Gamified Steganography: A Neuroeconomic Strategy for Covert Communications

This paper will study the potential of combining big data, spyware, image analytics, neuroeconomics, metadata analytics, spotify data, and snapchat stories as a covert communications channel for steganography.

Introduction

Definition and History:

Steganography is an ancient art of concealing messages within other non-secret data, making it invisible to the naked eye or to anyone who does not know where to look. The word steganography comes from the Greek words steganos, meaning "covered," and graphein, meaning "writing." The practice of steganography can be traced back to the ancient Greeks, who used it to send messages by tattooing them on the scalp of messengers. Over the centuries, steganography has been used by spies, military leaders, and criminals to hide their secrets.

One of the earliest known examples of steganography dates back to the 5th century BC, when the Greek historian Herodotus tells of a message tattooed on the shaven head of a messenger. Another example of steganography can be found in the works of Julius Caesar, who used a simple substitution cipher to encode messages, hiding them within the text of his letters. During World War II, the Germans used steganography to conceal messages within the margins of newspapers, and the Allied forces used similar techniques to send messages through radio transmissions.

Current Techniques:

Today, steganography is commonly used in digital communication, where it can be used to hide messages within images, audio files, video files, and other types of digital data. There are many steganography tools and methodologies available, each with its own level of efficiency and security.

One of the most commonly used steganography tools is the LSB (least significant bit) method. This method involves replacing the least significant bit of each pixel in an image with the message bit. Since the difference between the original pixel value and the modified pixel value is usually small, the changes are not noticeable to the human eye.

Another commonly used steganography tool is the DCT (discrete cosine transform) method, which involves hiding the message within the coefficients of the DCT transformation of an image. This method is particularly effective for hiding large amounts of data, but it can be vulnerable to attacks that target the specific properties of the DCT transformation.

There are also a number of more advanced steganography tools that use machine learning algorithms to hide messages within digital data. These tools can be particularly effective at hiding messages within complex data sets, but they can also be more vulnerable to attacks that target the underlying algorithms.

The efficiency of steganography tools and methodologies depends on a number of factors, including the size of the message to be hidden, the complexity of the data in which the message is hidden, and the level of security required. In general, steganography tools that use more advanced algorithms are more effective at hiding messages within complex data sets, but they may also be more vulnerable to attacks that target the underlying algorithms. Similarly, steganography tools that use stronger encryption algorithms are generally more secure, but they may also be less efficient at hiding messages within large amounts of data.

Deception:

Deception has been a critical aspect of warfare for centuries, and it remains an essential tool for militaries and governments around the world. The ability to deceive the enemy can provide a strategic advantage in combat, allowing military forces to outmaneuver and outwit their opponents. Here are a few reasons why deception is so important in wartime:

1. Misleading the enemy: Deception can be used to mislead the enemy about a variety of things, including troop movements, objectives, and capabilities. By providing false information, military forces can confuse and disorient their opponents, making it more difficult for them to mount an effective defense.
2. Concealing strategic intentions: Deception can be used to conceal the true intentions of a military force. For example, a military force might launch a diversionary attack to distract the enemy from a more significant operation taking place elsewhere. By concealing the true objectives of an operation, military forces can increase the chances of success.
3. Protecting critical assets: Deception can also be used to protect critical assets, such as military bases or weapons systems. By using decoys or other techniques, military forces can create the impression that an asset is located in one place when it's actually located elsewhere. This can confuse the enemy and make it more difficult for them to target the asset.
4. Gaining an advantage in negotiations: Deception can also be used in diplomatic negotiations or other non-combat situations. By providing false information or making false promises, a negotiating party can gain an advantage over the other party.

Steganography offers a unique opportunity for deception by planting false signals or mis-read signals, which can incur significant costs to the adversary in terms of time, resources, and potentially subsequent action.

Missing Data:

Missing data, or gaps in a dataset, can have a significant impact on the effectiveness of steganography. For example, if a dataset used for steganography is missing key pieces of

information, it may be more difficult to encode a message without disrupting the integrity of the data. Similarly, if a dataset is not of high quality, it may be more vulnerable to detection and decoding by adversaries.

In wartime, having access to more, better quality data can provide a significant advantage in steganography. This is because having a larger dataset provides more opportunities for encoding a message without disrupting the overall structure or meaning of the data. Additionally, high-quality data is less susceptible to detection and decoding by adversaries, which can help ensure that secret messages remain hidden and secure.

Furthermore, missing data can also be used as a form of steganography in and of itself. By selectively removing certain pieces of data from a larger dataset, it may be possible to encode a message within the remaining data in a way that is difficult for adversaries to detect. This can be particularly useful in situations where the availability of data is limited, such as in remote or hostile environments.

Some methods of using missing or hidden data for steganography include:

1. Hiding a message within the metadata of a file, such as the file creation date or author name.
2. Using missing or extra words in a sentence or paragraph to convey a hidden message or code.
3. Embedding a message within the white space or margins of a document.
4. Using variations in font size or style to encode a message.
5. Altering the spacing between letters or words to create a hidden message.
6. Hiding a message within a longer text by using specific letter sequences or patterns.
7. Using hidden codes or symbols within images or diagrams to convey a message.
8. Adding hidden messages within the unused portions of a digital file, such as the unused sectors of a hard drive.
9. Encoding a message within the length or frequency of pauses or breaks in an audio or video file.
10. Using specific patterns or arrangements of data within a dataset to encode a message or signal.

Leveraging 3rd Party Messengers:

Third-party steganography involves the use of a neutral intermediary to hide a message between two parties without any direct connection to the original sender. This approach can be useful in situations where the sender wishes to obscure their identity or location, or where it is not safe or feasible to directly communicate with the intended recipient.

The use of third-party steganography can make it difficult for adversaries to detect or intercept messages, as there is no direct connection between the sender and recipient. Additionally, by

using a neutral intermediary, the original sender can avoid any potential legal or social repercussions that may arise from the content of the message.

One example of a third-party steganography system is the hawala system, which is commonly used in Middle Eastern and South Asian countries for the transfer of funds. In the hawala system, funds are transferred between two parties through a network of intermediaries who act as brokers. These intermediaries, known as hawaladars, use a system of codes and passwords to verify the identity of the sender and recipient and ensure that the funds are transferred securely.

Similarly, in the context of steganography, third-party steganographers can act as intermediaries to securely transfer hidden messages between two parties. These steganographers may use a variety of techniques to hide messages, including embedding them within images, audio files, or other digital media, and then transmitting them through secure channels.

Technological Requirements (explanation of each technology available in appendix):

1. Backdoors: specific to a user (spotify and snapchat)

Critical backdoors here are for spotify data (data about the music as well as a user/messenger) and snapchat (snapchat stories for a user and accessing memories/screenshots folder).

The use of the spotify backdoor will provide steganalysts untethered access to spotify data. This can be leveraged for creating steganographic codes which can then be accessed by a user when they click the shuffle. In addition to creating signals (legitimate or false), the steganalaysts also have access to the user's neuroeconomic parameters and can use this data to create better stop/pause mechanisms in the signals flow. This mechanism provides a covert means of communicating messages to the user as the covert messages are hidden in the general spotify network data entering the phone. Since there is no additional network traffic, the messages are concealed and secure.

The use of the snapchat backdoor can be used for 2 purposes. The first is for analyzing the pattern of arrangement of screenshots in the user's memories/screenshots folder. This is critical as different patterns will give rise to different messages. This, along with the content posted, can be analyzed and the right content/messages can be extracted and transferred to the recipient.

2. Pegasus 2

Pegasus 2 serves an offensive purpose here rather than defensive purpose.

Firstly, Pegasus 2 is used as a mechanism for the messenger or asset to communicate with the intelligence agency HQ. A few methods for communication can include: hiding the message deep in their notes application (in the case of iphone), using the volume button as binary,

swiping screenshots in either the left or right direction creating a binary or morse code, etc.. If Pegasus 2 can be combined with edge AI, a post on social media or certain input into the phone can generate personalized notifications, emails, or message which cryptographically conceal the message.

This offensive strategy provides Pegasus 2 with more responsibility. Since it is possible to hide a message within a user's phone data, steganographers who have remote access to a messenger's phone can leverage the data to embed messages covertly without the messenger having awareness of this as well. Overall, Pegasus 2 offers a secondary covert channel for steganography, hiding messages deep within a user's personal data.

3. Big Data and Knowledge Graph to embed message into code

Steganalysts require certain algorithms or data constraints to embed messages into spotify data. In this case queries through a knowledge graph can provide you with detailed relationship between objects/entities which can carry the necessary data required to embed the message. Here, the knowledge graph should be integrated with other forms of non-spotify knowledge, such as synonyms, rhyme patterns, alternate forms of messaging, etc.. By having a database pre-loaded with other metadata about words, phrases and key data points within the song, steganalysts have more flexibility when programming their messages. In addition, the use of big data and a knowledge graph provides great intelligence into other potential messages/ideas that could be generated, thereby providing the analysts with a set of possible messages that an adversary might decode. In order to maximize the deception, steganalysts can leverage unwanted data by removing, hiding, or ignoring it. By changing the data types, quantity, and quality, steganalysts can change the set of messages and deceive enemies further.

4. Image analytics

Image analytics is a crucial step in this version of steganography. Firstly, it has to be used to analyze album art. This can be done on a centralized server or at edge, and the data must be integrated into the knowledge graph such that it can be leveraged for steganography. Album art can contain objects or other data which can be deciphered as symbols or communicated ideas. In addition, image analytics is necessary at edge if the user is editing an image manually with a color pen (in snapchat or over the screenshot). Without edge image analytics, these symbols will not have merit as they will not be integrated into the knowledge graph and leveraged for future reference.

5. Interoperable and communicating AI's

The critical aspect of having multiple AI's in constant communication is because the human behavior and mechanism for posting can change. Hence, having 1 AI for image analytics, 1 AI for programming near accurate listens to force a user to stop, an AI for neuroeconomic feedback of the messenger, and different AI's for posting behavior. In these cases, each AI reinforces another and can help train each other as well. For example, the image analytics AI can communicate that a symbol was drawn on the screenshot, which can be further codified by a secondary AI into a steganographic message, which is then neuroeconomically rewarded by a third AI.

6. Neuroeconomics

Time, number of posts, type of posts, etc, are all a function of neuroeconomic parameters. For example, a user may filter through 10 songs to listen to the 11th song in the list. Without having neuroeconomic parameters to near accurately guess which song the user will land on, steganalysts will not be able to adequately codify in the messages as a user may have an unfavorable/undesirable behavior. In addition, neuroeconomics is used for gamification. Messengers can receive alternate UI's for posting signals (real or deceptive) or be rewarded for their behavior (old or novel). For example, a loading symbol UI can be indicative of a signal whereas a flash UI is indicative of no code. Alternatively, researchers can employ the placebo effect by informing users of different UI for different codes, when in reality, the loading symbol appears on a partial reinforcement basis. Neuroeconomic gamification also increases KPI's for this weapon, such as time spent shuffling codes, quality of codes, etc.. Without the right nudges, it is difficult to predict how and what the messenger will do. Neuroeconomics provides a controlled setting in an otherwise uncontrolled, unpredictable environment.

Neuroeconomics can also be applied for near accurate prediction of a user's thoughts and emotions. This can be employed not just in adtech, but in covert communications. If a steganographer is going to add text or symbols, steganalysts should be able to predict that behavior. By knowing what the user is reading, seeing, listening, etc. at all points of time, steganalysts can better near accurately predict the behavior or response.

In addition, neuroeconic programming can deliver fabulous results by eliciting a desirable behavior. By rewarding users for a type of behavior, a user is more likely to continue on that behavior. This is a critical strategy for steganography as 1 behavior, which translates to a messaging behavior type, can be broken by an adversary. Messengers need to have multiple behavioral strategies that can all be improvised in the field. Without neuroeconomics, this can be uncontrolled and unpredictable.

7. Spotify

When a user selects the shuffle feature on Spotify, they are presented with a random selection of songs from their library or a playlist. This seemingly arbitrary selection process can be influenced by several neuroeconomic factors. For example, studies have shown that people have a preference for familiar music and are more likely to choose songs they have heard before over new or unfamiliar songs. This preference for familiarity is based on the brain's tendency to seek out and respond to novel experiences, which can be perceived as a potential threat or risk.

Another factor that can influence music choices is the emotional response elicited by different songs. Research has shown that certain types of music can elicit specific emotional responses in listeners. For example, upbeat and fast-paced music can trigger feelings of happiness and excitement, while slower and more melodic music can evoke feelings of relaxation and calmness. The emotional response elicited by a particular song can influence the decision to include or exclude it from a shuffle playlist.

In addition to emotional responses, cognitive biases can also influence the choices made when using the shuffle feature on Spotify. For example, the availability bias can lead to the over-representation of certain artists or genres in shuffle playlists simply because they are more easily recalled by the user. This bias is based on the brain's tendency to rely on readily available information when making decisions, even if that information is not representative of the overall population.

Overall, the choices made when using the shuffle feature on Spotify are influenced by a complex interplay of neuroeconomic factors, including preferences for familiarity, emotional responses, and cognitive biases. By understanding these factors, music streaming platforms like Spotify can better tailor their features and recommendations to enhance the user experience and encourage continued engagement with the platform. This is critical for shuffle based steganography.

Spotify collects a vast trove of data on its users, including their listening habits, search queries, and demographic information. This data can be used for a variety of purposes, including personalizing recommendations, improving the platform's algorithms, and generating insights into music trends and consumption patterns.

However, the wealth of data collected by Spotify also presents potential opportunities for steganography. In the case of Spotify, the platform's vast collection of music data could be used as a carrier for hidden messages or information.

Here are 17 examples of how steganography could be used in Spotify. This list was generated by ChatGPT which indicates that these strategies have been burned. Nonetheless, they still can be leveraged.

1. Hiding messages within song titles or album artwork: Secret messages could be hidden within the titles or artwork of songs, albums, or playlists. This could be done by encoding

the message within the metadata of the files, or by carefully selecting the words or images used to convey the message.
2. Using song order to convey a message: By arranging songs in a specific order, a hidden message could be conveyed through the titles of the songs themselves or the order in which they appear.
3. Hiding messages within lyrics: Secret messages could be hidden within the lyrics of songs. This could be done by encoding the message within the lyrics themselves or by using specific words or phrases to convey the message.
4. Using song durations to encode messages: Song durations could be used to encode messages in a similar way to morse code. For example, a series of short and long song durations could be used to spell out a message.
5. Hiding messages within album descriptions: Album descriptions could be used to convey hidden messages, either through the use of specific words or phrases, or by encoding the message within the text.
6. Using playlist descriptions to convey a message: Similarly to album descriptions, hidden messages could be conveyed through the use of specific words or phrases in playlist descriptions.
7. Hiding messages within artist bios: Artist bios on Spotify could be used to convey hidden messages, either through the use of specific words or phrases or by encoding the message within the text.
8. Using custom playlists to encode messages: Custom playlists could be created with specific songs in a specific order to encode a hidden message.
9. Hiding messages within user profiles: User profiles on Spotify could be used to convey hidden messages, either through the use of specific words or phrases in the bio section or through the use of custom playlists.
10. Using song popularity to convey a message: The popularity of songs could be used to convey hidden messages. For example, the number of times a song is played or added to playlists could be used to spell out a message.
11. Hiding a message within the waveform of a song.
12. Concealing a message within the album cover art.
13. Adding a message within the metadata of the music file
14. Using a specific playlist or album to indicate a meeting time or location.
15. Using song release dates to encode a message or coordinate an event.
16. Hiding a message within the shuffle or repeat functions of the app
17. Embedding a secret message within the audio itself by altering specific frequencies or sounds within a song.

8. Snapchat

Snapchat is a popular social media platform that allows users to share photos and videos with their friends and followers. One of the key features of Snapchat is the "Stories" function, which allows users to post a series of photos or videos that are available for 24 hours before

disappearing. Neuroeconomics can play a role in keeping users engaged with the platform and posting on their Stories.

Snapchat rewards users with "Streaks" for posting consistently on their Stories, which can incentivize them to continue posting even when they may not have much to share. Neuroeconomics can also be used to optimize the content of Snapchat Stories to keep users engaged. Studies have shown that people are more likely to engage with content that is emotionally stimulating, visually interesting, and socially relevant. Snapchat's filters, stickers, and other features allow users to enhance their Stories in these ways, which can increase the likelihood that their followers will engage with their content and keep them posting.

In addition to its use as a social media platform, Snapchat's Stories feature can also serve as a covert communications channel. Because Snapchat Stories disappear after 24 hours, they can be used to share information or messages that are meant to be temporary or secret. For example, users could encode hidden messages within the content of their Stories by using specific colors, symbols, or other visual cues. These messages could be deciphered by those who are in the know, while remaining hidden to others.

Here are a few examples of hiding messages within snapchat. This list was generated by ChatGPT which indicdates that these strategies have been burned. Nonetheless, they still can be leveraged in steganography.

1. Using specific colors or filters in a story to represent a hidden message or code.
2. Posting images or videos in a specific order to convey a secret message or coordinate an event.
3. Adding hidden messages within the caption or text of a story by using specific words or letters.
4. Posting a story at a specific time or on a specific day to indicate a meeting time or location.
5. Using the duration of a story or the number of snaps in a story to convey a hidden message.
6. Hiding a message within the background of a story, such as a poster or other objects in the frame.
7. Concealing a message within the text overlay or drawing on a snap or story.
8. Using emojis or stickers in a specific sequence to convey a hidden message or code.
9. Adding a message within the geotags or filters of a story.
10. Embedding a secret message within the audio of a video story by altering specific frequencies or sounds.

Data Collection

Collecting data is an important part of this communication procedure. The use of the backdoor is critical for quickly attaining the metadata about each song/artist/album. With the backdoor, agencies have access to knowledge graphs of the user and can predict song choice selection based on the user's neuroeconomic parameters.

The knowledge graph can be used to connect different "ideas" presented by the messages to thread the message together. This is valuable during image analysis since different songs may have similar data/metadata which can be used to express a future signal or deceive the enemy with multiple options.

In addition, data mining with Pegasus 2 can give greater scope for hidden messages and predicting a messenger's behavior. Without all the knowledge, predicting near accurate thoughts and behavior gets difficult. Pegasus 2, with the trove of data it offers, can provide better insights into the messenger's thoughts, thereby easily programming their behaviors much better.

Spotify Screenshots Important Data (Not limited to this set of examples):

1. Song Title
2. Song Duration
3. Time point in song
4. Time remaining
5. Time listened
6. Artist Name
7. Color
8. Album Art
    a. RGB codes
    b. Objects
    c. Shapes
    d. Words/letters
9. Music Video (screenshot at any 1 point of time)
    a. RGB codes
    b. Objects
    c. Shapes
    d. Words/letters
10. Certain lyrics captured in the screenshot (if any)
11. Whether the song belongs in the liked songs
12. Playlist/Album name
13. Output device for listening
14. Remix or Single (if listed in song title)
15. Repeated Songs
16. Shuffle on

Spotify Missing Data from Screenshots:

1. Metadata
    a. Publication date
    b. Record label
    c. Artist bio
    d. Album bio
    e. Genre tag
    f. Explicit tag
2. BPM
3. Key
4. Melodies
5. Bass
6. Instruments
7. Chord sequence

Snapchat Data used for Steganography (Not limited to these examples):

1. Patterns in arrangements of screenshots
2. RGB codes
3. Filters
4. AI text producer (above keyboard) used for predictive word matching
5. Stickers/ GIFs
6. files/URL
7. Drawn images or text (using the pen option)

Communications Procedure

The first step in this procedure involves steganalysts preparing a Spotify shuffle queue using a user's liked song history. The shuffle is generated with all codes embedded in the file. The user then clicks shuffle on the liked songs and takes a screenshot of every song, capturing some but not all data. The user will keep taking screenshots of the songs one by one until they reach a desired song to stop at and listen to.

The next step is for the user to open Snapchat and select the song they want to post. The user can post all the songs in the same order the shuffle generated them or in a different order. While listening to the song, cryptograms/sounds can be embedded in real-time into the user as they are listening to communicate with the messenger. If Pegasus2 is being used for the recipient, they can listen in on the embedded message.

Image steganography and video steganography can be done during point of contact or post screenshot. Using the LSB or DCT method, steganographers can hide the message that can only be viewed once posted.

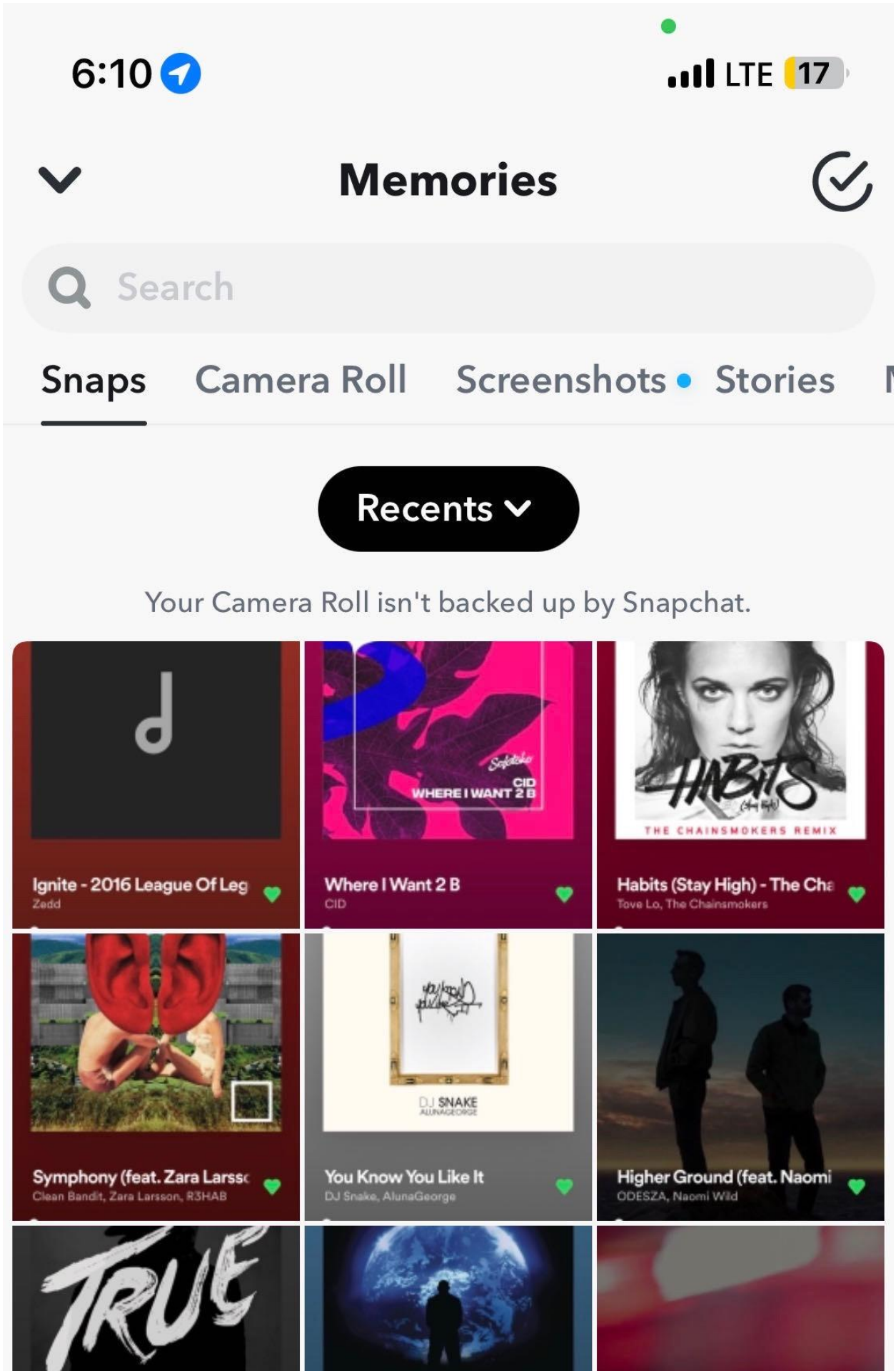
The next phase involves rewarding a user for the signal. If the user sends a covert message, Snapchat will provide them with a loading circle UI. If the user does not send a covert message, Snapchat will provide them with a quick flash UI. This process can be repeated as many times as necessary. For placebo effect, you can inform messengers that the reward scheme is for signals, thereby neuroeconomically incentivizing them to seek the reward more, when in fact the actual reward scheme is based on a partial reinforcement scheme.

Examples:

Below are 10 examples of how messages can be sent:

1. Snapchat Memories: Grid Formation Messages

As you can see in the image, Snapchat Memories can display 12 images at a time. This can breakdown a message into sub parts or conceal a message in a different arrangement. For example, a message can be in the order of the 12 songs, or be 3 across or be 3 down or be 3 diagonal. Using the hidden data, from songs posted before the 12 that are displayed, steganographers can create unique paths of different messages by combining vertical, horizontal and diagonal formations to create threads of codes/deceptive messages.


6:10
LTE 17
Memories
Search
Snaps
Camera Roll
Screenshots
Stories
Recents
Your Camera Roll isn't backed up by Snapchat.
Ignite - 2016 League Of Leg
Zedd
Where I Want 2 B
CID
Habits (Stay High) - The Cha
Tove Lo, The Chainsmokers
Symphony (feat. Zara Larsso
Clean Bandit, Zara Larsson, R3HAB
You Know You Like It
DJ Snake, AlunaGeorge
Higher Ground (feat. Naomi
ODESZA, Naomi Wild

2. Lyric Based

As you can see in the image, the steganographer can easily post the lyrics of what they are listening to. Highlighting/ marking text can either be legitimate or deceptive.

3. Latency/Image Steganography

As you can see in this image, the messenger can use a blurry image response as a signal as well. Here, the blurred image can be a post processed image that has a steganographic message embedded in it. If it has a steganographic message, it is near impossible to detect since the message is contained only within that image within the grid and no other images in the grid are effected. Alternatively, this can be caused by latency with the snapchat server. This poses an option for deception, or using latency as a signal itself.

4. Generative AI Text

In this image, you can see that the messenger has the freedom to autogenerate text messages by clicking on the 3 predicted next words. Here, keywords can be embedded into the recommended word choice which the messenger can select. The key word/words will be concealed in a generative AI text which is just a carrier of the key word.

5. Unseen albuma art/video

As you can see in this photo, latency has caused the album art/video not to be captured in this screenshot. This can either be indicative that the message is concealed in the album art, the album art is irrelevant, or have a alternate meaning entirely. Nonetheless, this latency issue can be leveraged for deception.

6. Failed to Post

As you can see in this image, certain screenshots or messages can “fail to post”. Though it is a rare occurrence, it can be used to prevent a leak of sensitive information, signal the messenger to transition to a different covert channel, or all together stop the messenger from posting for a short period of time. In the first case, in a leak of sensitive information, this provides a crucial backstop. In the case of transitioning to a different channel, this is critical as otherwise

7. Removing Songs from the Queue

As you can see in this image, the messenger has posted a queue of songs. Here, a few songs are invisible, thereby hidden to the messenger and viewer/s. This is critical for hiding data or deceiving the enemy.

8. Code Words for repeated

As you can see in this thread of examples, code word cupid was generated through a lyric and the code phrase “cupid take aim was generated”. For future reference, cupid came up again, which triggered the messenger to alter the code phrase to “cupid shoot”. By using repeated code words, AI’s can be alerted to perform actions. In this case, a potential hack or signal for end of an operation.

9. cryptograms/random noises

As you can see in this image, the steganographer indicates that a cryptogram was embeded whilst listening to the song. Cryptograms or random noises can be signals or they could be used for neuroeconomic programming. For example, if the messenger seems to not be paying attention or needs to move on, a cryptogram or noise can be a signal for that.

10. Idea repetition

Idea repetition is critical for this version of steganography. It is heavily used for deception as the same idea presented multiple times can be confusing. As you can see in this image we have the same song presented, but with 2 different album arts. In this case, a distinctive feature of one of the album arts can be a signal, or can be used to deceive the enemy. Similar examples include having a remix and original song in the same queue, not too far apart in the song queue.

Advantages

1. Still viable if leaked

Unlike cryptographic protocols, steganography has a greater deception rate as the meaning of the message is only crackable with the right context. Hence, if adversaries pick up the threat and are monitoring it, they are bombarded with:

a. Misrepresentative data
b. N false meanings and deceptive trails

2. Doubt Creation and Adaptable Behavior

In addition, humans have faster pattern recognition and potential to be misdirected, which can be used to achieve end means. In relation to a messenger's behavior, this could mean generating idea signals or markings on certain posts which are neuroeconomically programmed into the messengers themselves.

3. Need to Know/Confidentiality Attained

With the advantage of pre-programmed messages being generated, the messenger has no context to any signal at any point of time. This maintains confidentiality down the chain. Further, the use of the 3rd party and publicly viewable covert channel, it obscures the sender and messenger's identity.

4. R&D Value Exponentially Goes up

Like any other big data solution,

Disadvantages

1. Requires Multiple Teams

Since there is no absolute behavioral control over the messenger, there needs to be 2 sets of behavioral teams. One for programing new behaviors and reward schemes, one for analyzing novel behaviors. In addition, you would require a team for deception planning, data selection, and a strong IT team to maintain the network.

2. Requires Integration of Multiple AI's and Multiple Backdoors

The complexity in system architecture can pose multiple problems.

3.

Conclusion

Appendix

Backdoor:
Backdoor technologies refer to a type of software or hardware vulnerability intentionally designed to bypass security measures and provide access to a system or network. While these

vulnerabilities are sometimes used for legitimate purposes, such as providing technical support or performing software updates, they can also be exploited by malicious actors to gain unauthorized access to sensitive data. In recent years, there has been controversy surrounding the use of backdoors by governments to access corporate data and user data without permission or notification. This practice has raised concerns about privacy and civil liberties, and has sparked debate about the appropriate balance between national security and individual rights.

Backdoors can provide governments with several benefits, especially in the context of national security and law enforcement. One of the primary benefits of backdoors is that they can allow government agencies to gain access to encrypted data that may be otherwise inaccessible. This can be particularly useful in cases where law enforcement agencies need to access data related to criminal investigations or national security threats.
Another benefit of backdoors is that they can enable governments to monitor communication networks for suspicious activity, such as terrorist plotting or cyber attacks. By monitoring network traffic and identifying patterns of suspicious activity, government agencies can take steps to prevent or mitigate potential threats to national security.

Additionally, backdoors can provide a means for governments to collect intelligence on foreign governments or organizations that may pose a threat to national security. By accessing data on foreign networks, governments can gather valuable information about the activities and intentions of other countries or groups.

Overall, the use of backdoors can provide governments with enhanced capabilities for protecting national security, preventing crime, and gathering intelligence. However, the use of backdoors is also controversial, as it can raise concerns about privacy, civil liberties, and the potential for abuse. As such, any use of backdoors by governments must be carefully balanced with respect for individual rights and the rule of law.

Pegasus 2:
Pegasus 2 is a highly sophisticated spyware tool that has been developed by the Israeli cybersecurity firm, NSO Group. It is designed to be used by law enforcement and intelligence agencies to monitor the communications of suspected criminals and terrorists. However, the technology behind Pegasus 2 is extremely powerful and can be used offensively for communications interception, allowing governments to monitor the activities of political dissidents, journalists, and other individuals who are perceived as a threat to national security.

One of the primary ways that Pegasus 2 can be used offensively for communications is by intercepting voice calls and text messages. The software is able to monitor and record all communication that passes through a target device, allowing governments to listen in on private conversations and read messages exchanged between individuals. This can be a powerful tool for intelligence gathering and can help governments to identify potential threats before they can carry out any harmful activities.

Another way that Pegasus 2 can be used offensively for communications is by monitoring social media accounts and other online activity. The software is capable of tracking activity on popular social media platforms such as Facebook, Twitter, and WhatsApp, as well as monitoring email accounts and other online services. This can provide governments with valuable insights into the activities and affiliations of individuals who may be involved in criminal or terrorist activities.

Pegasus 2 can also be used to intercept and monitor internet traffic, including web browsing activity and online searches. This can provide governments with information about the interests and intentions of individuals, as well as the websites and online services that they use. By monitoring this activity, governments can gain a better understanding of the potential threats that individuals may pose and can take appropriate action to prevent harm.

Finally, Pegasus 2 can be used to remotely activate the microphone and camera on a target device, allowing governments to listen in on conversations and observe the activities of individuals in real-time. This can be a powerful tool for intelligence gathering and can provide governments with valuable information about the activities and affiliations of individuals who may be involved in criminal or terrorist activities. However, the use of this capability also raises significant privacy concerns and can be highly intrusive.

Knowledge Graph:
A knowledge graph is a data structure that represents knowledge in a way that machines can understand. It is a type of graph database that is designed to store, organize, and query complex, interconnected data. Knowledge graphs are used to represent entities (such as people, places, and things) and their relationships to one another.
A knowledge graph is constructed by identifying the entities and relationships within a domain and representing them as nodes and edges in a graph. Each node represents an entity, and each edge represents a relationship between entities. The nodes and edges are labeled with attributes and properties, which can be used to store additional information about the entities and relationships.
One of the key benefits of a knowledge graph is its ability to support efficient data extraction. Because knowledge graphs represent data as a graph, it is possible to use graph-based algorithms to traverse the graph and extract data in a way that is both efficient and intuitive. For example, a query can be constructed that follows a specific path through the graph, retrieving all of the entities and relationships that match the query criteria.
Another benefit of knowledge graphs is their ability to support semantic search. Because knowledge graphs represent data in a way that machines can understand, they can be used to support advanced search functionality that goes beyond simple keyword matching. Semantic search uses the relationships between entities in the knowledge graph to infer meaning and context, allowing for more accurate and relevant search results.
Knowledge graphs are used in a variety of applications, including natural language processing, machine learning, and data analytics. They are particularly well-suited to applications that require the efficient extraction and analysis of complex, interconnected data. Some examples of

applications that use knowledge graphs include recommendation systems, fraud detection, and personalized medicine.

Image Analytics:
Image analytics is the process of analyzing images to extract valuable insights and information from them. It involves the use of advanced algorithms and machine learning techniques to analyze and interpret images in a way that is both efficient and accurate. Image analytics can be used in a variety of applications, including surveillance, medical diagnosis, quality control, and autonomous driving.

One important application of image analytics is real-time image analysis at the edge. Edge computing involves processing data at or near the source of the data, rather than sending it to a centralized data center for processing. Real-time image analysis at the edge can be used to analyze images as they are captured, allowing for faster response times and more efficient use of resources.

Real-time image analysis at the edge involves deploying image analytics algorithms and machine learning models directly on edge devices, such as cameras or sensors. These algorithms and models are designed to analyze images in real-time, extracting valuable insights and information from them.

One example of real-time image analysis at the edge is the use of cameras in a security system. Cameras can be equipped with image analytics algorithms that analyze video footage in real-time, detecting anomalies, recognizing faces, and identifying suspicious behavior. This allows security personnel to quickly respond to potential threats, improving overall security.

Another example of real-time image analysis at the edge is the use of autonomous vehicles. Cameras and other sensors on autonomous vehicles can be equipped with image analytics algorithms that analyze the environment in real-time, detecting obstacles, identifying road signs and markings, and recognizing other vehicles and pedestrians. This allows autonomous vehicles to navigate complex environments safely and efficiently.

Overall, real-time image analysis at the edge has the potential to revolutionize a wide range of applications, from security to healthcare to transportation. By analyzing images in real-time, edge devices can provide valuable insights and information that can be used to improve efficiency, safety, and overall performance.

Metadata Analytics:
Metadata analytics is the process of analyzing metadata to extract valuable insights and information. Metadata is data that provides information about other data, such as the size, format, or location of a file. It is an important component of big data analytics because it provides context and structure to the data, making it easier to analyze and understand.

The importance of metadata for big data analytics cannot be overstated. Without metadata, big data would be unmanageable and nearly impossible to analyze. Metadata provides information about the data that is being analyzed, such as the source of the data, its format, and its structure. This information can be used to identify patterns, correlations, and trends in the data, enabling organizations to make better decisions and improve their overall performance.
However, metadata can also be weaponized in certain contexts. For example, metadata can be used to track the location and activities of individuals, potentially violating their privacy and civil liberties. Metadata can also be used to create targeted advertising and propaganda campaigns, using information about individuals' interests and preferences to influence their behavior.
One example of metadata being weaponized is the use of metadata by intelligence agencies for surveillance purposes. By collecting and analyzing metadata from phone calls, emails, and other forms of communication, intelligence agencies can track the movements and activities of individuals, potentially violating their privacy and civil liberties.
Another example of metadata being weaponized is the use of metadata by social media platforms for targeted advertising. Social media platforms collect metadata about their users, such as their likes, dislikes, and search history, and use this information to create targeted advertising campaigns. These campaigns can be used to influence the behavior of users, potentially leading to unintended consequences.
In conclusion, metadata analytics is an important component of big data analytics, providing valuable context and structure to the data being analyzed. However, it is important to recognize that metadata can also be weaponized in certain contexts, potentially violating individuals' privacy and civil liberties. It is important for organizations to use metadata in a responsible and ethical manner, respecting individuals' rights and using metadata for legitimate purposes.

Intercommunicating AI's:
Bi-directional communication refers to the exchange of information between two entities in which each entity can send and receive data from the other. In the context of artificial intelligence (AI), bi-directional communication can refer to the ability of two AI systems to interact with each other in which each system is moving in opposing directions.
In this scenario, each AI system would have the ability to send and receive data from the other AI system. This could be accomplished through the use of APIs or other forms of machine-to-machine communication. The AI systems could exchange information such as data sets, models, or other forms of output.
This type of bi-directional communication between two AI systems can have many applications. For example, it could be used in machine learning competitions, where two AI systems compete against each other to solve a particular problem. The AI systems could exchange information about their models and training data, allowing them to learn from each other and improve their performance.
Another application of bi-directional communication between two AI systems could be in the development of autonomous systems, such as self-driving cars. Two AI systems could communicate with each other to coordinate their actions and make decisions in real-time based on the data they receive from each other.

Overall, bi-directional communication between two AI systems has the potential to enable more efficient and effective machine learning and autonomous decision-making. However, it is important to consider the potential ethical implications of this technology, such as the possibility of AI systems collaborating in ways that could be harmful to humans.

Neuroeconomic Analysis:
Neuroeconomics is an interdisciplinary field that studies the neural and cognitive processes underlying economic decision-making. It combines methods and theories from neuroscience, psychology, and economics to understand how the brain processes information to make decisions about economic behavior.
One example of neuroeconomic research is a study that investigated how people make decisions about financial risk. Researchers used functional magnetic resonance imaging (fMRI) to measure brain activity while participants made decisions about whether to take a guaranteed payment or a gamble with a potentially higher payoff but greater risk of losing money. The study found that activity in the brain's prefrontal cortex was associated with the level of risk that participants were willing to take.
Another example of neuroeconomic research is a study that investigated how people make decisions about charitable giving. Researchers used fMRI to measure brain activity while participants decided how much money to donate to different charities. The study found that activity in the brain's reward centers was associated with the decision to donate, and that people were more likely to donate to charities that were associated with a positive emotional response.
In order to conduct neuroeconomic analysis, several parameters are typically needed. These include:

1. A well-defined research question: This is necessary to guide the research design and ensure that the data collected is relevant to the research question.
2. A sample of participants: Neuroeconomic studies typically require a sample of participants who are willing to participate in the study and meet certain criteria, such as age, gender, and health status.
3. A behavioral task: Neuroeconomic studies often involve behavioral tasks that require participants to make decisions about economic behavior, such as financial risk-taking or charitable giving.
4. Brain imaging technology: Brain imaging technology such as fMRI or electroencephalography (EEG) is typically used to measure brain activity while participants engage in the behavioral task.
5. Statistical analysis methods: Sophisticated statistical analysis methods are needed to analyze the data collected from brain imaging and behavioral tasks to identify patterns of brain activity associated with economic decision-making.

Overall, neuroeconomics provides a valuable tool for understanding the neural and cognitive processes underlying economic decision-making, and has the potential to inform policy and interventions aimed at improving economic behavior.

Pegasus 2 Data Capture:
Call logs

SMS messages
Email messages
Contacts
Calendar appointments
Location data
Photos
Videos
Audio recordings
Device settings
Browser history
Cookies
Saved passwords
Social media activity
Instant messages
VoIP calls
Screen recordings
Clipboard data
App usage data
Installed app information
Running app information
Network information
SIM card information
IMEI number
MAC address
IP address
Device model
Device manufacturer
Device serial number
Device carrier information
Battery level
Screen lock status
Bluetooth settings
Wi-Fi settings
GPS settings
App permissions
App data
App metadata
System logs
Error logs
Kernel logs
Crash reports
User agent string
Sensor data
Gyroscope data

Accelerometer data
Magnetometer data
Ambient light sensor data
Proximity sensor data
Barometer data
NFC data
Fingerprint sensor data
Face recognition data
Voice recognition data
Speech-to-text data
Audio fingerprinting data
Video fingerprinting data
Audio analysis data
Video analysis data
Image analysis data
OCR data
Document metadata
Document contents
File system contents
File system metadata
Keychain data
Secure Enclave data
Encryption keys
Decryption keys
Cryptographic certificates
Private keys
Public keys
Usernames
Passwords
Security question answers
Credit card information
Bank account information
Payment information
Tax information
Medical information
Health data
Fitness data
Food logs
Sleep data
Step count data
Heart rate data
Blood pressure data
Medication information
Health insurance information

Travel itineraries
Flight information
Hotel reservations
Rental car reservations
Restaurant reservations
Event tickets
Entertainment preferences
Shopping preferences
News reading habits
Political affiliations
Social network connections
GPS location history
Timestamps of when the device was active
MAC address of nearby Wi-Fi access points
MAC address of nearby Bluetooth devices
Wi-Fi hotspot information
Bluetooth device information
SIM card information, including phone number, SIM card ID, and network operator
Data usage information
Battery usage information
Device temperature
Device orientation
Keyboard input
Touchscreen input
Voice input
Multitouch input
Volume settings
Ringer settings
Vibration settings
Notification settings
Language settings
Keyboard language settings
Date and time settings
Timezone settings
Accessibility settings
Display settings
Font settings
Wallpaper settings
Security settings
Screen lock type
Passcode or PIN
Fingerprint authentication data
Facial recognition data
Iris recognition data

Biometric authentication settings
App-specific settings
Social media app settings
Email app settings
Browser app settings
App-specific data usage
App-specific battery usage
App-specific notifications
App-specific permissions
App-specific contacts
App-specific messages
App-specific photos
App-specific videos
App-specific audio recordings
App-specific location data
App-specific settings data
App-specific account information
App-specific purchase history
App-specific search history
App-specific browsing history
App-specific bookmarks
App-specific cached data
App-specific analytics data
App-specific advertising data
App-specific API requests
App-specific error logs
App-specific crash reports
App-specific user data
App-specific preferences
App-specific configuration data
App-specific device data
App-specific system data
App-specific diagnostic data
App-specific debug data
App-specific log data
App-specific transaction history
App-specific messages sent and received
App-specific contacts saved
App-specific media files shared
App-specific chat history
App-specific calls made and received
App-specific events attended
App-specific news articles read
App-specific songs played

App-specific podcasts listened to
App-specific videos watched
App-specific purchases made
App-specific search queries
App-specific location data shared
App-specific documents accessed
App-specific files downloaded or uploaded
App-specific emails sent or received
App-specific user activity
App-specific social graph
App-specific metadata
App-specific user profiles
App-specific account settings
App-specific customer support data
App-specific subscriptions
App-specific billing information
App-specific credit card data
App-specific transaction logs
App-specific ad targeting data
App-specific ad performance data
App-specific ad creative data
App-specific ad placement data
App-specific ad spend data
App-specific conversion data
App-specific impression data
App-specific attribution data
App-specific audience targeting data
App-specific user acquisition data
App-specific retention data
App-specific engagement data
App-specific user feedback