisdictions where the state wiretap law is not as restrictive, or for cases involving violations that are covered by statute, establishing the requisite necessity for a wiretap should not be problematic. Most wiretap laws require that normal investigative procedures have been tried and have failed or reasonably appear either to be unlikely to succeed if tried or to be too dangerous to attempt. Traditional investigative techniques for cases involving Snapchat are largely irrelevant. As noted, search warrants, court order, and grand jury subpoenas addressed to the company are ineffective. Seizing a suspect's mobile device pursuant to a search warrant would alert them to the existence of the law enforcement investigation giving them time to flee and/or conceal or destroy evidence. Mail covers, video surveillance, pen registers, and GPS trackers are largely irrelevant and unlikely to produce relevant information if attempted. Undercover operations or the use of confidential informants are similarly unlikely to succeed.

The remaining investigative option would be to compel Snapchat to retain messages, pictures, and video using an electronic surveillance order.

Author

Aaron Edens is an instructor and author with POLICE TECHNICAL. He is the author of the seminal work on cell phone investigations, Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery (POLICE TECHNICAL 2014). He writes frequently in areas of cell phone and online investigations. .

Mr. Edens can be reached at aedens@policetechnical.com and 812-232-4200.

Search Warrant

Search warrants are the best option for obtaining information from Snapchat. However, they need to be detailed enough to obtain the relevant information without being overly broad. Each item of Snapchat information to be seized needs to be supported in the Affidavit. Simply putting the phrase "any and all information" is a bad practice as this language has consistently been found to be unconstitutionally vague as it fails to meet the reasonable particularity requirement of the Fourth Amendment.

Many investigators feel it is pointless to serve Snapchat with a search warrant as the evidentiary messages have likely long since been deleted. This should not dissuade an investigator from seeking a search warrant for the provider as there may be undelivered Snaps, as well as, other information that can only be seized with a search warrant.

Snapchat Sample Search Warrant

I, [[OFFICER NAME]], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND OFFICER BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat accounts that are stored at premises owned, maintained, controlled, or operated by Snapchat, Inc., a communications company incorporated in Delaware and headquartered in Venice, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under California Penal Code § 1524(a)(7) and Title 18 United States Code § 2703(d) to require Snapchat to disclose to the investigating officer records and other information in its possession, pertaining to the subscriber or customer using the service.

2. I am a [INSERT RANK/POSITION] with the [[AGENCY]], and have been since [[DATE]]. [[DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS QUALIFICATION TO SPEAK ABOUT THE INTERNET AND OTHER TECHNICAL MATTERS]].

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of [[STATUTES]] have been committed by [[SUSPECTS or unknown persons]]. There is also probable cause to search the information described in Attachment A for evidence of these crimes [[and contraband or fruits of these crimes]], as described in Attachment B.

PROBABLE CAUSE

5. [[Give facts establishing probable cause. At a minimum, establish a connection between the Snapchat account and a suspected crime; mention whether a preservation request was sent (or other facts suggesting Snapchat still has the records desired)]]

6. Snapchat, Inc. owns and operates a communications service that transmits alphanumeric text messages, pictures, and videos from a software application installed on a user's mobile device to another application on the mobile device or one or more users. These messages are referred to by the company, and the people who use the application, as "snaps."

7. Snapchat may be installed and used on tablet or mobile phone including those using Apple's iOS and Google's Android operating systems.

8. Snapchat's differentiating feature from other communications applications is that once a sender is able to set a variable amount of time the message is viewable by the receiver. This time can be between one and ten seconds. At the expiration of time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices.

9. If the receiver of a Snapchat message does not access the application on their device the message remains undelivered. Snapchat stores undelivered messages for 30 days. After 30 days the messages are deleted from the company's servers.

9. Before a user can begin employing the features of Snapchat they must create an account consisting of personally identifiable information and/or information that may provide additional investigative avenues for which additional search warrants or other legal process may be sought. The initial stage of creating an account is creation of a unique username. This is the name visible to other Snapchat users. A new user also enters a data of birth. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding

with the registration step. Snapchat also retains the account creation date.

10. Snapchat retains log files that are roughly analogous to the call detail records maintained by telecommunications companies. Recorded data includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status, including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

11. Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

12. If a user consents, Snapchat can access from their device's electronic phonebook or contacts list and images. It is unclear if the company stores phonebook information for any extended period of time or if they simply use it to assist with identifying any other Snapchat users among the contacts.

13. A Snapchat user can keep a sort of photo/video diary using a feature called Story. Each snap is a Story documents the user's experience. Based on the user's privacy settings, the photos and videos added to a Story can be viewed either by everyone on Snapchat or just the user's friend. Stories are visible to other users for up to 24 hours.

14. Our Stories is a collection of user submitted snaps from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event or specific geographic location. Users can also view Our Stories events if they are not actually present at the event by subscribing to the story.

15. Snapchat offers a money transfer service called Snapcash. Users are able to transfer up to $2,500 per week using this service. Snapcash transactions are only permitted using Visa and Mastercard debit cards issued by a United States Financial Institution. Money transfers can only occur if the sender and receiver both have Snapchat installed and have linked an appropriate debit card to their accounts. To facilitate these transaction, Snapchat retains retains information about the method and source of payment including debit card information such as the card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and social security number of those involved in money transfers.

16. Therefore, the computers of Snapchat are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Snapchat, such as account access information, transaction information, and account application.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

17. I anticipate executing this warrant under the California Penal Code, specifically § 1524(a)(7), and Title 18 United States Code § 2703(d) by using the warrant to require Skype to disclose to the government copies of the records and other information, including the content of communications, particularly described in Section I of Attachment B.

CONCLUSION

18. Based on the forgoing, I request that the Court issue the proposed search warrant.

19. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, 18 U.S.C. § 2711 (B) a court of general criminal jurisdiction of a State authorized by law of that State to issue search warrants.

REQUEST FOR SEALING

20. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

REQUEST FOR NON-DISCLOSURE

21. I am aware Snapchat may notify the subscriber of receipt of a search warrant unless they are specifically prohibited from doing so by the issuing judge. Disclosure of the existence of a search warrant would seriously jeopardize the on-going investigation. Accordingly, I request Snapchat, it's employees and agents, be prohibited from notifying their customer, nor anyone else not directly involved in satisfying the requirements of the search warrant, until further order of the Court.

Respectfully submitted,

[[OFFICER NAME[]

[OFFICER POSITION OR TITLE]

[[AGENCY]]

Subscribed and sworn to before me on
_____, 201___

SUPERIOR COURT JUDGE

_____