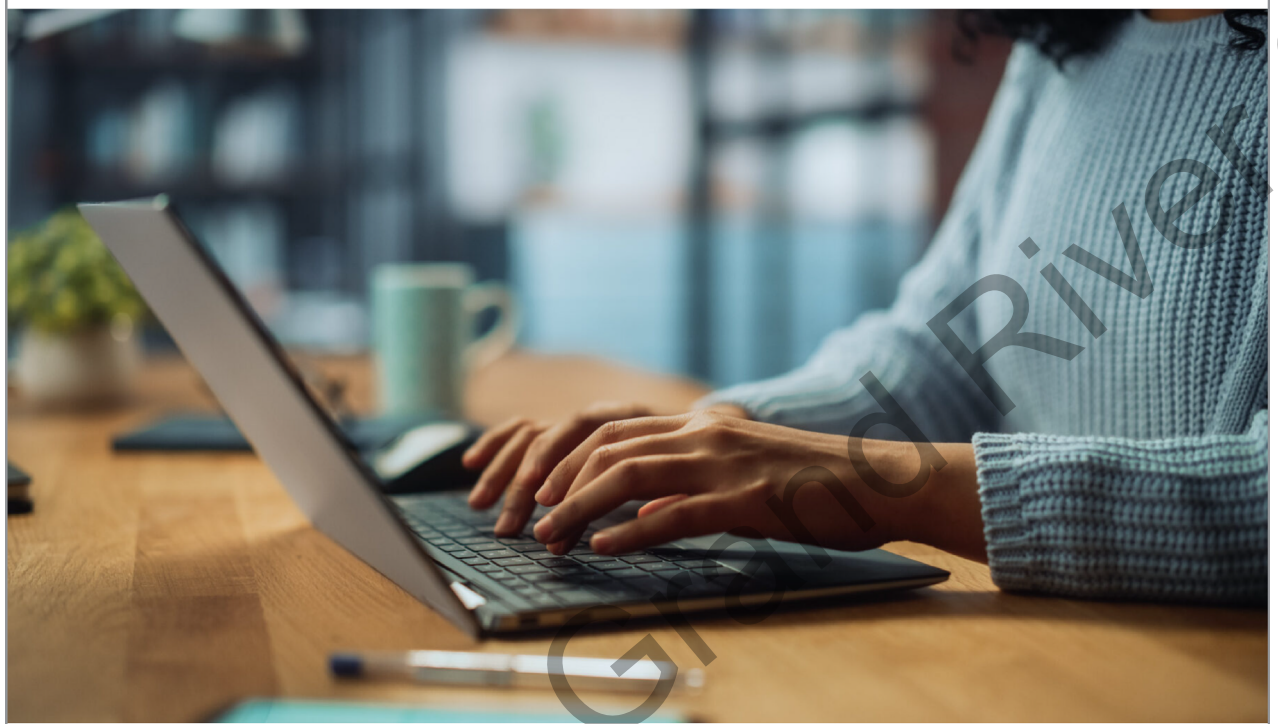
live | virtual training

Digital Evidence in Equity Cases

Tools for Evaluations & Management



with Kate Legee and Isabel Matthews

January 16, 2026

MEET YOUR FACILITATORS

Kate Legee

Senior Solutions Specialist

Isabel Mathews

Senior Solutions Specialist

AGENDA

- Introduction to Digital Evidence
- Disclosures, Intake, and Notices
- Investigations
- Analyzing Evidence and Metadata
- Evidence Relevance and Weight

ABOUT US

Vision

We exist to create safe and equitable work and educational environments.

Mission

To bring systemic change to how school districts and institutions of higher education address their Clery Act & Title IX obligations.

Core Values

- Responsive Partnership
- Innovation
- Accountability
- Transformation
- Integrity

DIGITAL EVIDENCE IN CASES

- Digital Evidence
- Social Media
- Artificial Intelligence(AI)

WHAT IS DIGITAL EVIDENCE?

Photos

Videos

Audio Recordings

Message Screenshots and Call Logs

Location Data

Metadata

TYPES AND SOURCES (APP STYLE)

- Posting Apps
- Dating Apps
- Communication Apps
- Location Sharing Apps
- Anonymous Apps

POSTING APPS

- TikTok
- Instagram and Threads
- X (formerly Twitter)
- Facebook
- Snapchat
- Reddit
- YouTube
- VSCO

- Functionality: Social networking app where Users can post various types of app specific content, such as: written posts, videos, photos, and "stories"
- Users can privately message each other

DATING APPS

- Tinder
- Hinge
- Bumble
- Grindr
- Feeld
- Coffee Meets Bagel
- Facebook Dating

Functionality: Users can "like" or swipe to match with other Users

Many apps are based on location

COMMUNICATION APPS

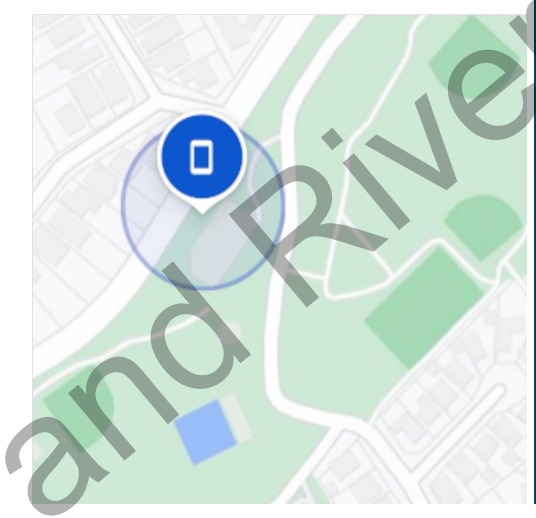
- Apple iMessages
- Android Messages
- WhatsApp
- Discord
- Instagram Messages
- Facebook Messanger
- Snapchat
- Telegram
- Free Texting Apps

Functionality: App or platform that allows Users to communicate with each other by sending messages, photos, videos, audio recordings, and location sharing between two Users or multiple Users

LOCATION SHARING APPS

Find My

- Fitness Apps (Strava, Map My Run)
- Find My Device (Google)
- Google Maps
- Find My Friends (Apple)
- Life 360
- Snapchat
- Instagram



Functionality: Shows historical and/or current device location with other Users

ANONYMOUS APPS

- YikYak
- Reddit
- Fizz/Hush
- Whisper
- SecretChat
- Blind

Functionality: Users can post verbal messages and pictures/videos by location or topic without including personally identifying information

DIGITAL EVIDENCE IN THE TITLE IX PROCESS

Disclosures

Intake & Formal Complaints

Notice of Allegations

Investigation

Hearing

Appeal

DISCLOSURES

- Considering "actual knowledge"
- Use of live stream and video media
- Message/post disappearances
- Institutional expectations around use of social media
- Barriers to reporting

TYPES OF DIGITAL DISCLOSURES

Intentional Disclosures

Party is attempting to communicate to institution

Unintentional Disclosures

Party is disclosing enough information to move forward, but not communicating to institution

Public Outcry

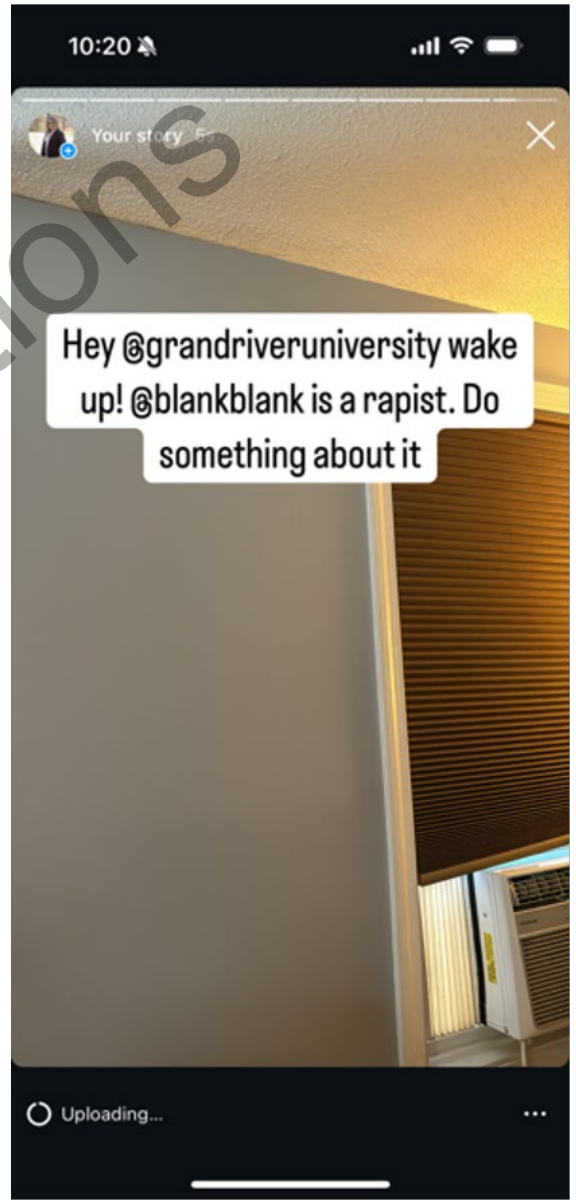
Party is communicating about institution to wider audience

Calls to Action

Party is requesting action by others

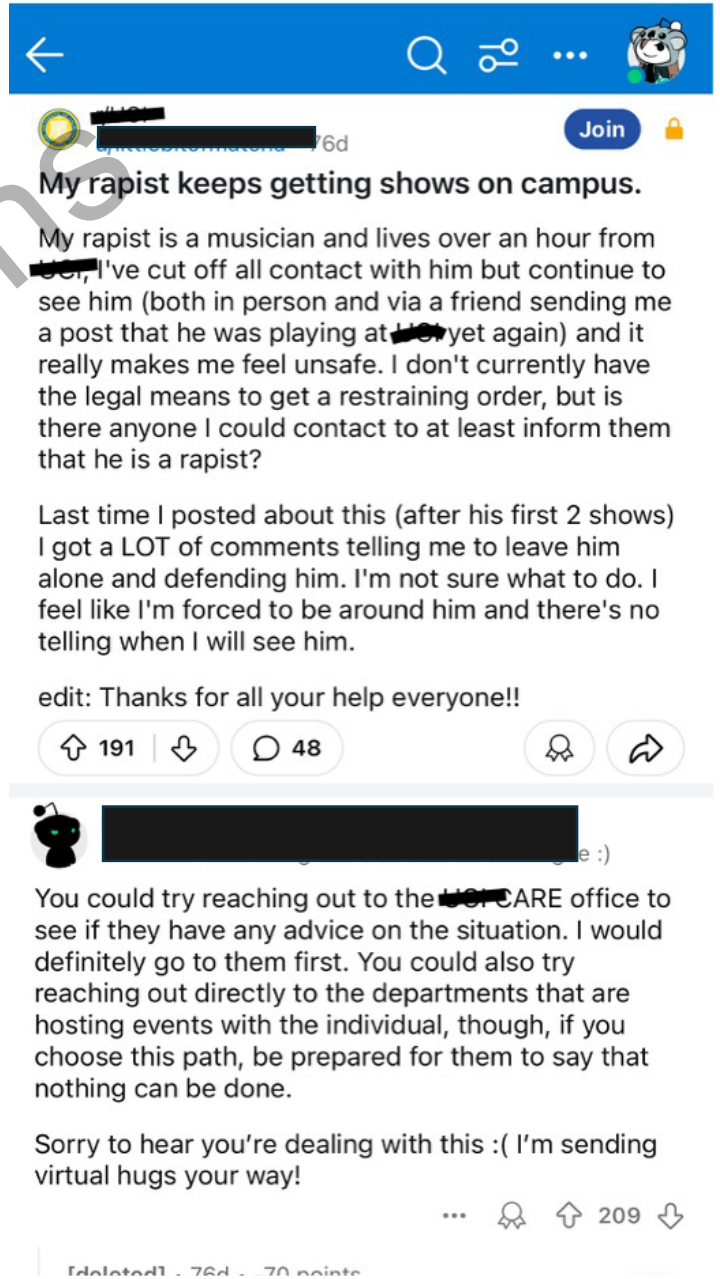
SOCIAL MEDIA DISCLOSURES

- Intentional
  - Directed to an official university account
  - Containing information that enables follow-up
  - Reported by an account that enables follow-up



SOCIAL MEDIA DISCLOSURES

- Unintentional
  - Not directed to an official university account
  - Does not contain clear information
  - May or may not be affiliated with the university



SOCIAL MEDIA DISCLOSURES

- Public Outcry
  - May be directed to an official university account
  - May use information not intended for wide release
  - May lead to comments of similar concerns

This is your weekly update on the status of the Title IX investigation, provided identically to both parties. If you have questions that are not answered by this update, please email me directly.

Updates as of Friday 11/3/23:

- The Respondent and several witnesses were interviewed virtually this week. [redacted]
- [redacted]
- [redacted]
- The current goal is to have all interviews and evidence review complete by November 10th, which still looks accomplishable. The draft investigation report will be submitted [redacted] by November 21st, although that is subject to change. [redacted] will have 10 calendar days to review the draft report and evidence and submit any response to me.
- The Decision-Maker will issue a Written Determination of Responsibility in early December to both parties.

Please let me know of any questions or concerns.

Have a good weekend

SOCIAL MEDIA DISCLOSURES

- Calls to Action
  - Specific urge to act
  - May or may not be directed to an official university account
  - May be protected expression

INITIAL ASSESSMENT AND OUTREACH

1. Receiving Report
2. Outreach & Assessment
3. Emergency Actions & Notices

RECEIVING A REPORT

- Reports must be received at any time, in a variety of ways – electronic, phone, mail, in person
- Digital evidence is often included with the initial report
- Receiving large files
- Handling photographic evidence with responsible employees
- Consider how to receive digital evidence in a report
  - Ensuring privacy of report
  - Storing digital evidence provided in a report

INITIAL REPORT SCENARIO

- You receive a text from a colleague during the workday. The text is just a video taken from a SnapChat story by another phone. In the story, there is an older man in a locker room, naked. The video appears to have been taken in the locker room of the campus gym, and the story is from a student athlete who lives on campus. The man does not appear to know that he is being recorded.

- How would you respond?
- Can you identify any issues with this scenario?

AI OR ELECTRONIC EVIDENCE IN REPORTS

- Recording of non-consensual sexual act
- Non-consensual recording of consensual or non-consensual act
- Non-consensual distribution of a recording of sexual act
- AI generated photos or videos ("deep-fake")
- Threats to share sexual videos if individual does not engage in additional sexual acts
- Online sexual exploitation and catfishing
- Cyber-stalking

AI GENERATED "DEEP-FAKE" VIDEOS AND PHOTOS

University Response

- Consider the steps that need to be taken to address this evolving form of misconduct.
- The Complainant can experience real harm regardless of if the photo or video is real.
- Impacts of distribution of AI generated content can lead to a community response.
- Request assistance from local law enforcement.

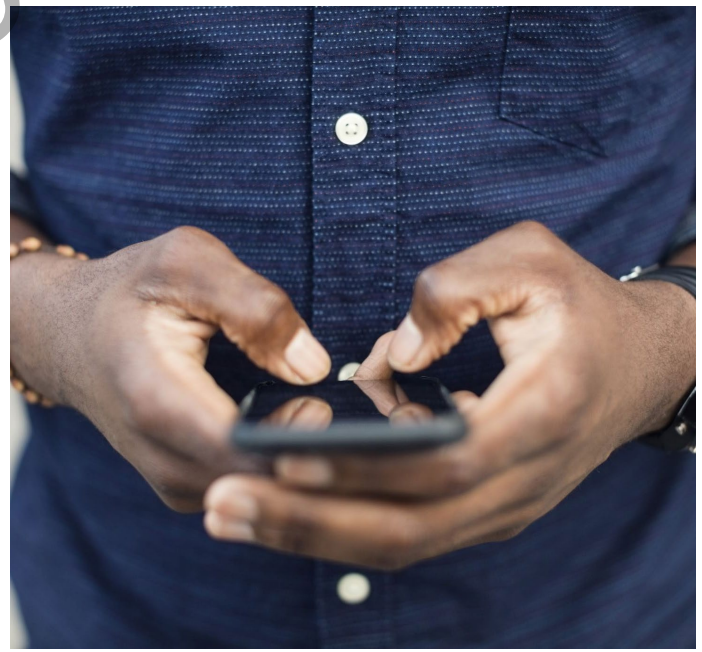
OUTREACH AND ASSESSMENT

- Capturing evidence in initial meetings
- Supportive Measures
- Formal Complaints
- Options for Resolution

- May involve significant trauma
- May involve minors, may need to include parents
- Safety concerns for meeting in-person and virtually

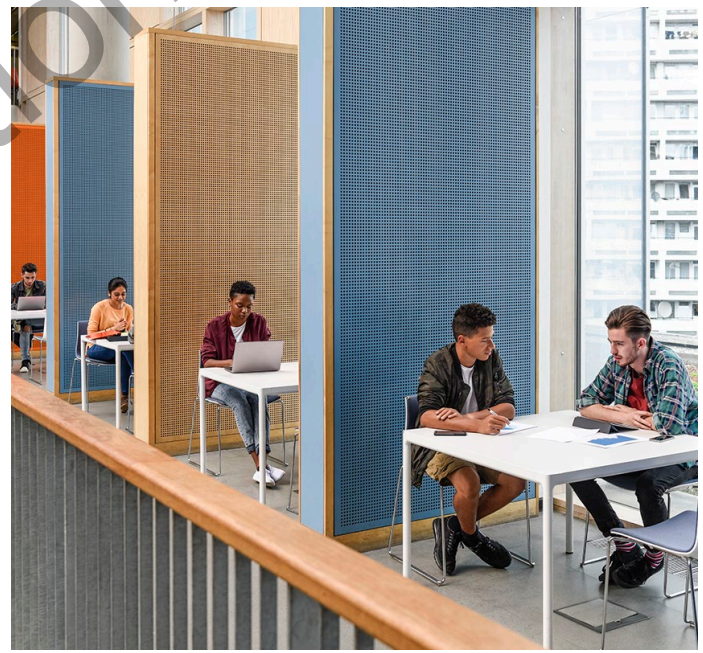
CAPTURING EVIDENCE IN INITIAL MEETING

- How to record video
- How to move files from phone to confidential database
- How to manage large files



SUPPORTIVE MEASURES

- Safety concerns/relocations
- Mutual No Contact Orders
- Technology Assistance



OPTIONS FOR RESOLUTION

1. Formal Resolution
2. Adaptive/Alternative/Informal Resolution
3. Support-Based Resolution

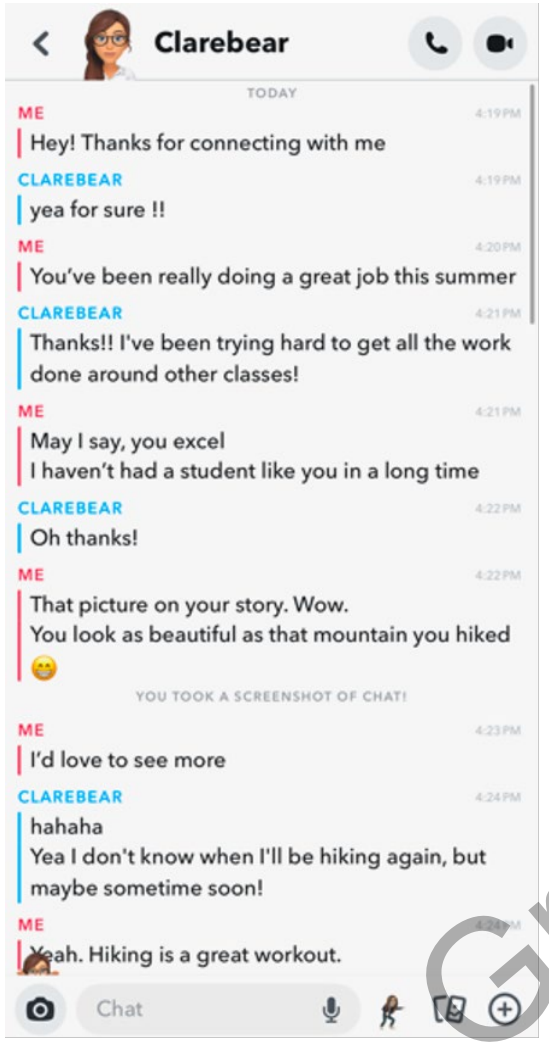
FORMAL COMPLAINT

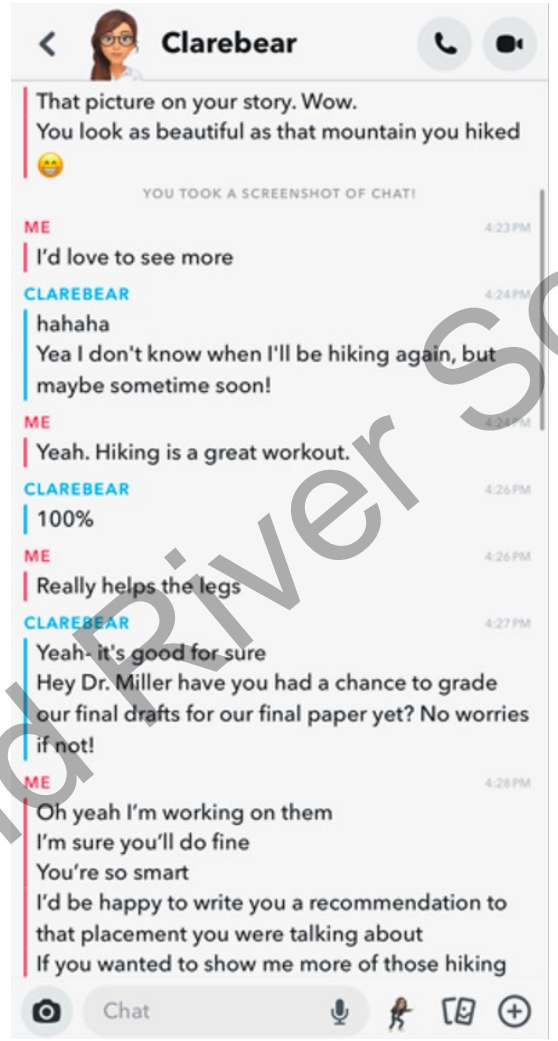
- What digital evidence is required for assessment, if any?
- How do you receive and store provided evidence?
- How do you use the formal complaint in Notice of Allegations/Investigations?

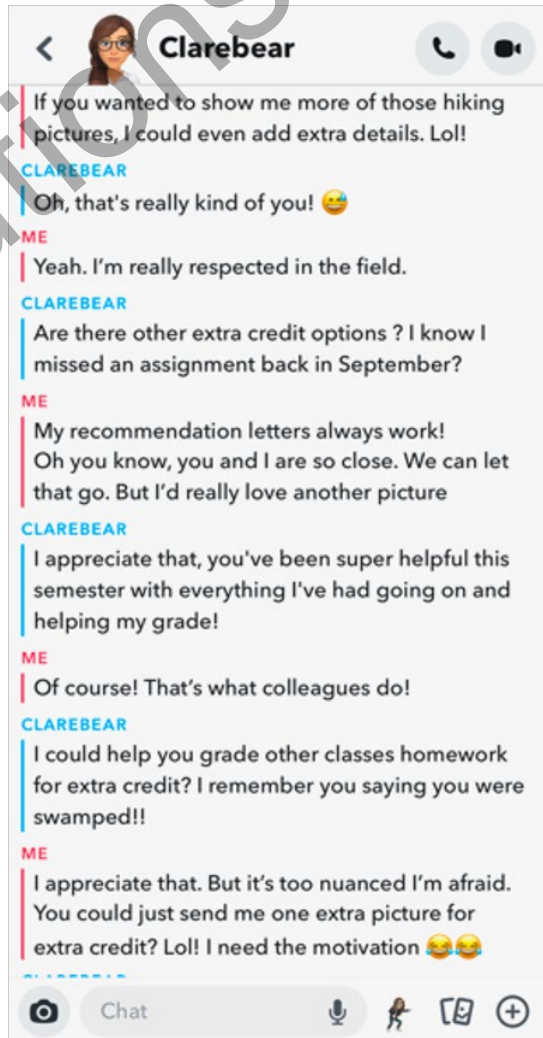
INITIAL MEETING CASE STUDY

- Clare, a freshman at Grand River University, discloses to her RA, Sarah, that her former professor, Dr. Miller, sexually exploited her during an internship program. Clare reveals that Dr. Miller, who was her academic mentor, repeatedly requested intimate photos via Snapchat, promising better grades and an academic recommendation in return. Clare felt pressured and complied out of fear that it would affect her future. Recently, Clare saw Dr. Miller boasting about their "close relationship" in a public social media post on Facebook, further distressing her. Another student tells Clare that they also saw posts on Instagram sharing censored versions of the pictures of Clare on Dr. Miller's story.
- After meeting with Clare, Title IX Coordinator learns that Clare is a minor.

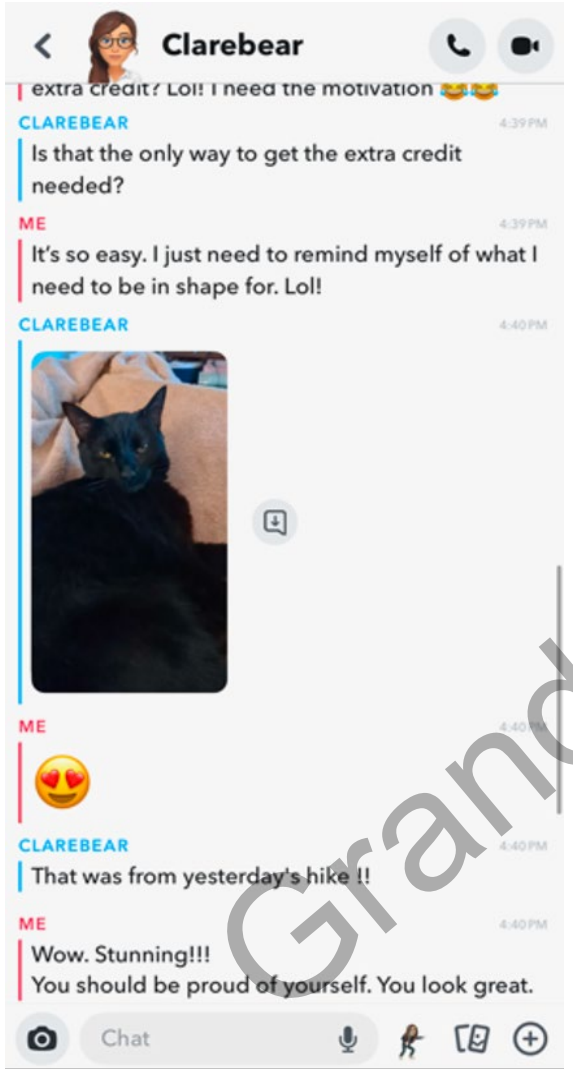
CASE STUDY EVIDENCE

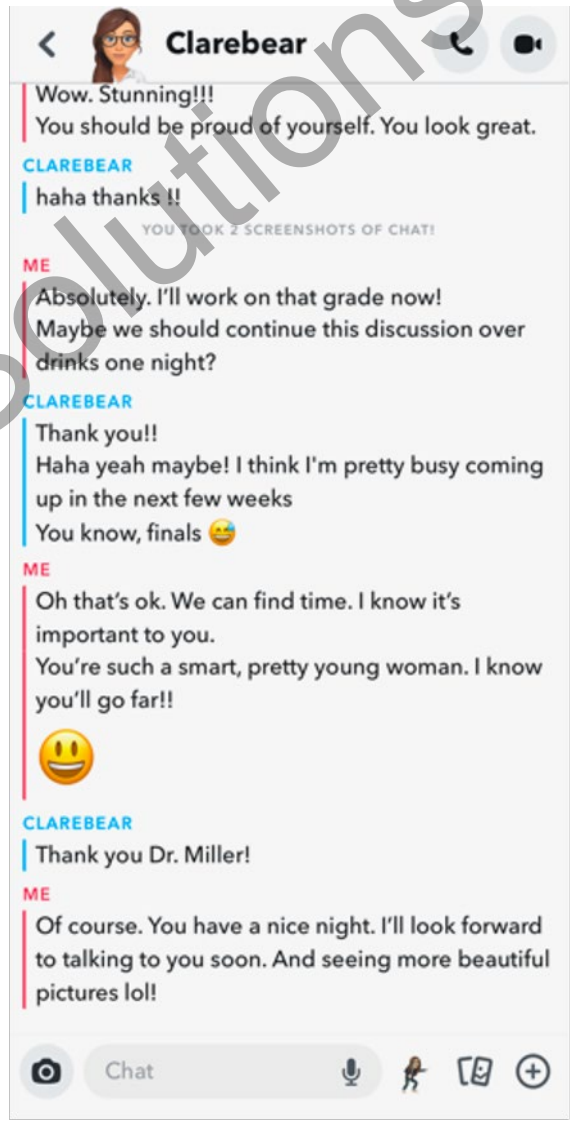




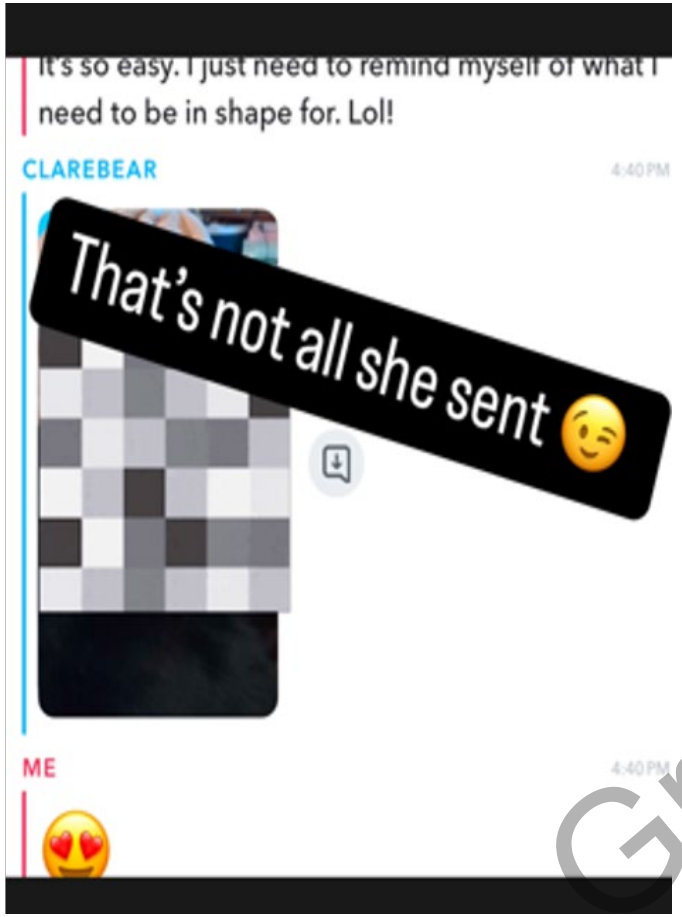


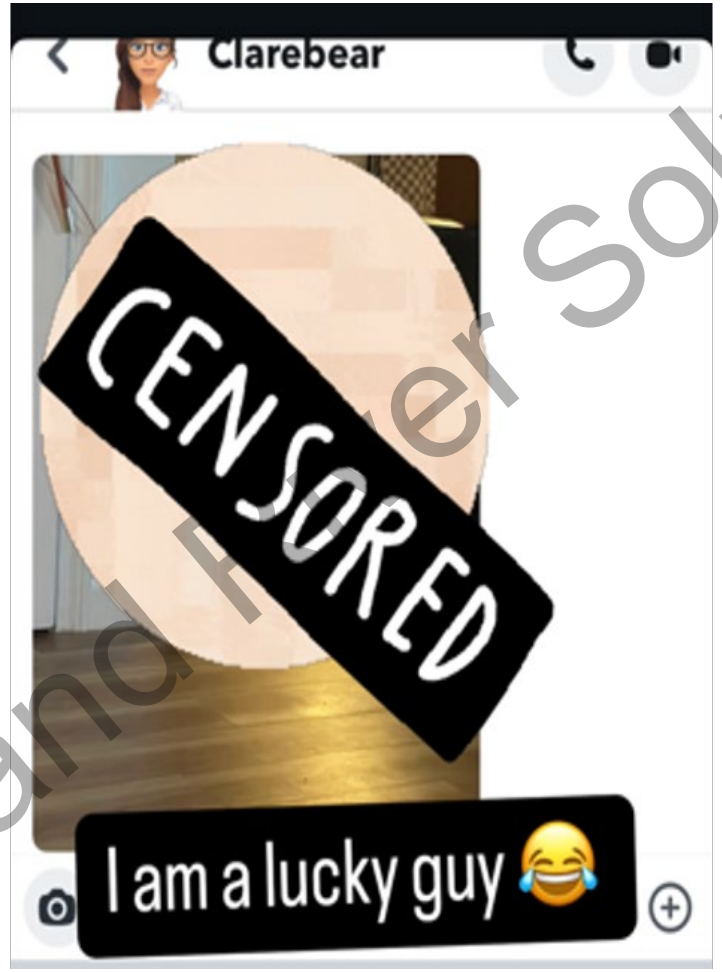
CASE STUDY EVIDENCE





CASE STUDY EVIDENCE





Just now ·

My colleague Clare and I are getting even closer. I'm so lucky to work with and mentor such smart young minds in the field. The next generation of researchers is going to keep blowing us away. I know she's blown my mind in more ways than one! lol!

Like Comment Send Share

ASSESSMENT

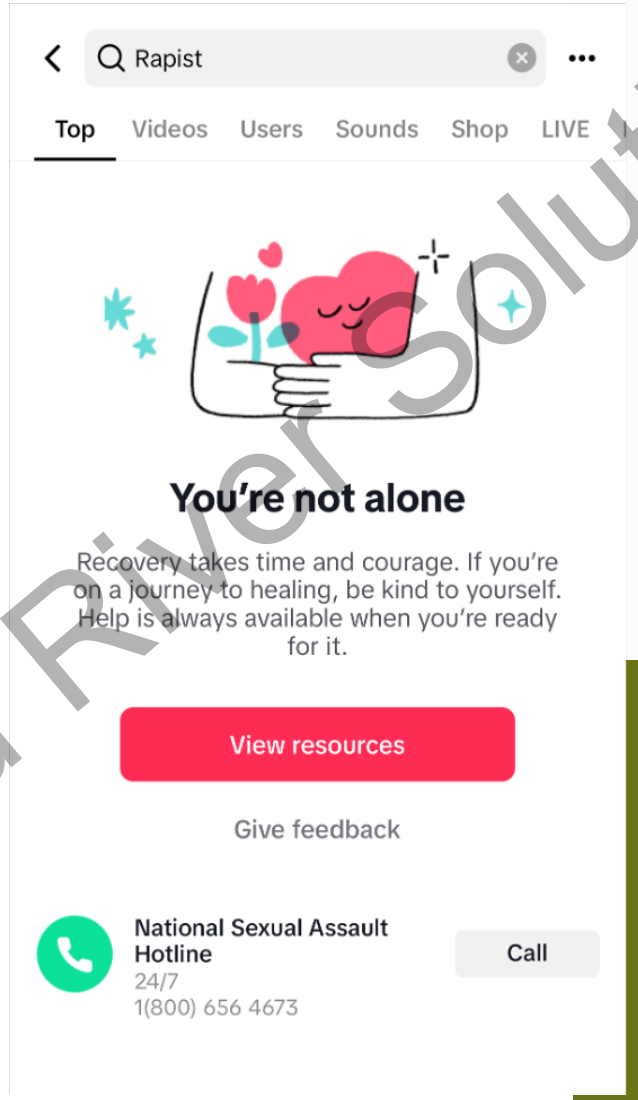
- Assess report for safety concerns
- Assess for applicability under the Policy

EMERGENCY ACTIONS

- Determine and gather specific information
  - *Location*
  - *Identities*
  - *Date/Time*

- Anonymous threats CAN be acted upon
  - *Requires* Law Enforcement Action
  - *Will* lead to sharing of IP from where post was made

- Lack of support on app
- Difficulty in learning identity
- Lack of jurisdiction



CLERY

- Geography
- Timely Warning or Emergency Notifications

EMERGENCY ACTIONS SCENARIO

- A staff member reports that there have been several posts made on YikYak that the poster intends to "curbstomp the next white b**** I come across." A similar post around the same time states "You B****es all think they're better than everyone. I'll show you what you really deserve." Finally, there is a post that says "Next girl who passes me gets it."

- How might you try to identify the poster?
- How could the University respond?

DRAFTING NOTICE

- Consider the formal complaint
- Consider evidence preservation may be lost
- Consider safety and related measures

NOTICE OF ALLEGATIONS OR DISMISSAL

Summarize digital evidence, use of formal complaint

Determining who reviews appeal

Summarizing Allegations

NOTICE SCENARIO

- Complainant reported to the Title IX office that there was a sexually explicit video of them posted on the Respondent's Instagram story. The video has since disappeared from public view, but Complainant did take a series of screenshots from the video. In the screenshots, they can be clearly identified, but the Respondent is blurry. It can be inferred from the screenshots that the parties are engaged in some type of intimate or sexual activity, but that is not visible. You know that Respondent will have the video in their Instagram history, and notice may cause them to attempt to delete the video.

- How would you respond as the Title IX Coordinator?
- What evidence might the Investigator ask for?

INTAKE WITH RESPONDENT

- Assess for safety in participating
- Provide supportive measures
- Consider evidence capture in initial meeting

INTAKE SCENARIO

- Respondent informs you that they are aware of the SnapChat photos Complainant is reporting about them engaged in consensual sex, but that Complainant is actually the individual who took them. Respondent deleted SnapChat after the two broke up, so they are unsure if the history will be able to be retrieved. Respondent also tells you they have a lawyer.

- How would you respond as the Title IX Coordinator?
- What evidence might the Investigator ask for?

INVESTIGATIONS

1. Requesting and verifying evidence from parties and witnesses
2. Investigative Report, Evidence Review and Analysis
3. Evidence and Record Retention

REQUESTING AND VERIFYING EVIDENCE

- Request photos, recordings, and videos with timestamps and metadata
- Request text message threads with timestamps
  - Party can screenshot contact card associated with message chain
  - Screen-recording of message chain with contact card
- If two participants have access to the same evidence, request the evidence from both individuals.
  - Example: Request a copy of John and Susie's text messages from both John and Susie separately.
- Request evidence from other sources that can verify party statements/evidence
  - Example: Access card swipes to residence halls, security camera footage
- At the beginning of the investigation, request that the party maintain a copy of the messages, photos, videos, etc.

REQUESTING EVIDENCE SCENARIO 1

- Alex discloses to the Investigator that they have several recordings of conversations that they took of conversations relevant to the investigation that prove that they did not commit the alleged behavior. Alex tells the Investigator that he did not tell anyone else who was part of the conversation that it was being recorded. Alex recorded the conversations off-campus at a party in Florida, which is a two-party consent state.

- Can the Investigator request the recordings?
- How should the Investigator respond?

REQUESTING DIGITAL EVIDENCE

- Data collection and evidence will vary by phone type, settings, and version of the phone's operating system
- Many apps have policies surrounding data retention and data requests on their websites.
- Ask parties to request their own data from the app
- Ask the party to check if the data is backed up on their personal device
- If communication occurred via school email or portal, copies can be requested through IT

GATHERING DATA FROM APPS

- Some apps have deleted or archived chats folder.
- Request data from apps via support or privacy request, or download their own data in Settings.
- Users can retrieve personal data, however, the data may not include messages between Users.
  - Messaging data may only include messages, photos, and videos sent by requesting User
  - Data may not be able to be retrieved past certain timeframe or if other User deleted account
- Requests can take extensive timeframe to be fulfilled, ask party to request from app as soon as possible
- Chats may be able to be restored in some apps if backed up in GoogleDrive
- Users can delete or edit their own data with certain apps

POPULAR COMMUNICATION APPS

iMessage

WhatsApp

Android Messages

Snapchat

Instagram

Discord

FUNCTIONALITY OF MESSAGING APPS

Editing Messages

- WhatsApp
- iMessage
- Android
- Instagram
- Discord
- Snapchat

Unsending Messages

- WhatsApp
- iMessage
- Android
- Instagram

Vanishing Messages

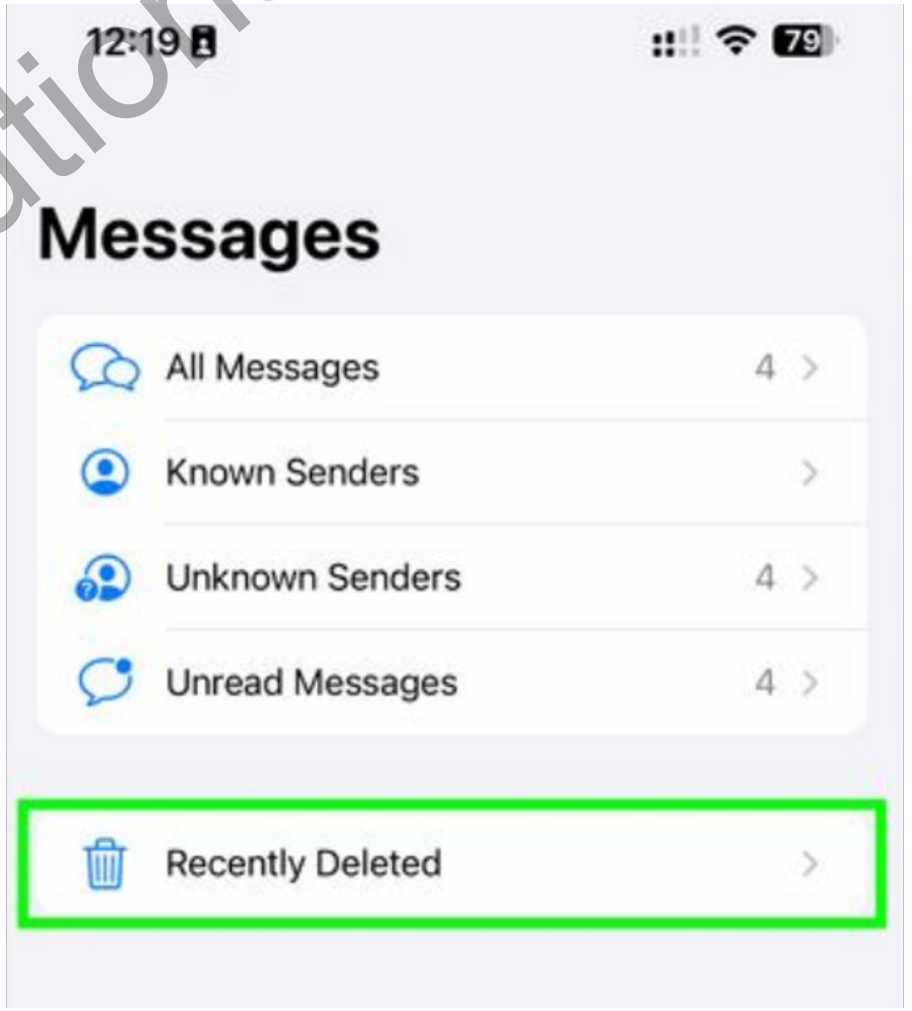
- WhatsApp
- Instagram
- Snapchat

GATHERING DATA FROM MESSAGING APPS

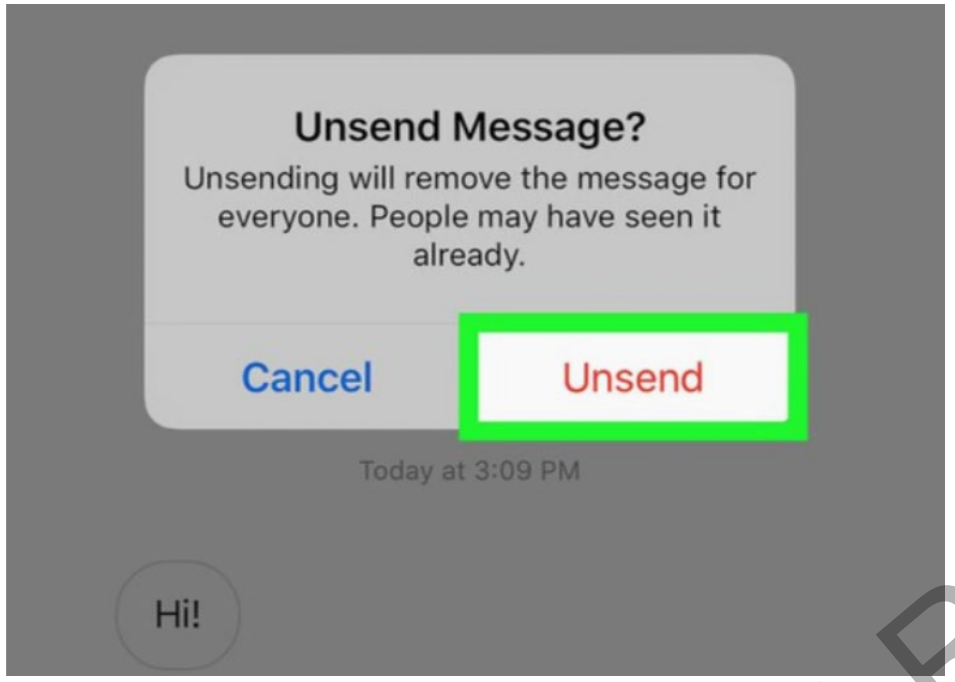
- Phone messages and call logs can be requested from User's mobile phone carrier or retrieved from a third-party software
- Many messaging apps have a recently "deleted" folder, where texts are temporarily stored before being permanently deleted from the device
- Many messaging apps are backed up through iCloud or GoogleDrive and can be restored

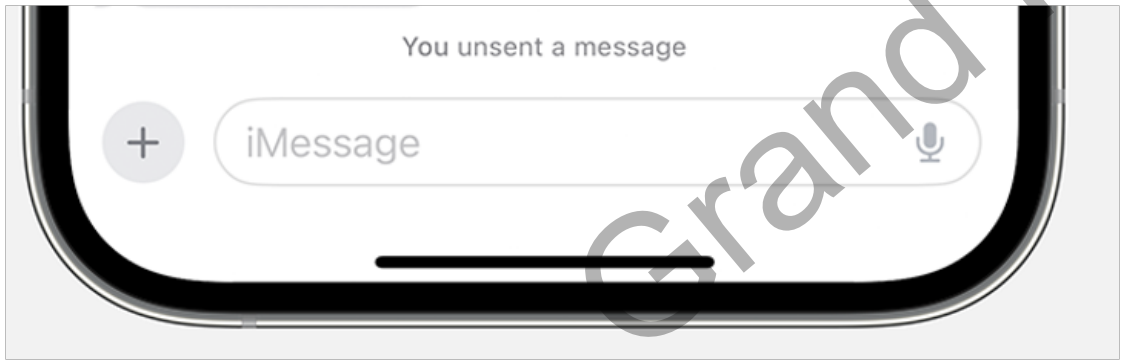
IMESSAGES (APPLE)

- Individual messages within in a text thread can be deleted by either User, but will only remove the message for the User who deleted it
- Deleted messages may still be accessible on User's iCloud account on Apple computers or in the "Recently Deleted" folder in messages
  - 30 days: deleted from devices
  - 40 days: deleted on iCloud
- If iCloud synchronization is turned "on", messages will delete across all devices using the same Apple ID
  - Settings > [user-name] > iCloud > Messages > On/Off



IMESSAGES

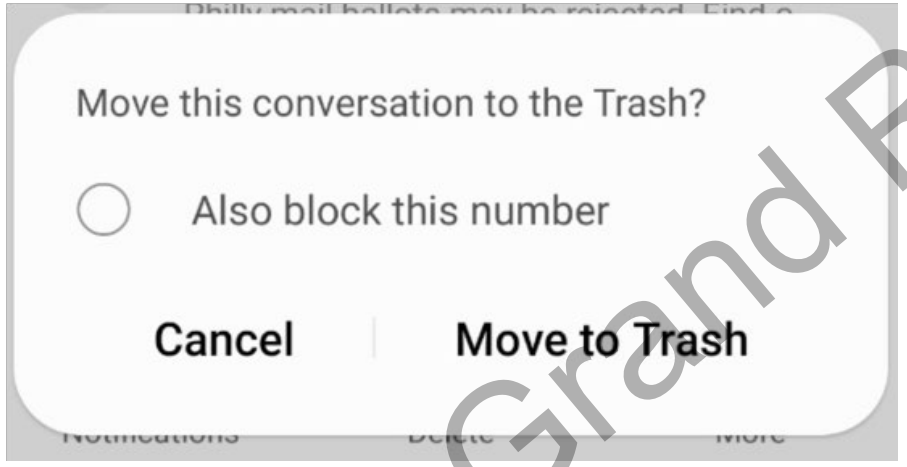


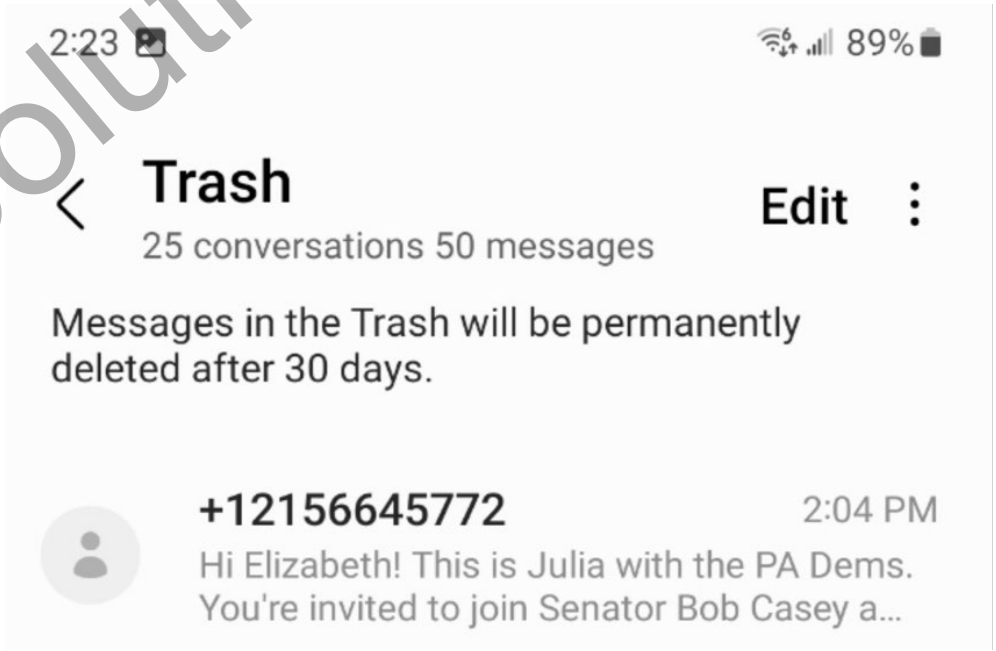


- Photos saved from messages sent from another person can be saved and then User can access photo metadata (location, time stamp, if it has been edited, etc)
  - Location, date, and other features can be edited by a User

ANDROID MESSAGES

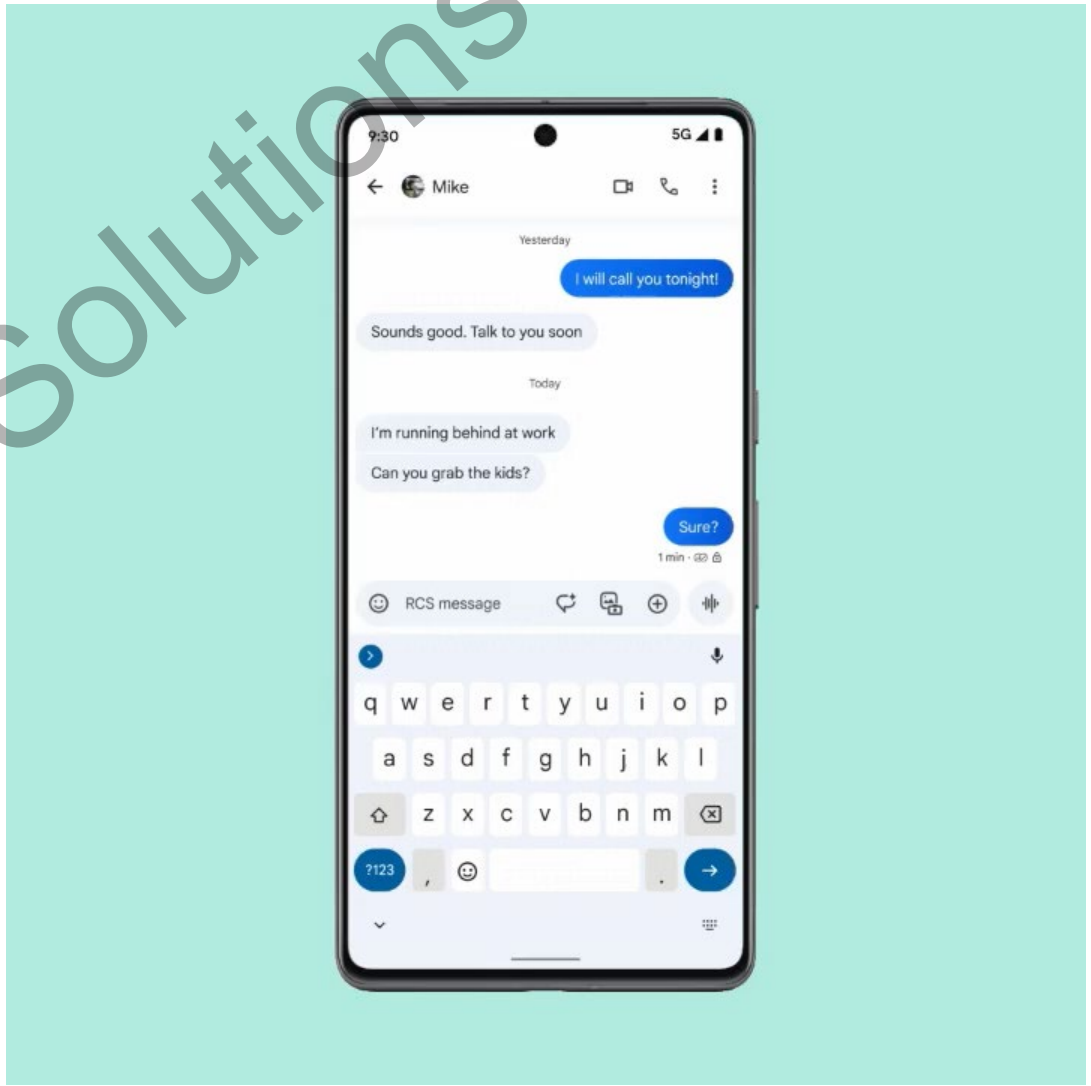
- To recover deleted messages on an Android, Users can check the "Trash"
  - 30 days: deleted from devices





ANDROID

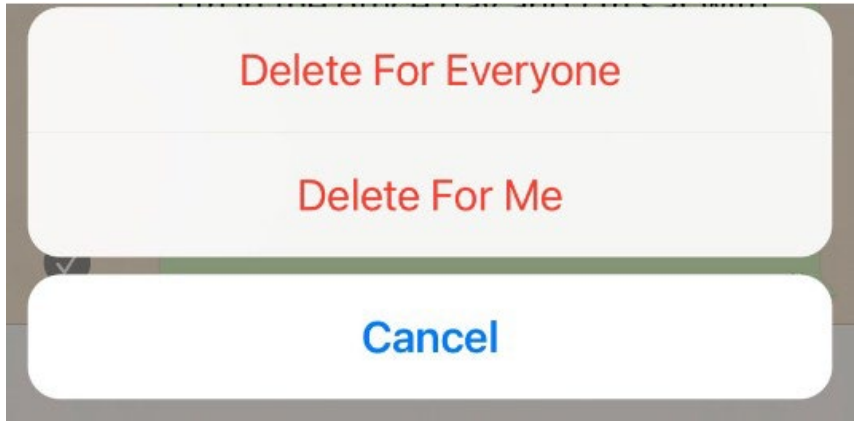
- Users can edit a message 5 times within 15-minute timeframe after being sent
- "Unsending" messages is not an option unless the User is using RCS GoogleChats and both Users have the setting on



WHATSAPP

- Messages can be deleted "For me" or "For everyone"
  - Messages can be deleted for everyone up to 2 days and 12 hours after they are sent
  - Users will see "This message was deleted" text in chat
  - Users have 5 seconds to "undo" deleting a message "for me"

- Chats can only be restored through a mobile device- not a computer

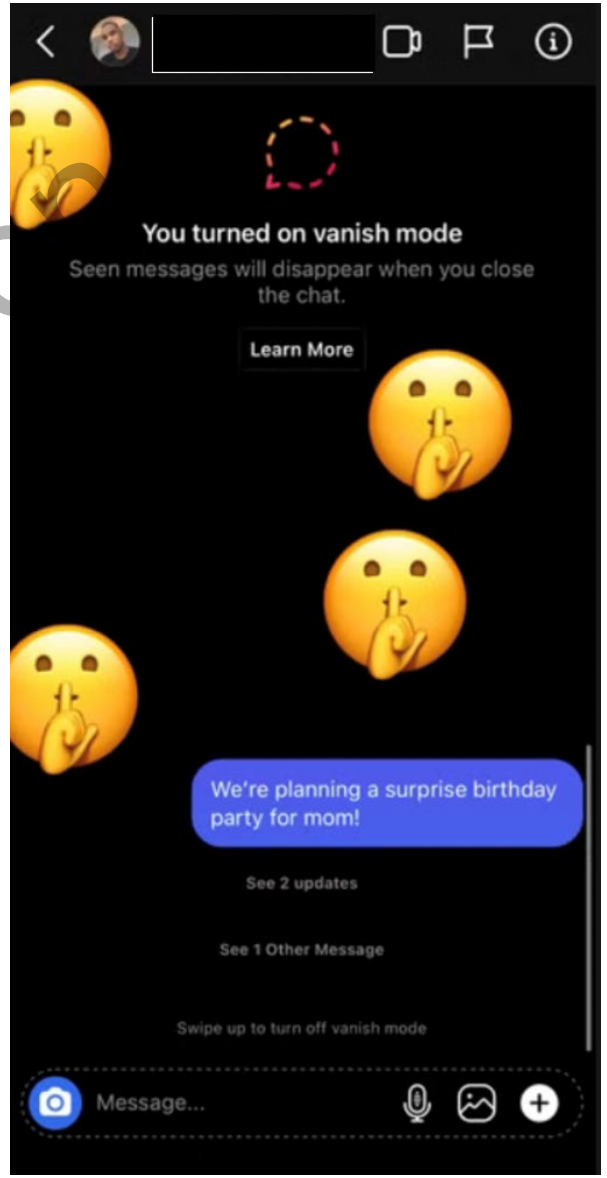


WHATSAPP

- Users can turn on "disappearing messages" option, which deletes messages for all Users after 24 hours, 7 days, or 90 days
  - Users can bookmark a disappearing chat to save it, but message sender can allow or deny the request
  - Group administrators can restrict who can save messages
  - Option to send disappearing voice messages, photos, and videos (can only be viewed once)
- Chats can be "locked" with a passcode/Face ID and hidden in a separate folder
  - Locked Chats folder can also be hidden from the main chat list and unlocked by typing code into search bar in chats

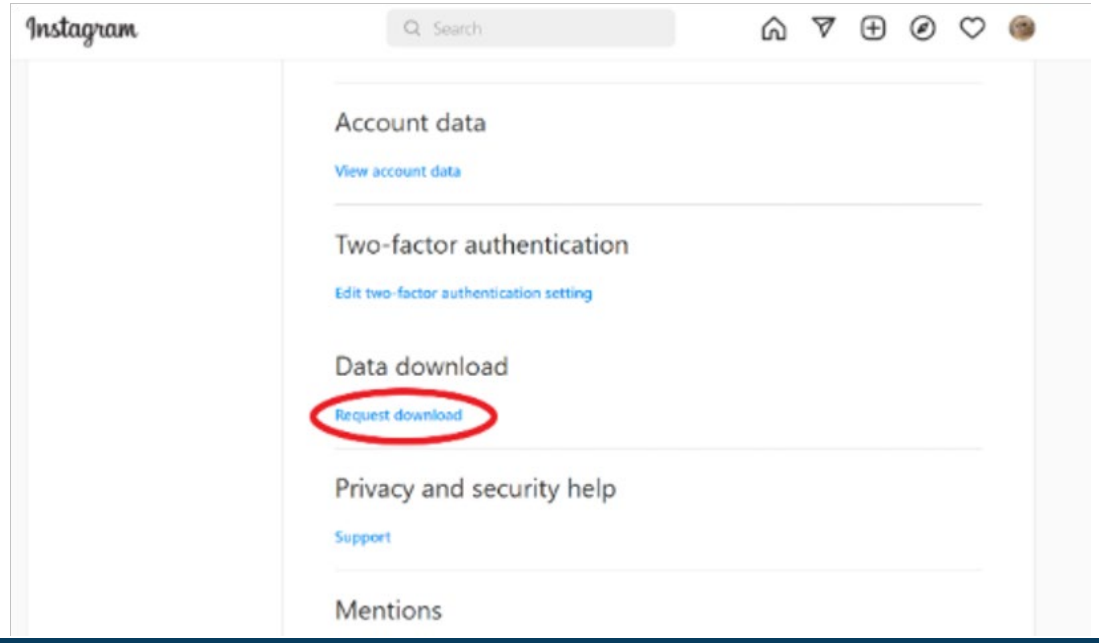
INSTAGRAM

- Vanish Mode: Messages will disappear from chat thread when both Users leave the chat
  - Both Users in the chat will be notified if Vanish mode is activated/deactivated when they open the chat thread
  - Not possible to recover or view deleted messages sent in Vanish mode
  - When Vanish mode is turned off, the messages and images sent in the chat while Vanish mode was activated will still disappear



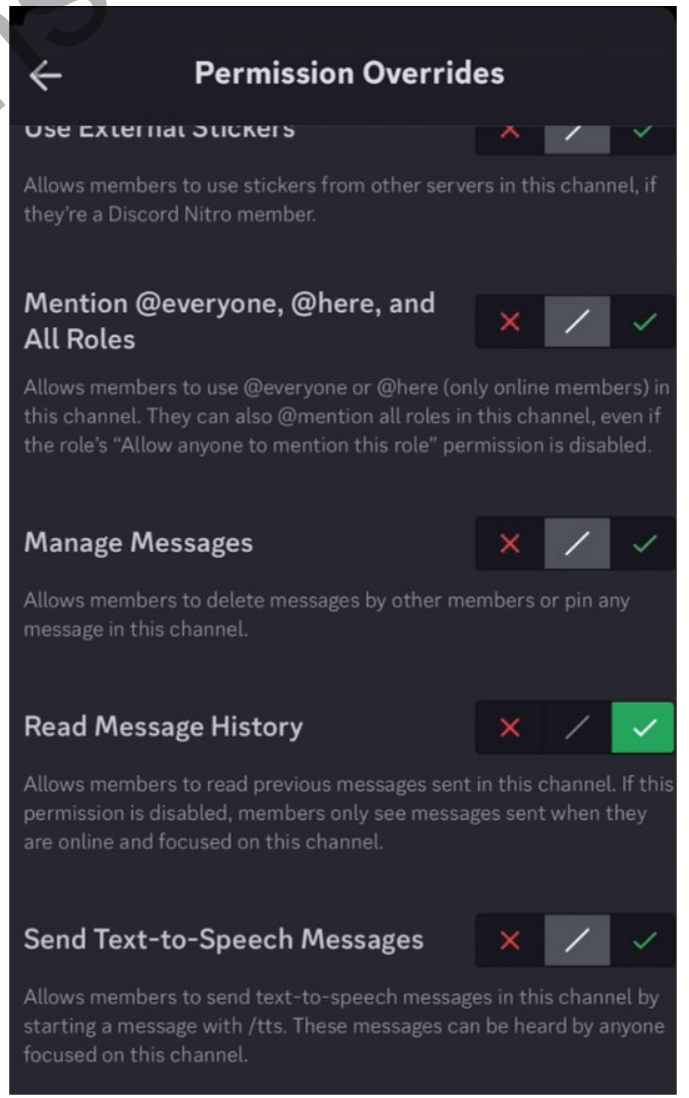
INSTAGRAM

- After a User is blocked, both Users still have access to the messages unless they choose to delete the message thread
- Deleted messages and messages sent in Vanish mode cannot be restored
  - Request data download link through Settings
  - Check "Recently Deleted" folder where content is available for up to 30 days (up to 90 days within app backup storage)
- Data Download
  - Up to 30 days to receive link via email
  - Does not include:
    - Unsent messages
    - All deleted content (dependent on timeframe and type of content)



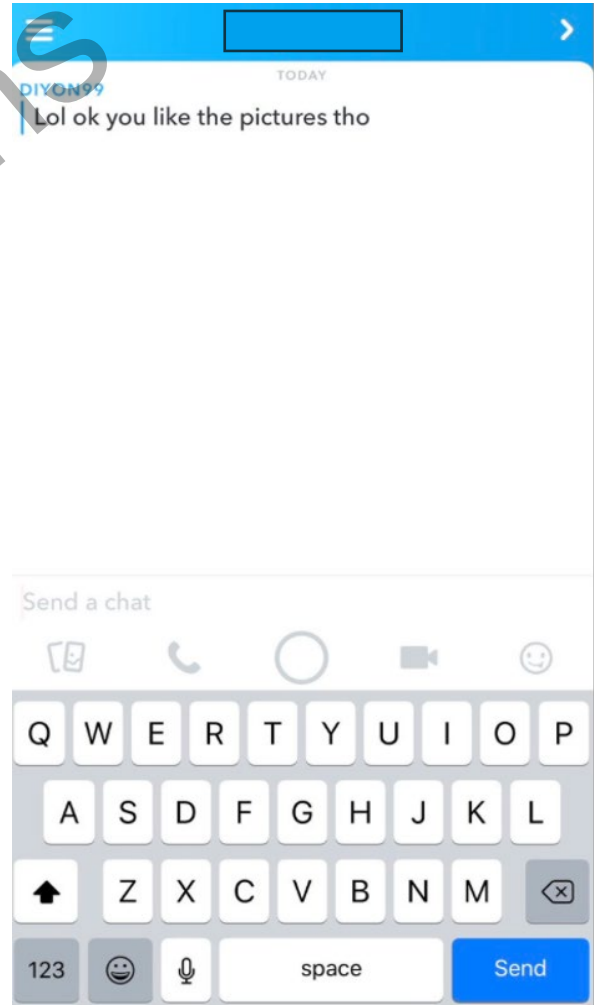
GATHERING DATA FROM MESSAGING APPS

- **Discord**
- Users can join text or voice "channels"
  - Administrators can control member permissions to send messages and view message history
- Messages can be edited
  - "Revert back to original message" option
- Messages can be forwarded between Users
  - "Forwarded" label will appear above message
- Deleted messages are removed from the chat for all Users
  - Administrators/Moderators can lock messages so they cannot be deleted.
  - Administrators/Moderators can delete other User's messages.



SNAPCHAT

- Snapchat photos/videos will be automatically deleted for all Users after being sent
  - Users will see message that content was deleted
- Deleted messages after being viewed cannot be viewed again by recipient unless saved by a User
- Messages can be edited within 5 minutes of being sent
  - "Recipient must not have opened message yet
- Messages that are not saved by either or both Users cannot be recovered
- Data download from Snapchat will only include saved photos, videos, or messages



POPULAR DATING APPS

Tinder

Hinge

Bumble

Grindr

Facebook Dating

Duet

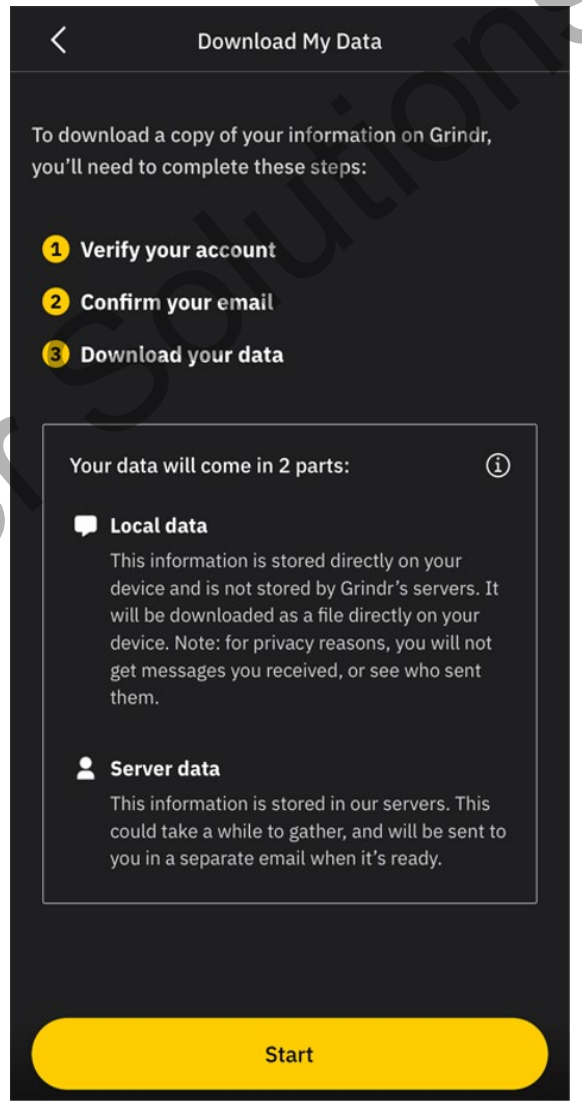
GATHERING DATA FROM DATING APPS

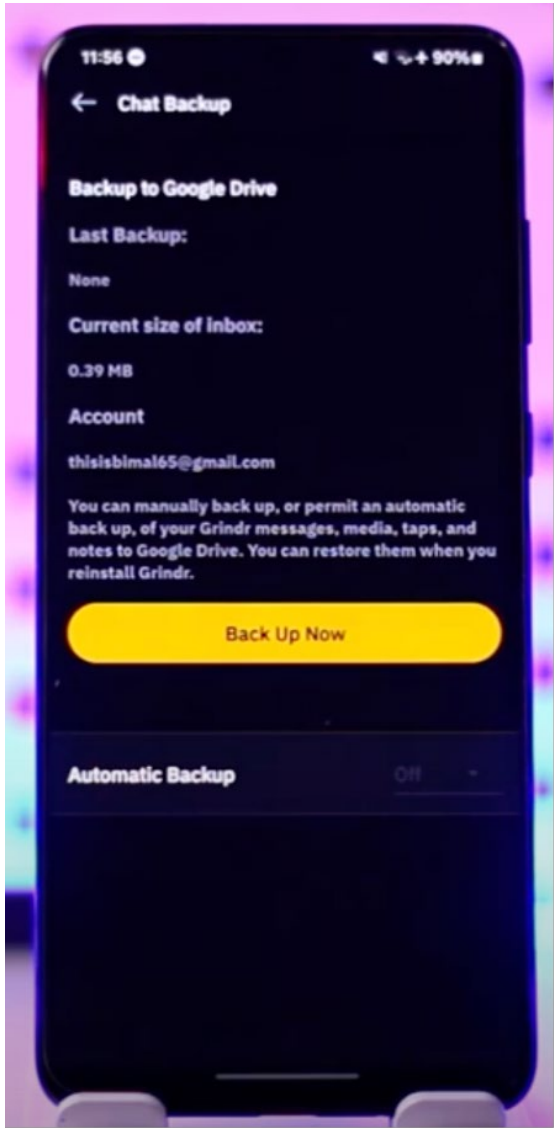
- Each dating app has a different timeframe for data retention.
- Users can download or request their information through the settings on the app or website.
  - If a profile has been deleted, data can be requested through the website.
- Data can also be restored if the app is backed up through the phone's iCloud or GoogleDrive.
- With certain apps, deleting the app off of a phone does not delete the User's profile or profile data.
- Information relating to other users, such as their messages, may not be provided in response to a data request.

GATHERING DATA FROM DATING APPS

- Tinder
  - "Manage my account" -> "Download My Information"
  - 30-day retention after account deleted

- Grindr
  - "Settings" -> "Security and Privacy" -> "Download my data"
  - Data requests can take 15-30 days to be processed and returned



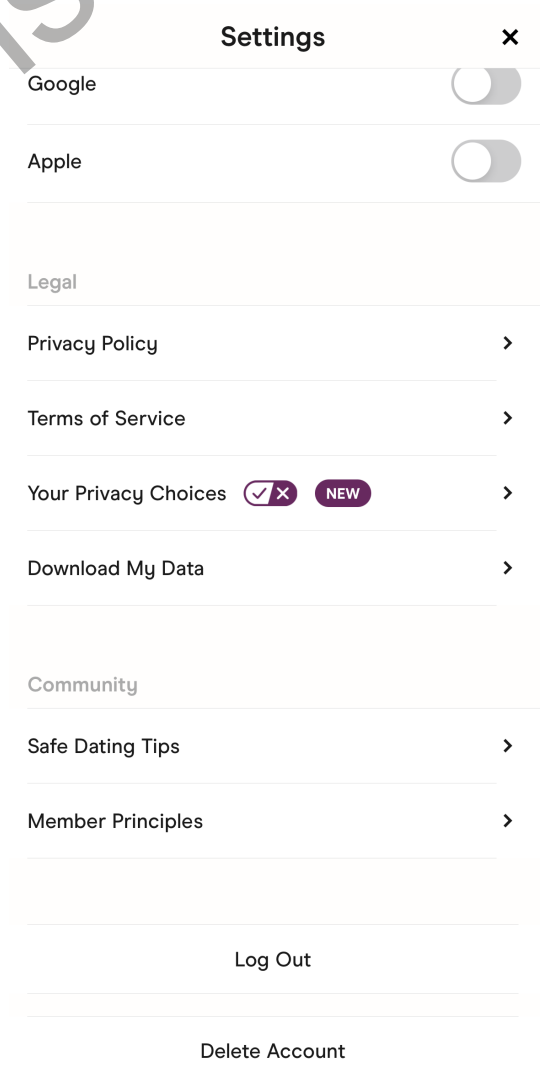


GATHERING DATA FROM DATING APPS

- Bumble
  - Some deleted accounts will remain in the conversations list as "Deleted user" for a short period of time.
  - When Date mode is disabled, all of a User's matches and conversations are removed from their account.
  - Past data and conversations can be accessed via a Subject Access Request on Bumble.
  - If an account has been deleted for over 28 days, data may not be able to be retrieved.
  - Requests can take 30 days or longer to be processed.

GATHERING DATA FROM DATING APPS

- Hinge
  - "Settings" -> "Download My Information"
  - Users have 48 hours to download the data when received
  - Users who have deleted their profiles can submit a Privacy Request and specify "I want to download or access my data."
  - Banned Users can retrieve data by clicking "Legal" from the Ban Notification.
  - As soon as an account is deleted, their personal information is removed from Hinge servers.



POPULAR LOCATION SHARING APPS

Apple Maps

Google Maps

Snapchat

Instagram

Fitness Apps

Find My

FUNCTIONALITY OF LOCATION SHARING APPS

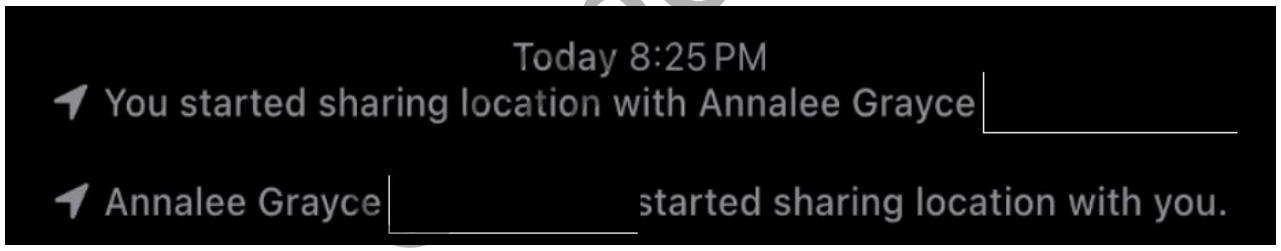
Shares live location	Share/follow multiple devices	Historical location data
• Find My (Apple) • Find My (Google) • Snapchat • Instagram	• Find My (Apple) • Find My (Google)	• Apple Maps • Google Maps • Fitness Apps

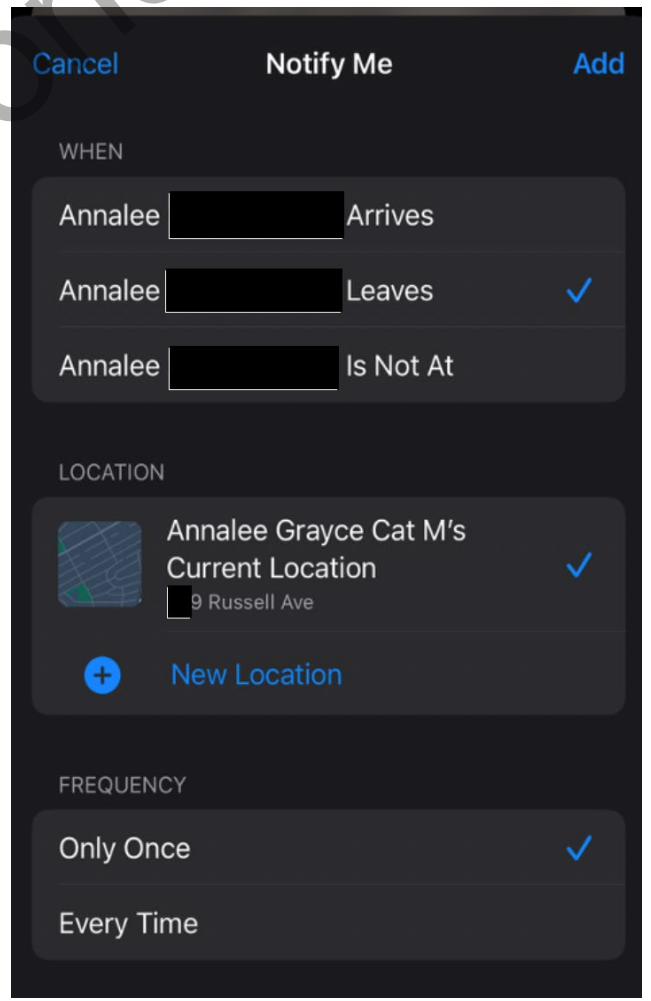
FUNCTIONALITY OF LOCATION SHARING APPS

- Exact/Approximate location and time shared
  - Can get directions to User's approximate location
  - Can set notifications when User's location changes
- Location can be shared with select others for:
  - One Hour
  - 24 hours
  - Indefinitely
- Users can temporarily restrict other Users from seeing their location

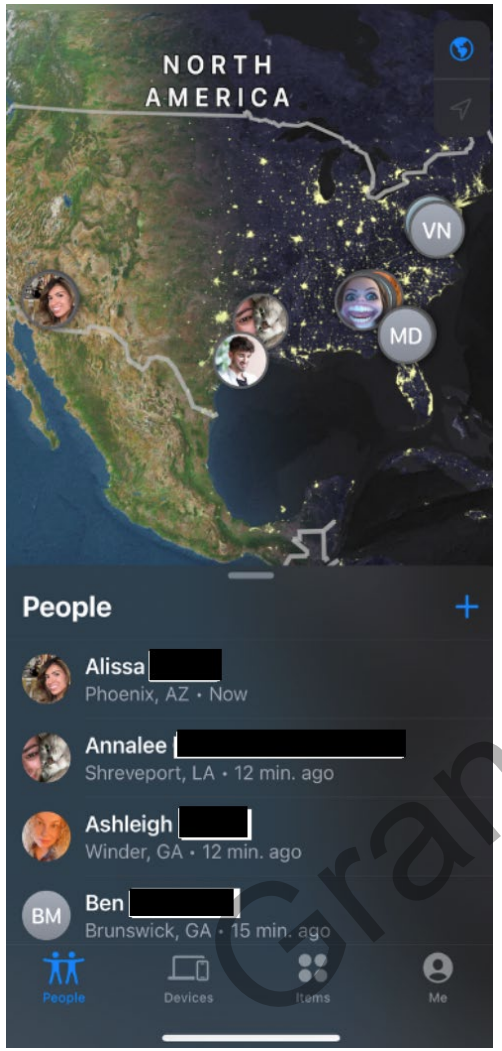
FIND MY FRIENDS (FIND MY IPHONE)

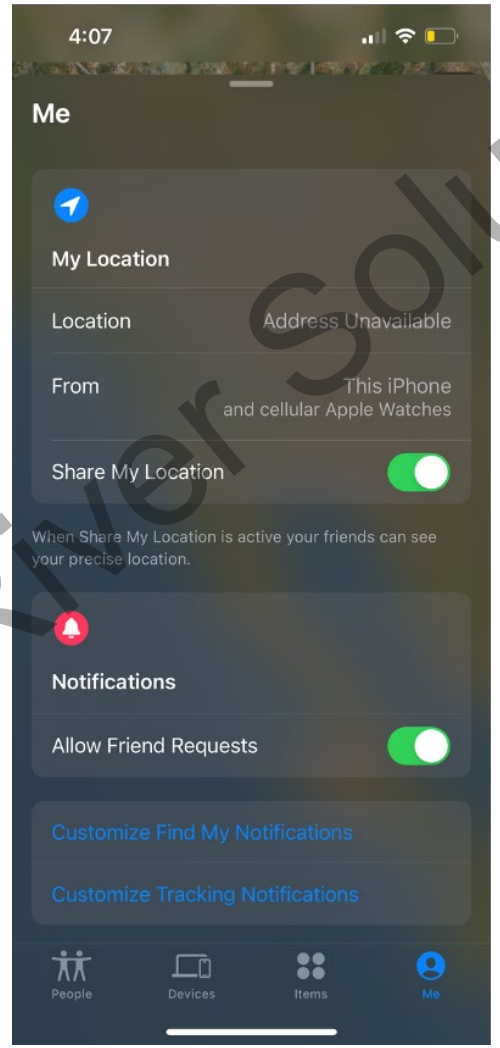
- If User's location cannot be seen:
  - Location not found: Connectivity or device issues
  - Location unavailable: User may have turned off location sharing
- Additional devices (iPad/Apple watches) can skew location data
- When location is shared or removed, a notification is included in the text message thread





FIND MY FRIENDS (FIND MY IPHONE)

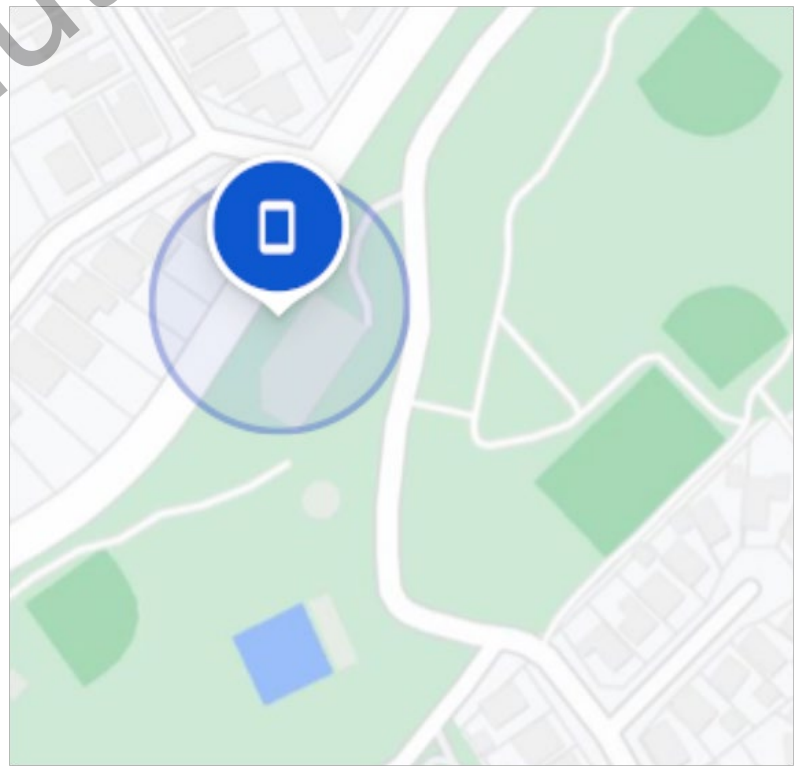




Find My

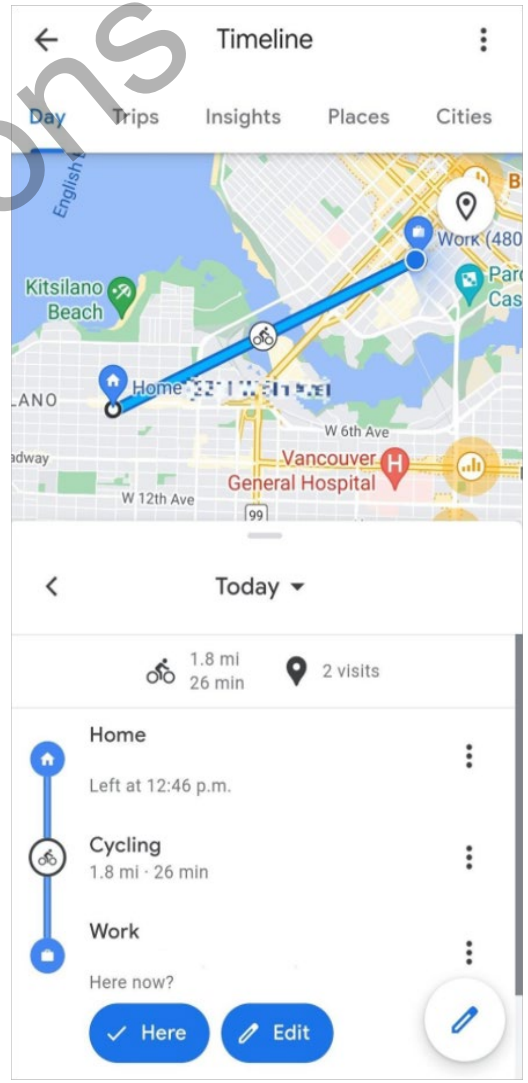
FIND MY DEVICE (GOOGLE)

- User can share device/accessory with up to 10 other Users
  - Recipient must accept or decline invitation within 24 hours
- Option for Primary and Secondary Owners to track singular device without sharing location with others
  - Location and battery level shared with owners



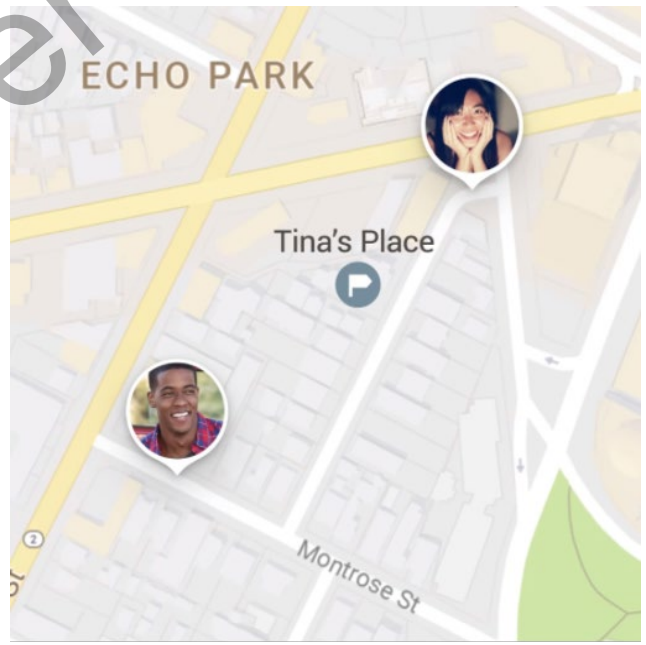
GOOGLE MAPS

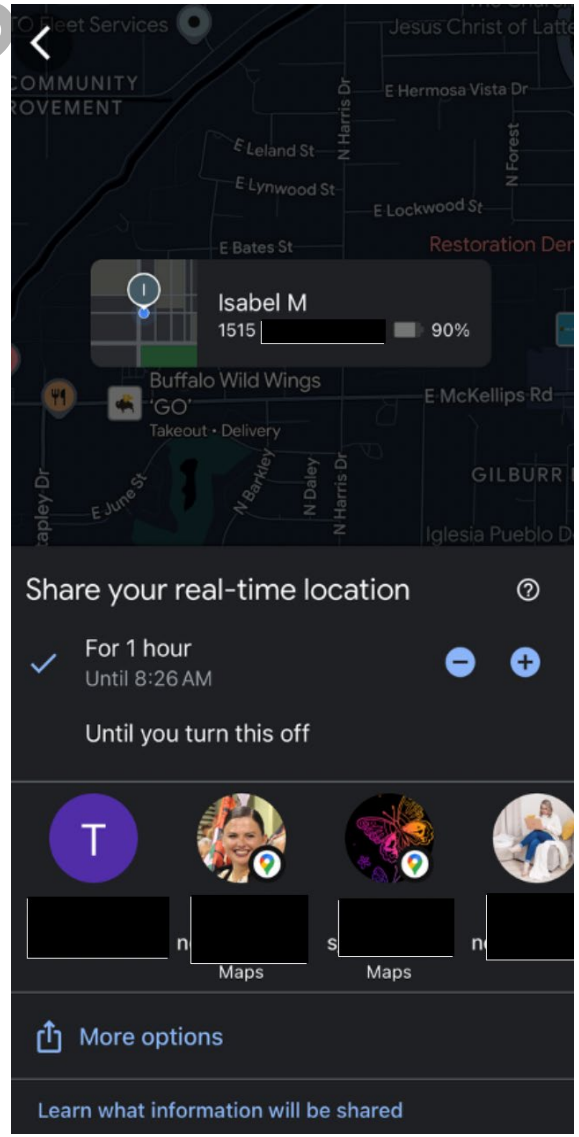
- Timeline Data
- Shows past "visits" (locations) and routes
- Specifies the time spent walking, driving, or taking public transit
- Can be set to auto-delete after set amount of time
- Location, date, and time can be edited by the User
- Location data can be deleted for a set range of time, or all data can be deleted



GOOGLE MAPS

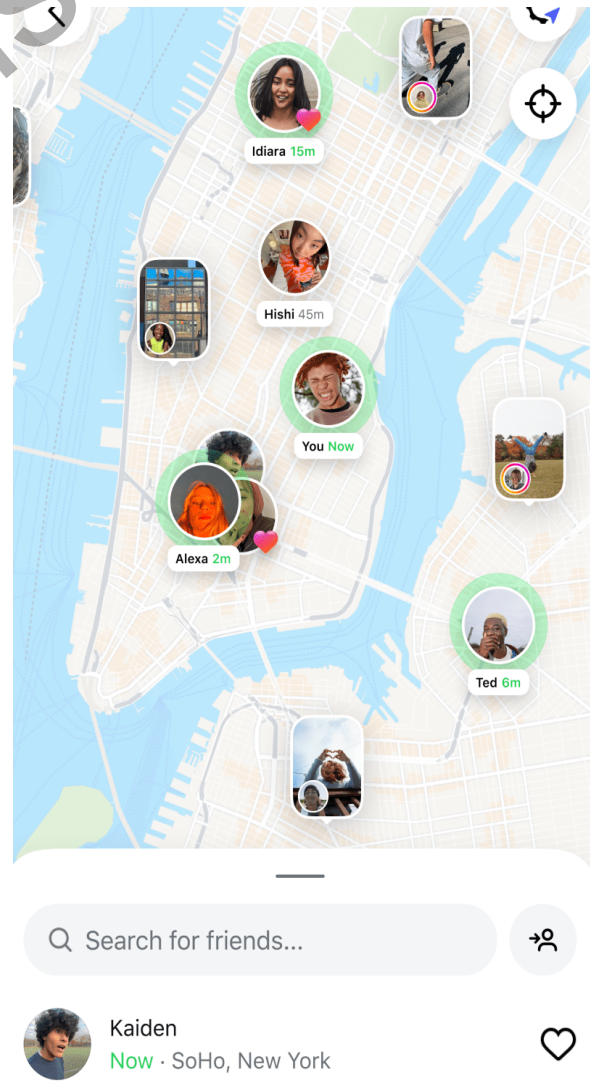
- When location is shared, other Users can view:
  - Name and photo
  - Recent location
  - Device's battery power and if it's charging
  - Location Sharing Notification- if on, shares arrival and departure time





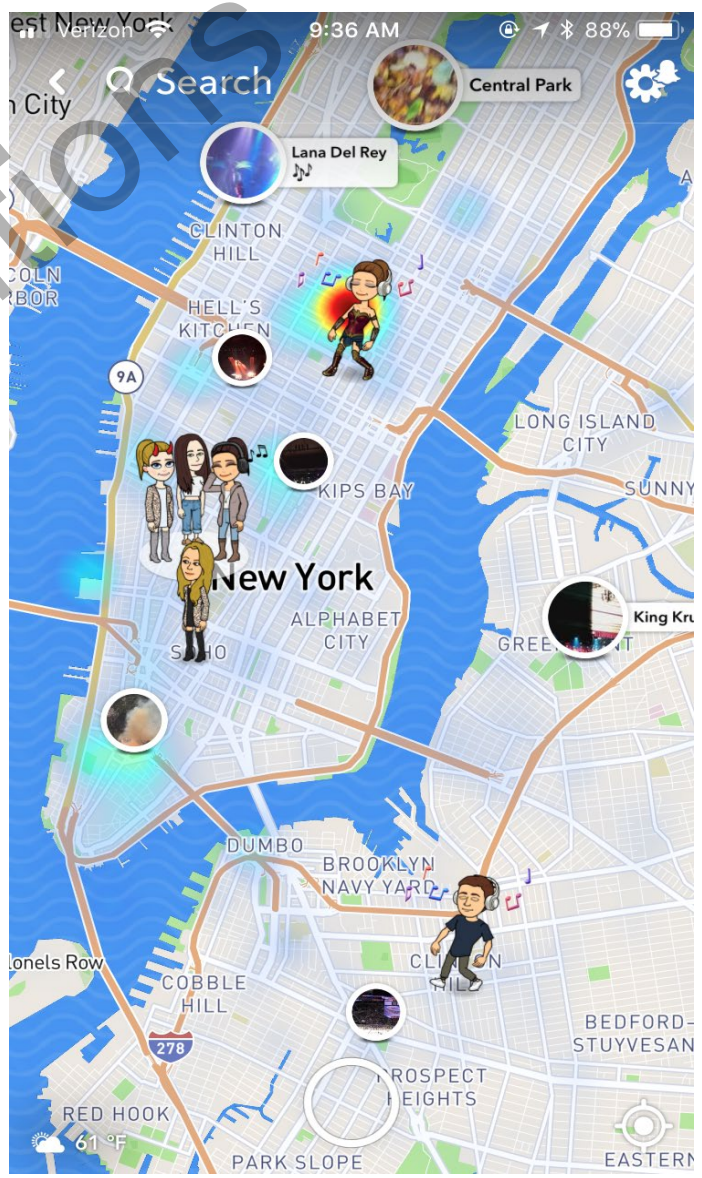
INSTAGRAM

- **Instagram**
  - Share via Instagram Maps feature or directly via DM
  - Can be shared with all friends, "close friends," or select group of Users
  - Can be turned off in phone Settings and directly in Instagram app



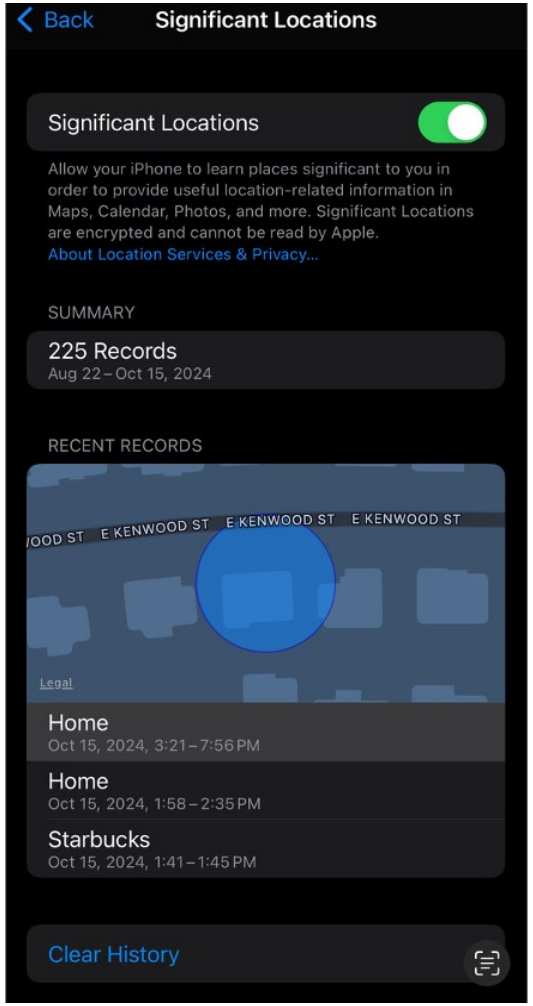
SNAPCHAT'S SNAP MAP

- Swipe right twice on main camera screen to access Maps
- Settings > Privacy Controls > Who Can See My Location
- Location Privacy Options:
  - Ghost Mode
  - My Friends, Except
  - Only These Friends
- Location Options:
  - Always share location updated in real time
  - Only while using (Last known location while app was open)



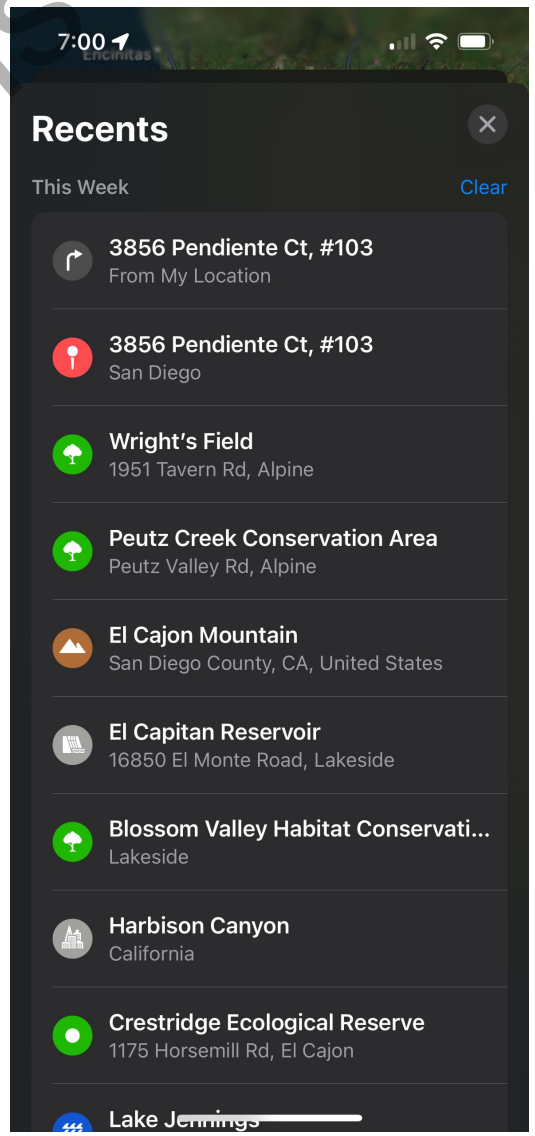
GATHERING DATA FROM LOCATION SHARING APPS

- **Apple Phone:**
- Find My Friends/ Find My iPhone:
  - Settings > Privacy & Security > Location Services > System Services > Significant Locations > Password > Summary
    - Shows Date and Number of Records
  - Full summary of locations cannot be seen
  - Data can be manually changed on phone to see significant locations on/around that date



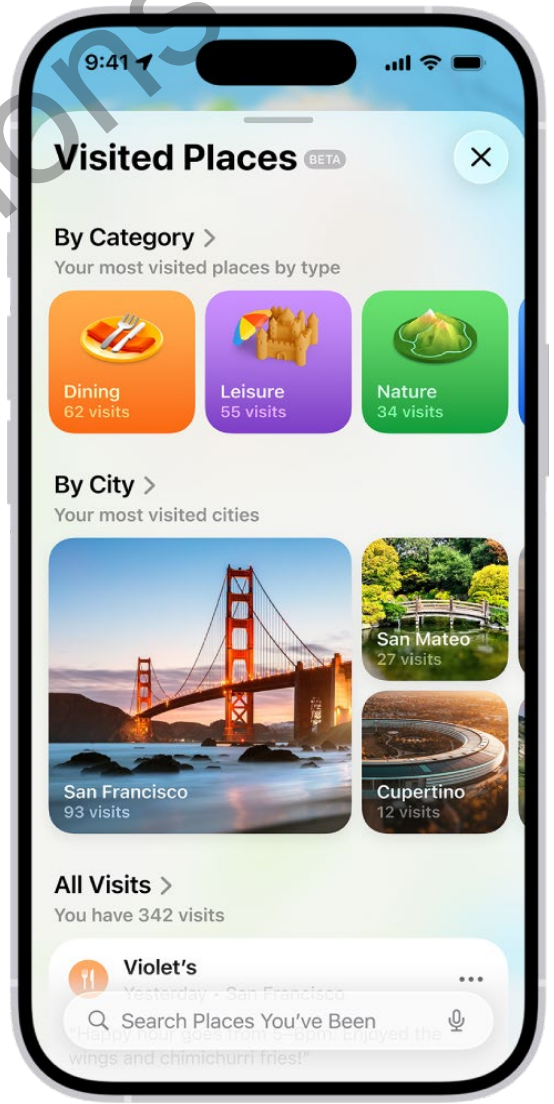
GATHERING DATA FROM LOCATION SHARING APPS

- **Apple Phone**
- Apple Maps -> "Recents"
  - Click search bar to see recently searched locations
  - Limited to specific timeframe or number of visited locations
  - Single items/locations can be deleted by User or entire history can be cleared



GATHERING DATA FROM LOCATION SHARING APPS

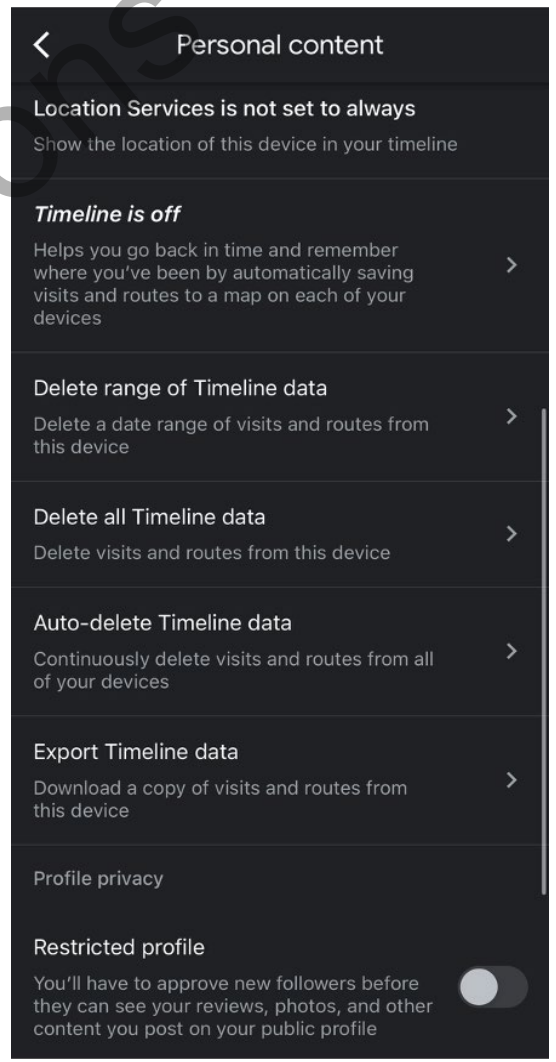
- **Apple Phone**
- Apple Maps -> "Places"
  - Search by name, category, address, or notes
  - "Filter" to filter by date, location, or category
  - "Show all visits"
- Precise location tracking can be turned off in Apple Settings
  - Feature can affect data gathered from location services app



GATHERING DATA FROM LOCATION SHARING APPS

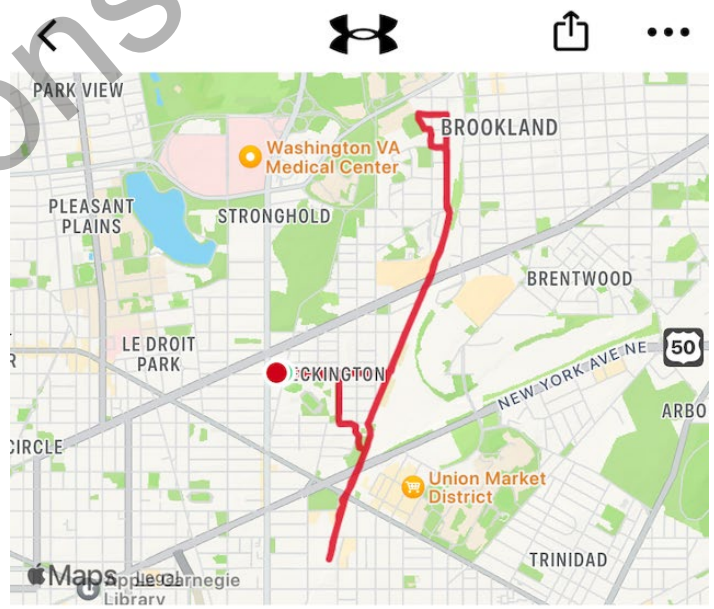
Google Maps

- Can be set to auto-delete after set amount of time
- Location, date, and time can be edited by the User
- Location data can be deleted for a set range of time, or all data can be deleted
- If Web & App Activity is turned off, you can't edit locations or activities on Timeline, but you can delete a day or your entire Location History.
- If Web & App Activity is turned on and Location History is off or data is deleted, User may still have location data saved in their Google Account
- If User's visit to a place is in Timeline, they can find the last time that they visited in Google Maps



GATHERING DATA FROM LOCATION SHARING APPS

- Popular fitness apps, like MapMyRun, Garmin, or Strava, can be used to track someone's location and common routes
- Routes can be shared with friends and followers after workout is completed, saved, and posted
- MapMyRun offers a premium membership that includes live tracking
- Strava offers privacy zones in Map Visibility that hide the start and end points of activities within a specified radius



5.03mi Run

Sunday, Jun 16 at 12:16pm

SUMMARY

5.03	1:01:02
Distance (mi)	Duration

REQUESTING EVIDENCE SCENARIO 2

Alex reports to the Title IX Coordinator that she has concerns that her ex-partner is stalking her. She says that she has noticed her ex-partner showing up in off-campus areas that she frequently trains for an upcoming marathon. Alex shares that she and her ex-partner also trained for the same marathon together, but they stopped running together when they broke up. Alex noted that she started running new routes off campus and was unsure how or why her ex-partner would have knowledge about her new running routes.

- What steps can you take as the Title IX Coordinator?
- How would you handle evidence gathering as the Investigator?

REQUESTING EVIDENCE SCENARIO 3

- Jack reports to Public Safety that during a consensual sexual encounter, Connor recorded the interaction without Jack's consent. Jack was 17 years old at the time of the non-consensual recording of the sexual interaction. Jack is requesting a formal investigation.

- Can the Investigator request the recordings?
- Does the Investigator need to notify Jack's parent/guardian?
- Who can the Investigator contact for support/guidance?
- How should the Investigator move forward?

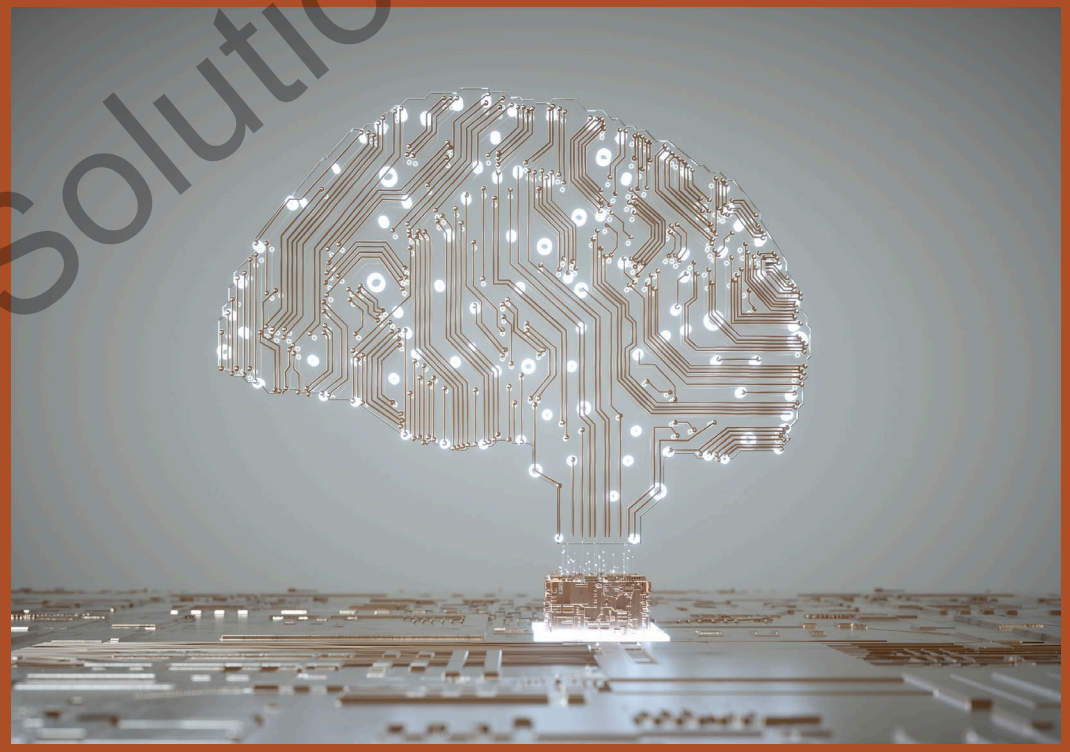
EVIDENCE INVOLVING MINORS

- Handling nudity and child pornography in investigations:
  - Consider the ages of the involved parties
    - Minor? Dual enrollment student?
  - Consider where the evidence is being sent
  - Notify appropriate departments/individuals if you become aware of this type of evidence before requesting a copy of the evidence from the party
    - Laws surrounding possessing, distributing, and producing child pornography include nudity and engaging in sexual acts
    - To avoid possessing or distributing child pornography during an investigation, school administrators should not print, copy, or transfer any sexually explicit photos onto school or personal devices.

ANALYZING EVIDENCE AND METADATA

ARTIFICIAL INTELLIGENCE (AI) IN CASES

- Videos, photos, and screenshots of text messages can be edited by various software programs and AI
- AI and editing software programs are easily accessible



ANALYZING EVIDENCE

Does the evidence accurately reflect the party's description of its contents?

Is the evidence corroborated by one or more other parties/witnesses or other forms of documentation?

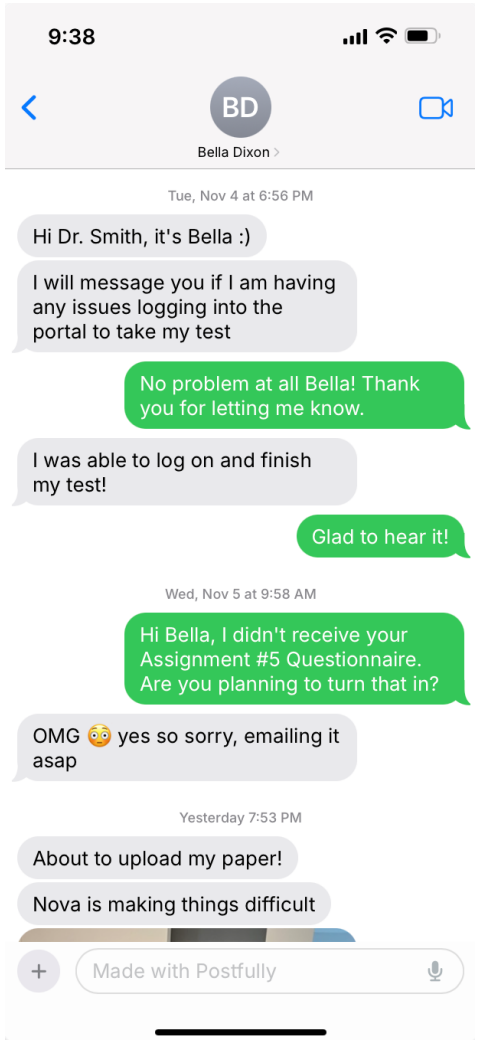
Upon review, do any other parties/witnesses dispute the contents of the evidence?

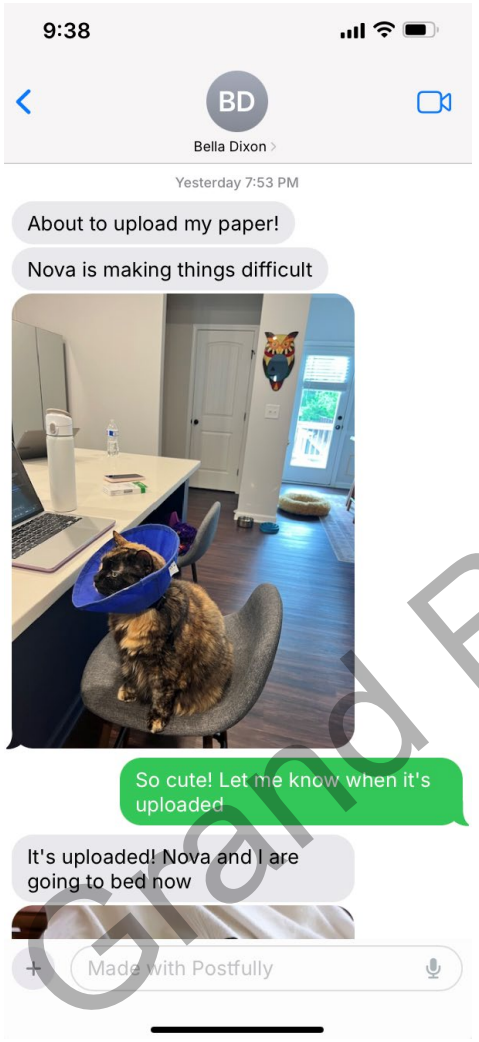
Does the evidence appear to be altered in any way?

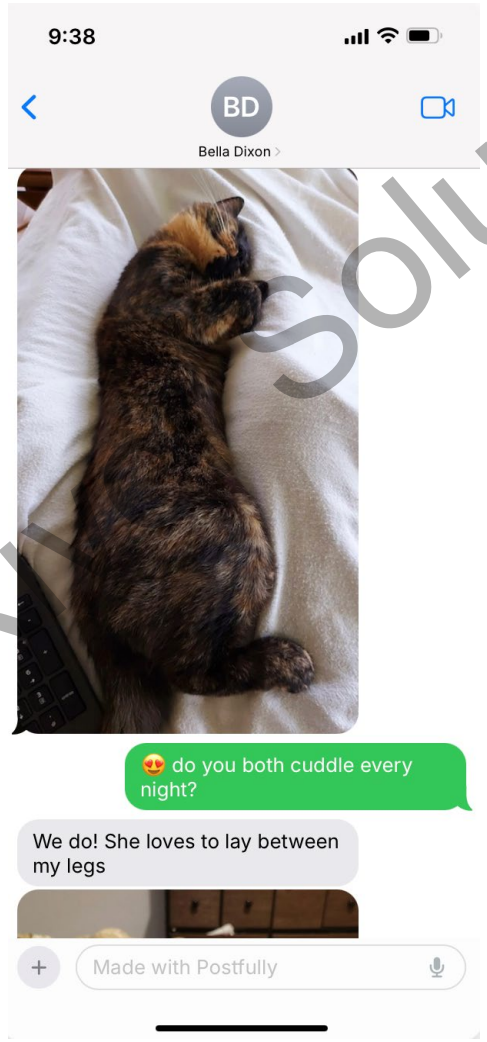
SCENARIO COMPARING ALTERED EVIDENCE

- Student Bella reported that after attending office hours for her Music Theory course, she and the professor, Dr. Smith, exchanged phone numbers. She began receiving messages from Dr. Smith. She stated that at first the messages were related to classwork and small talk. Bella stated that Dr. Smith began asking her inappropriate personal questions, including asking what she was wearing. When you speak to Dr. Smith, they confirm that they had messaged with Bella but disagree with Bella's description of the contents of their messages.
- The Investigator requests the text message screenshots, and the photos sent between the parties.

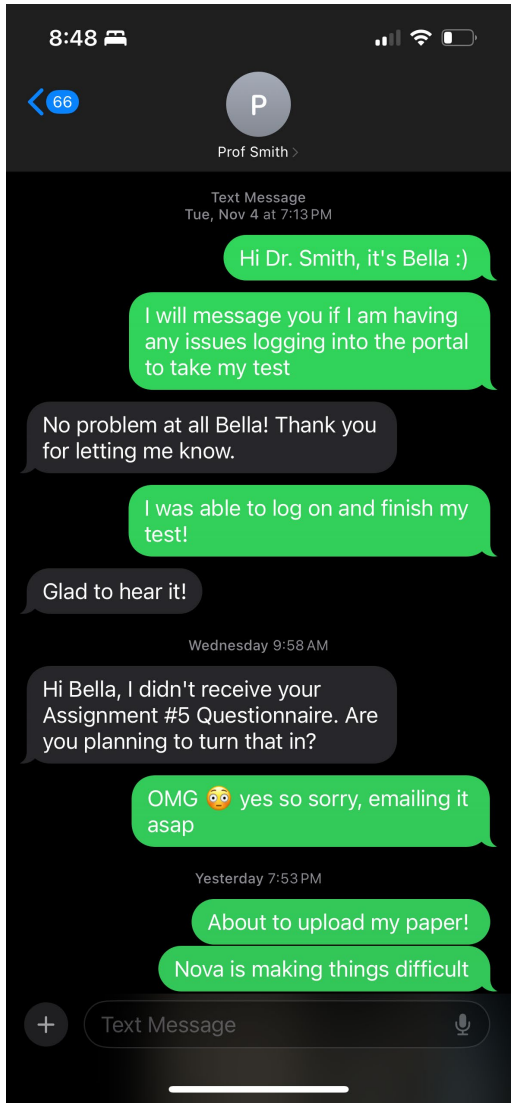
SCREENSHOTS FROM DR. SMITH

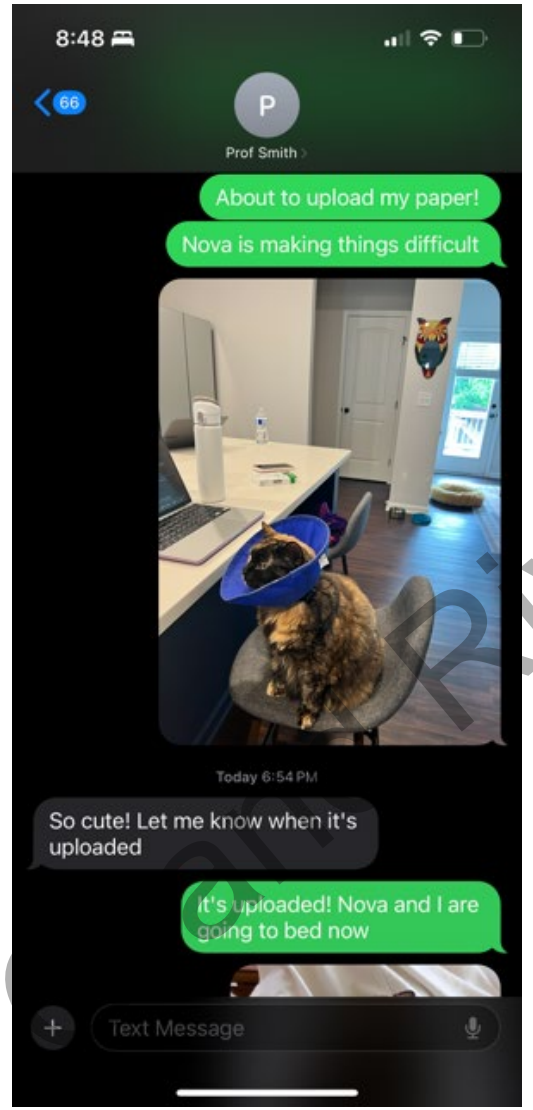


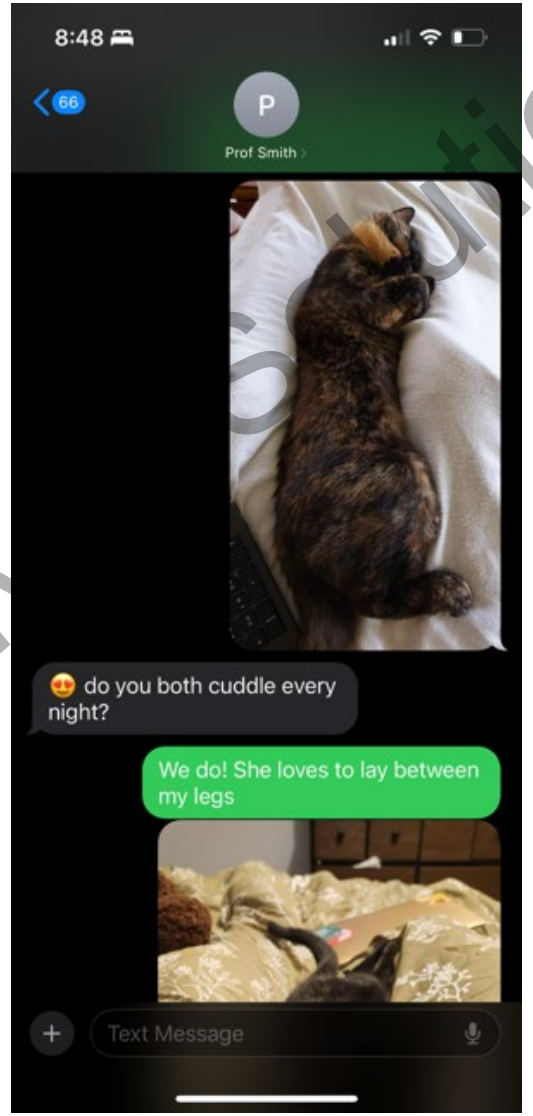


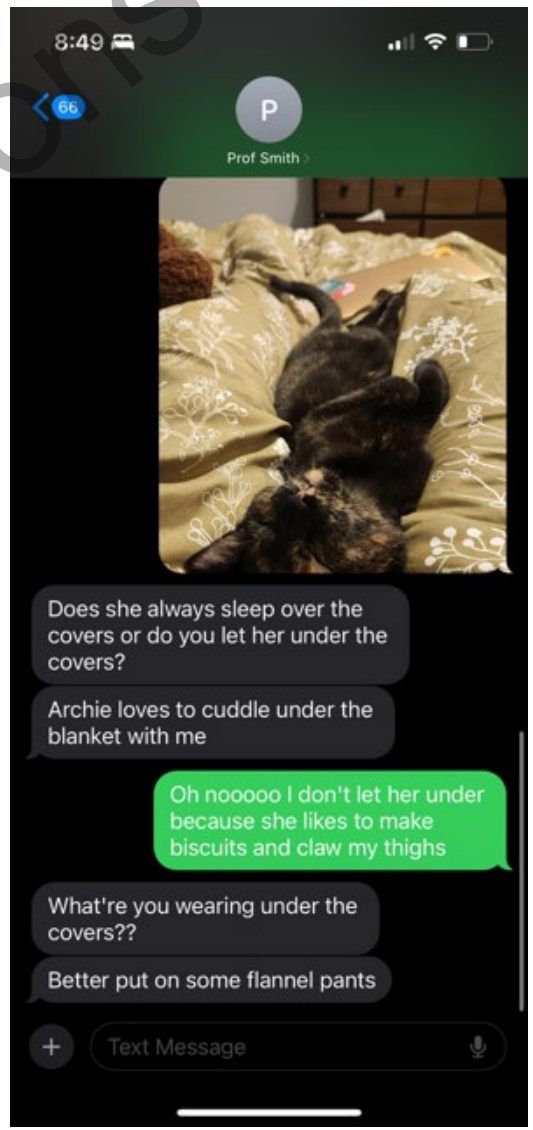


SCREENSHOTS FROM BELLA







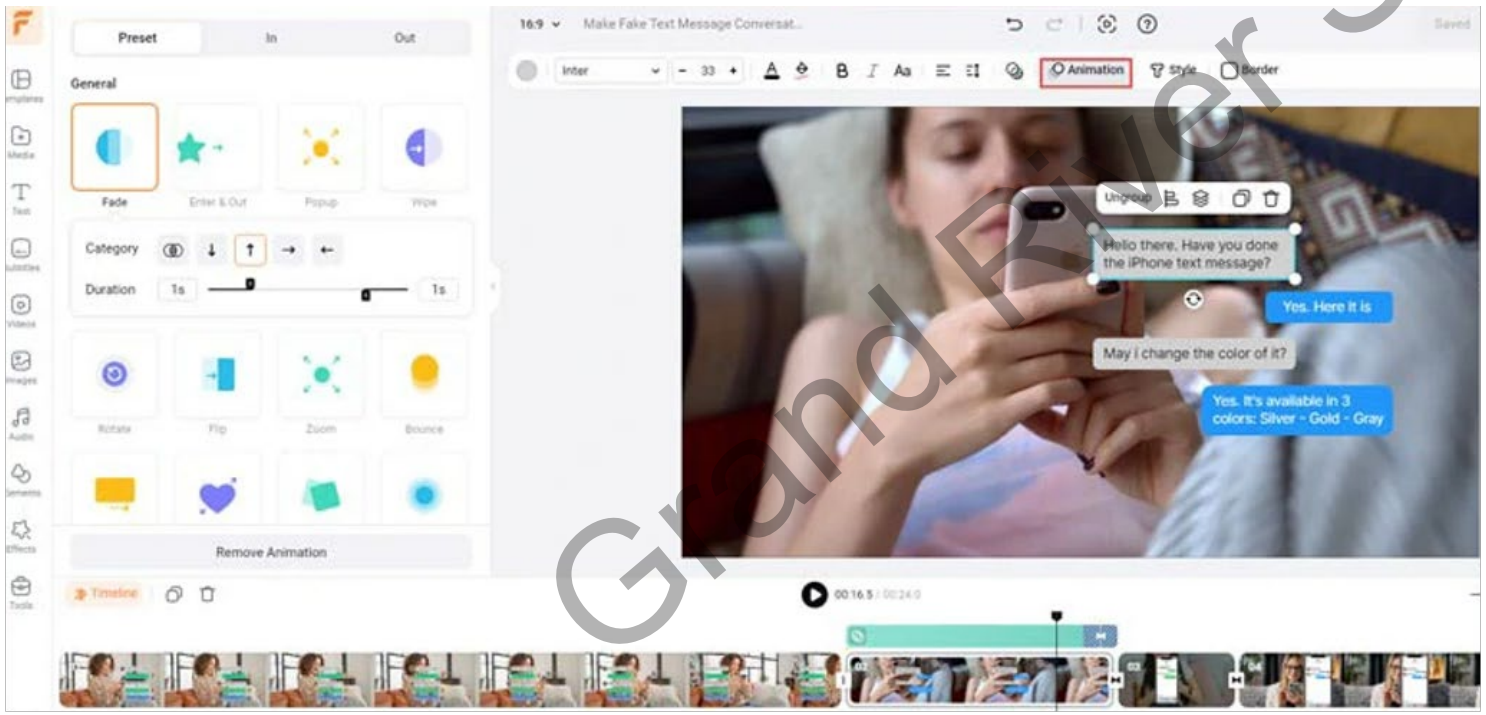


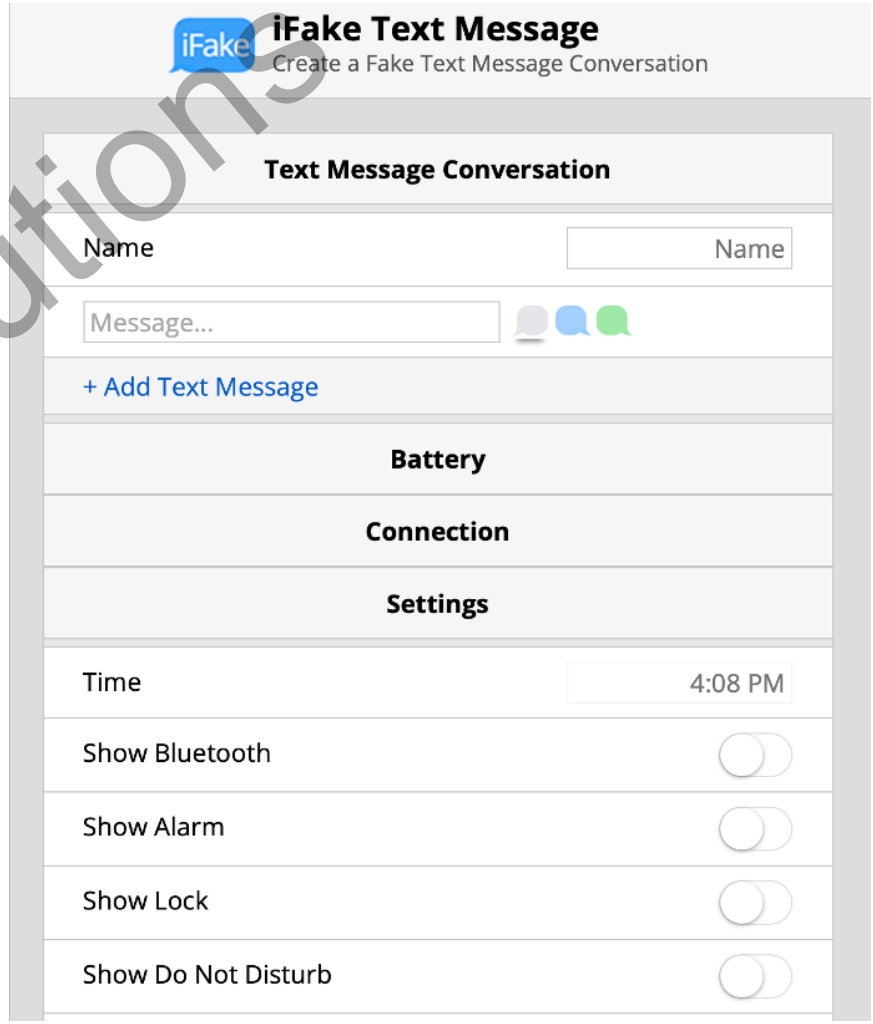
SCENARIO COMPARING ALTERED EVIDENCE

- What differences, if any, do you notice between the screenshots provided by the parties?
- How would you address these differences with the party?
- How can the Investigator verify the evidence submitted by the parties?
  - Request the same evidence from both parties.
  - Compare and contrast the submitted evidence.
  - Review the evidence for any potential edits and alterations.

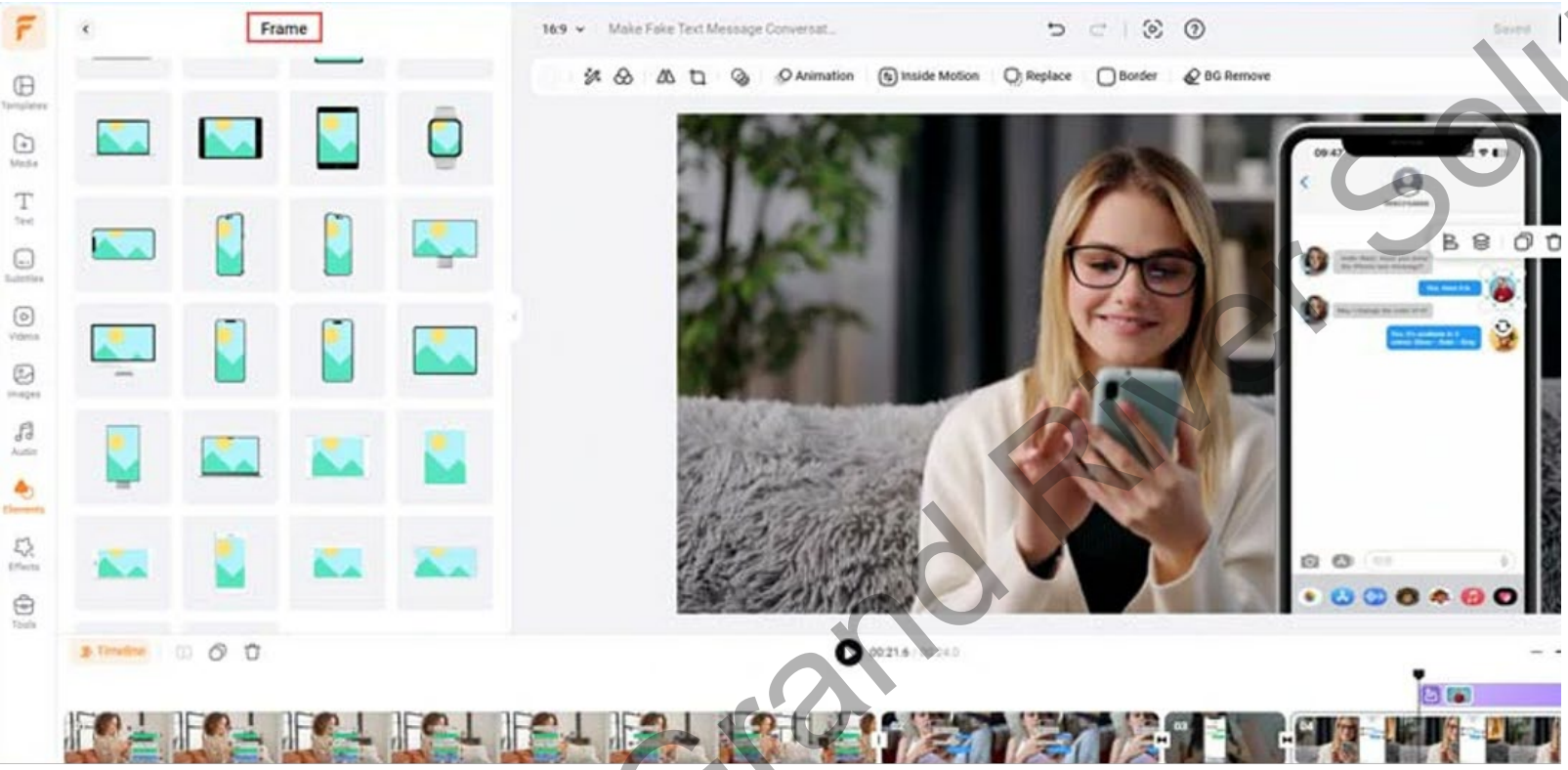
EVIDENCE SUBMISSION

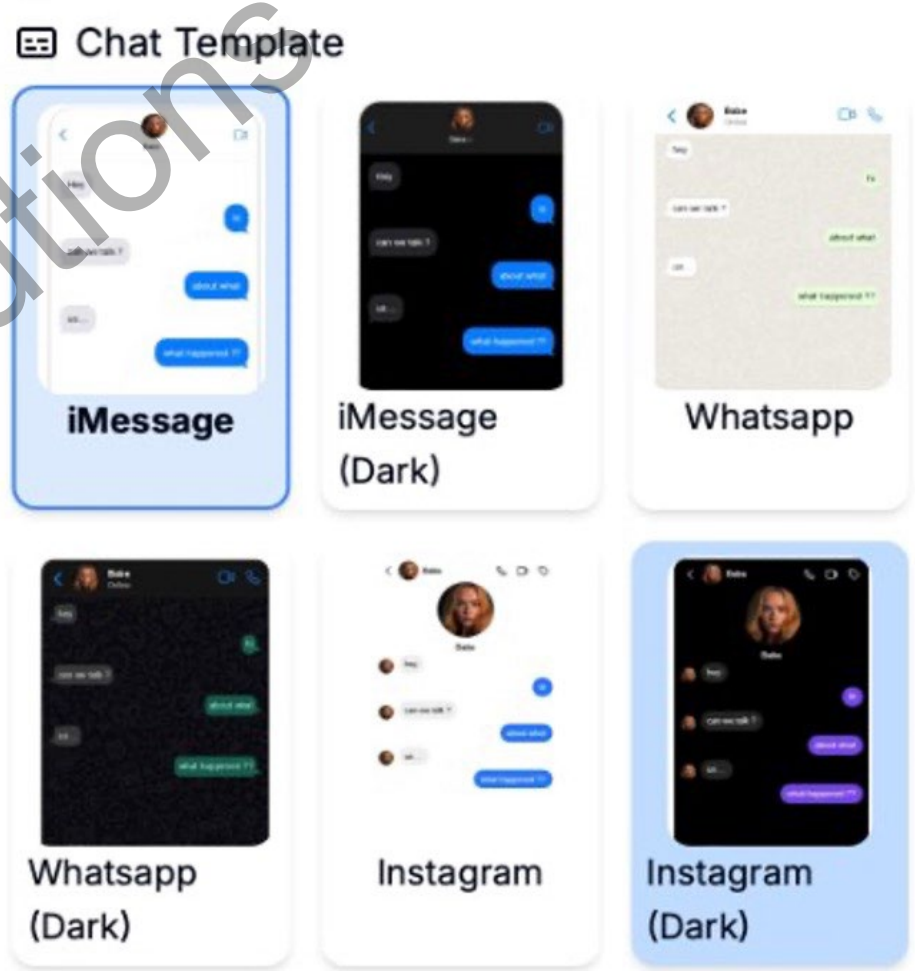
- Online websites and apps to create text and social media messages
  - Fake Text Message and Fake DM
  - AI programs
  - Adobe Photoshop
  - Flexclip



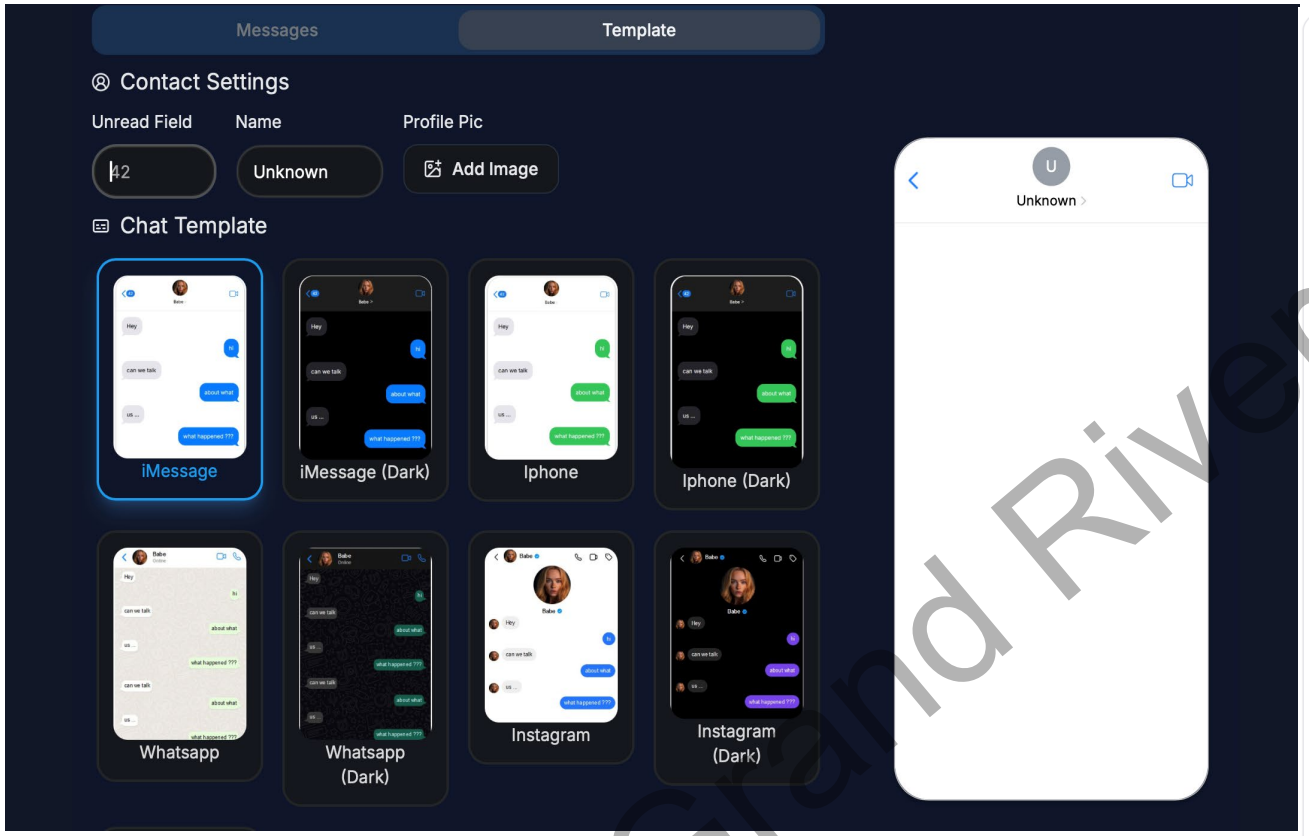


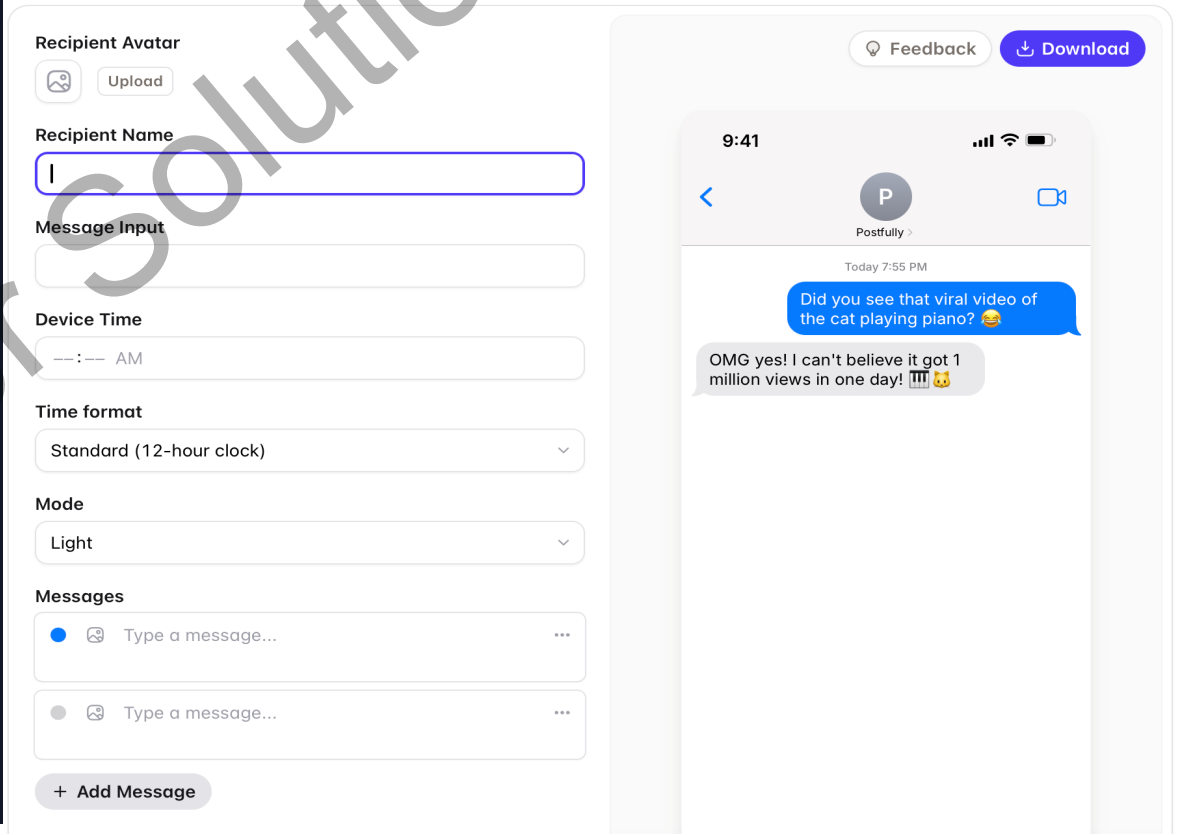
EVIDENCE SUBMISSION



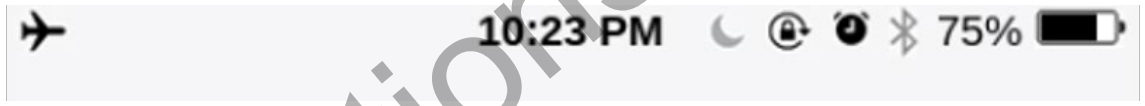


EVIDENCE SUBMISSION



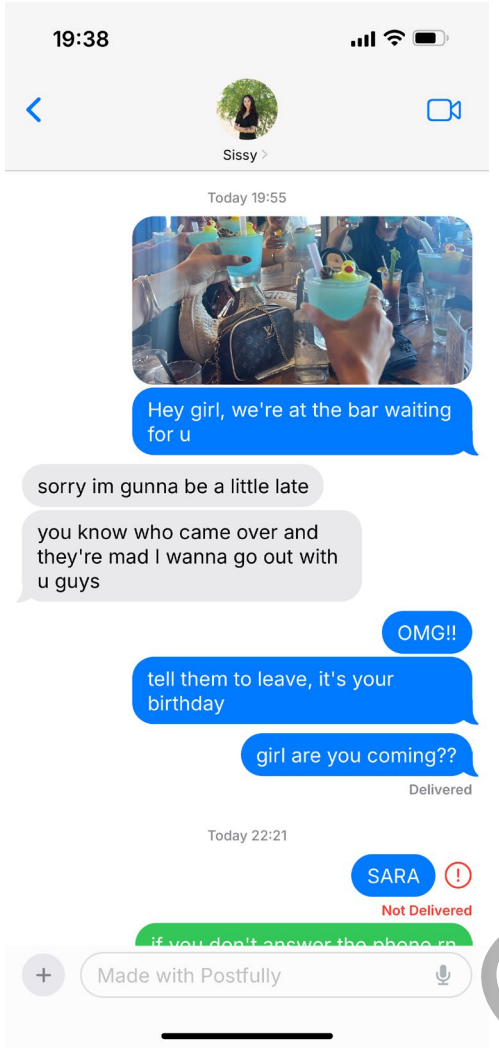


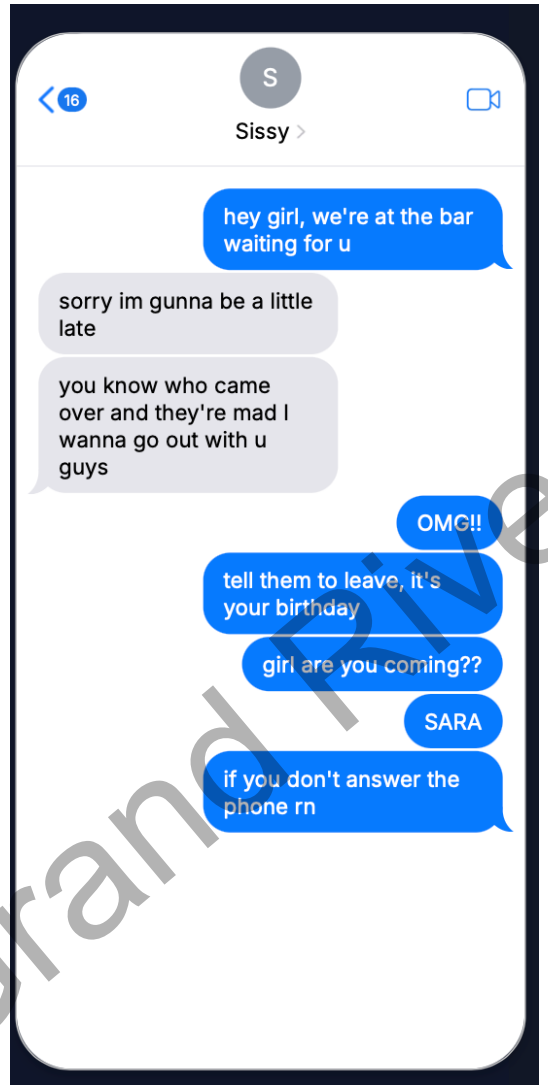
ANALYZING EVIDENCE

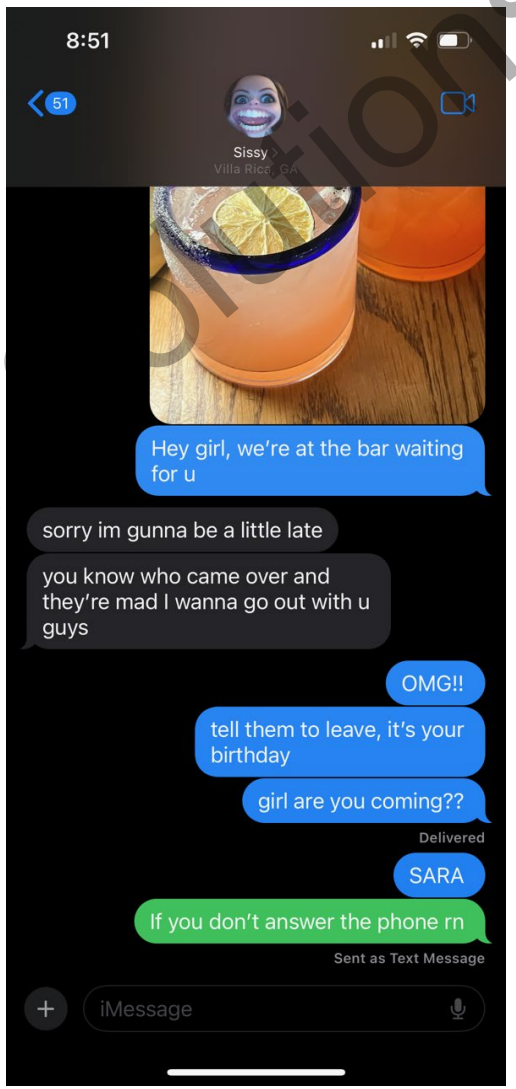


- Identifying fake messages
  - Request message screenshots or screen recording from all individuals included in text thread with corresponding contact cards
  - Verify messages with message/call log from phone carrier
  - Verify contact information
  - Analyze submitted screenshots
    - Timestamps and message flow
    - Operating system details and app interface
    - Uneven spaces between messages
    - Bubble size and color
    - Color around text- does it match? Borders?
    - Font

ALTERED MESSAGE COMMUNICATION



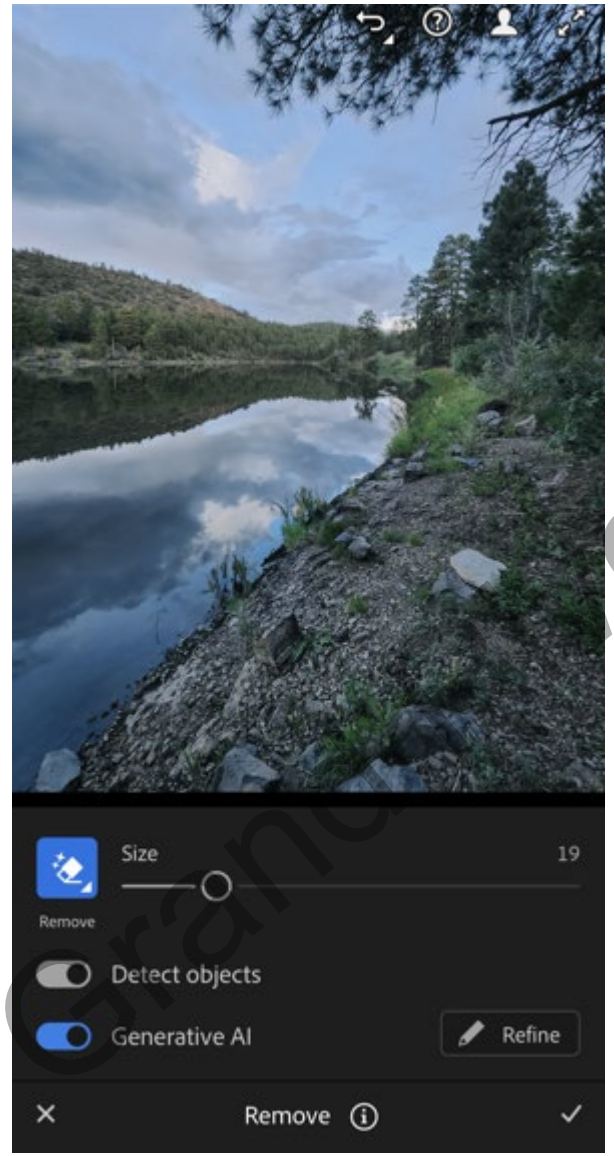


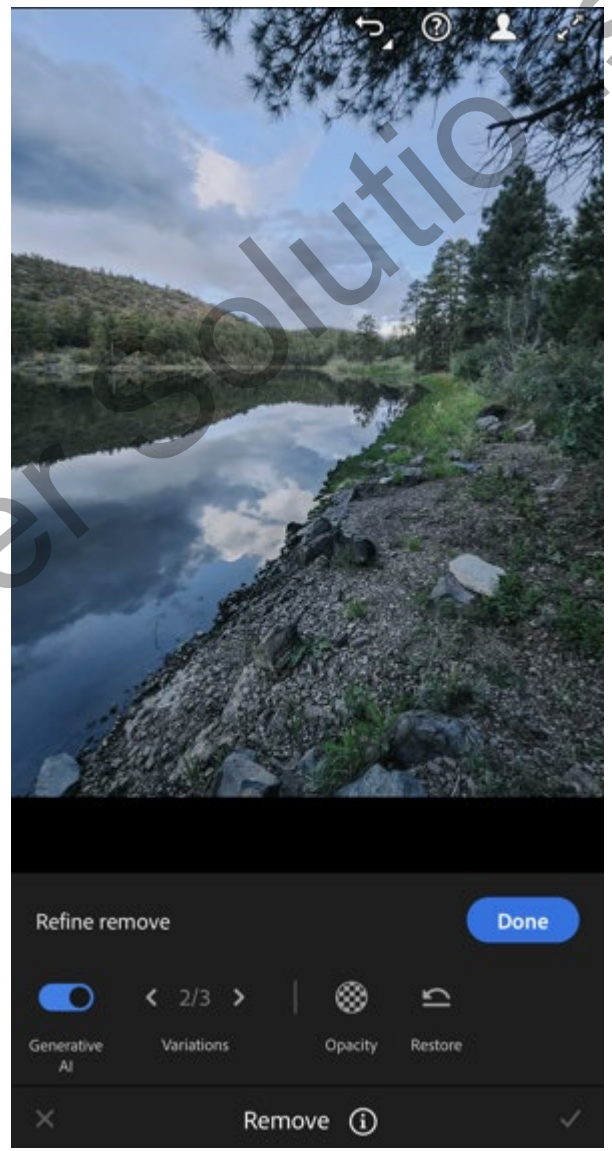


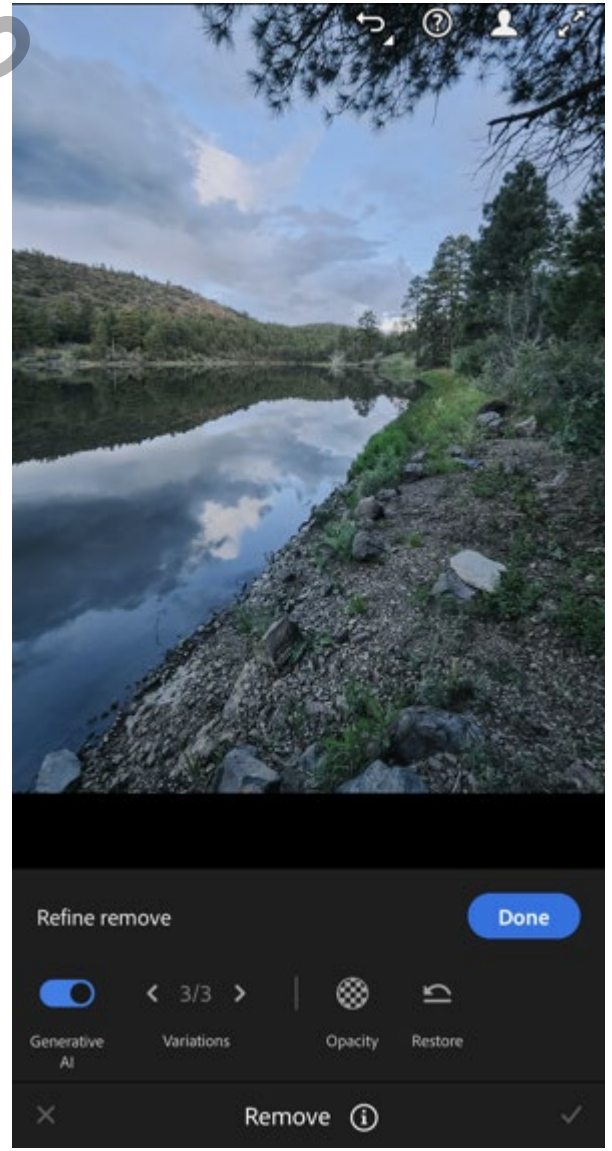
ANALYZING EVIDENCE

- Identifying edited photos
  - Analyze inconsistencies in lighting, shadow, highlight, perspective, orientation, warping, and reflections in image
  - Analyze pixel anomalies and compression variations (details are too blurry, too sharp, or pixelated in areas)
  - Check photo metadata and EXIF (creation date, file size, author, GPS coordinates, camera settings, etc) in photo properties
    - Metadata can be edited or erased
  - Edit > Revert back to original > Save a copy
  - Adobe Photoshop forensic tools or other programs to detect edits
  - Reverse image search

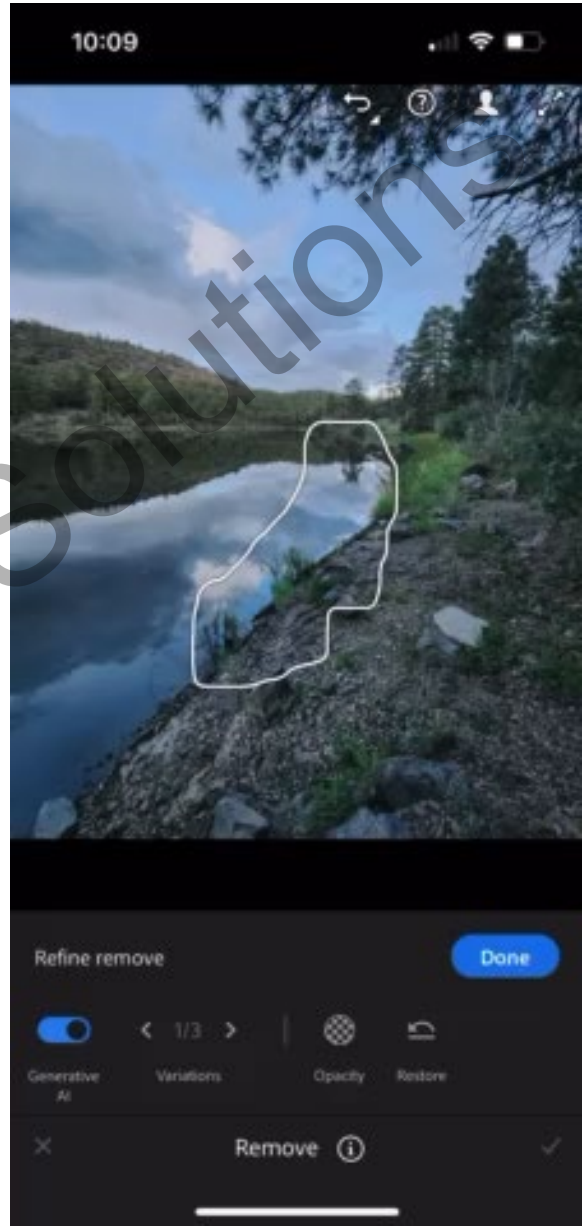
ANALYZING EVIDENCE





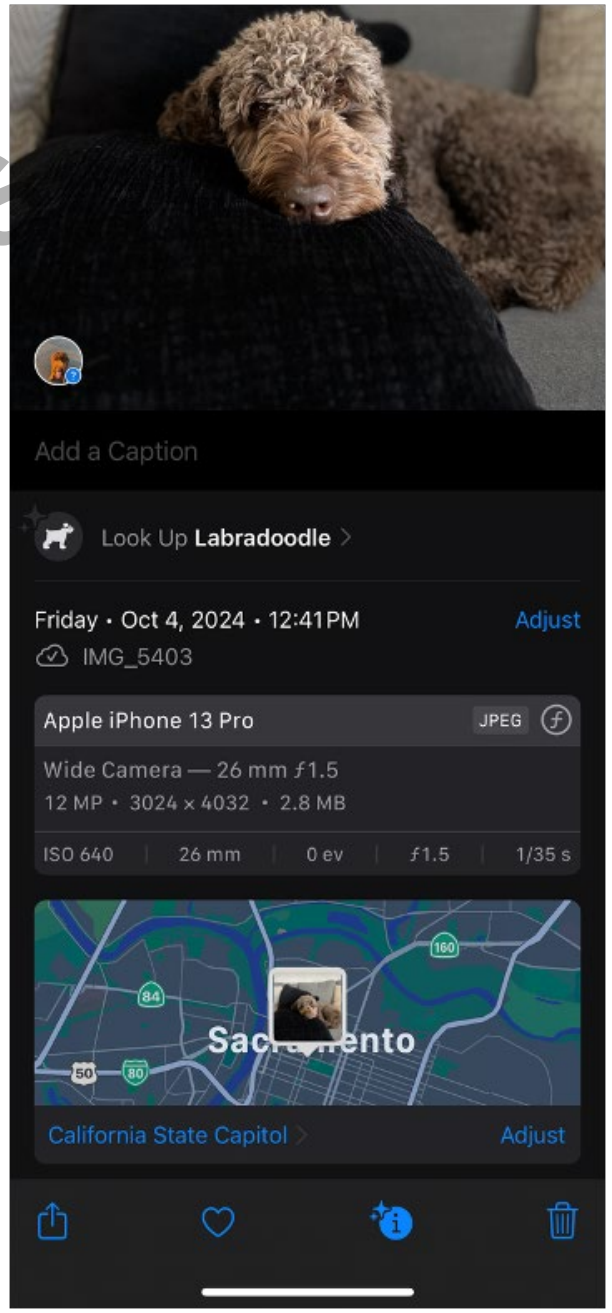


ANALYZING EVIDENCE



ANALYZING METADATA

- Photo/video metadata is embedded information in digital image
  - Date, time, and location
  - Aperture, shutter speed, ISO
- Metadata can be turned off in settings
- Certain types of metadata can be edited after a photo or video is taken
  - Date and time
  - Location



GENERATIVE AI – VERIFICATION AND CREATION

- There is no one way to identify AI generated photos and videos, however, there are different techniques that can be used.
- AI Video Generator
  - Google Veo 3 and Google Gemini
  - Kling AI
  - Seedance
  - Hailuo Minimax
  - Runway Gen 4
  - MetaCreate
  - Artlist.io
  - ChatGPT
  - Adobe Firefly

ANALYZING EVIDENCE- AI

- Look for physical anomalies or discrepancies
  - Vanishing point
  - Shadows
  - Warping
  - Reflection of objects in image (window, water, mirror, etc)
  - Object permanence and space
- AI generators alter the noise residual in photos
  - Noise residual: Visual distortion (graininess, discoloration) in the photo
  - AI uses the noise patterns in one image to generate a new image

ANALYZING EVIDENCE- AI

- AI Videos
  - Unnatural facial expressions
    - Movement of lips if person is speaking
  - Unnatural eye movements
  - Perfectly symmetrical faces
  - Unique individual characteristics (tattoos, birthmarks, etc)
  - Check fingers and hands
    - Stiff hands
    - Unnatural movement
    - Too many or too few fingers
  - Object permanence, space, and movement

AI GENERATED "DEEP FAKE" VIDEOS AND PHOTOS

A mother allegedly used explicit deepfake photos and videos to try to get her teenage daughter's cheerleading rivals kicked off the team.

Two more families later came forward after receiving similar messages.

Raffaela Marie Spone was arrested and charged with harassment and cyber-harassment

AI GENERATED "DEEP FAKE" VIDEOS AND PHOTOS

- Questions to establish motive and intent
  - Recent break-up
  - Direct threats to create or distribute content
  - Access to software/knowledge of creating AI generated content
- Likeness to Complainant's face and/or body parts
  - Ask who the content was meant to look like (if Respondent's statement is that they created the content but it was not meant to look like Complainant)
  - Tattoos or other identifying features
- Determining how/if Respondent distributed images/videos
  - IP address tracking
  - Assistance from law enforcement and other resources

ADDRESSING DISCREPANCIES IN EVIDENCE

1. Review evidence submissions with both parties
2. Include all versions of the evidence in the report documentation
3. Include party/witness responses to evidence discrepancies in report documentation

ADDRESSING DISCREPANCIES SCENARIO

GRS University initiates a formal investigation regarding allegations of sexual harassment and stalking. Both the Complainant and Respondent have submitted screenshots of their conversations with one another to Investigator.

In Complainant's screenshots, Respondent can be seen repeatedly asking where she is and telling her that she sees Complainant, with no response from Complainant. In Respondent's messages, some of the same messages are worded differently and Complainant can be seen replying to the messages.

- How would you address this with each party?

ADDRESSING DISCREPANCIES SCENARIO

Complainant

- Did you reply to any of Respondent's messages asking where you were?
- Did you delete any of your or Respondent's messages?
- Did you edit any of your or Respondent's individual messages?

Respondent

- Did you edit any of your or Complainant's individual messages?
- Did you delete any of your or Complainant's messages?

ADDRESSING DISCREPANCIES

Ask direct questions and point to specific elements of evidence

Are there any other differences between the two versions of submitted evidence that you noticed?

Ask if the evidence was altered

Request to see their device in person if possible

DISCLOSURE OF EVIDENCE ALTERATION

1. Ask questions to determine how altered evidence affects the allegations and possible finding of a policy violation
2. Request copies of unaltered evidence
3. Include in report documentation as appropriate

REVIEWING EVIDENCE WITH PARTIES

- Evidence may be shared with the parties during the investigation or during the evidence review period
- Prepare evidence for review by party
  - Redact evidence prior to review if appropriate
- Create separate file folder to be accessed during interview

DISCLOSURE OF EVIDENCE ALTERATION

- Refer to policy for next steps of process
  - Is the party admitting to fabricating their allegations?
  - Is the party admitting to engaging in a policy violation?
  - How does the altered evidence affect the substance and details of the allegations?
- Notify parties of the inclusion of the information into the report and next steps of process
  - Include in party summary, summary of evidence, credibility assessment, evidence appendix (as appropriate)

EVIDENCE SHARING IN THE REPORT AND HEARING

DOCUMENTING ALTERED EVIDENCE

Altered by party/witness

- Include original and doctored evidence
- Include specific statements by party/witness regarding disclosure and response
- Document thoroughly
- Hearing Officer asking in hearing if they believe any evidence has been doctored

Altered by Investigator

- Partial and intentional blurring of private body parts
- Summarization of evidence by objective individual
- Document thoroughly in report

EVIDENCE REVIEW (HOW TO MANAGE SENSITIVE DATA)

- Allow parties to schedule time in person to view the file in your office
- Allow parties to schedule time to view file virtually
  - Certain devices will allow the parties to screen-record without your notice
- Share via secure file-sharing platform
  - Limits party's ability to share, copy, print, or save report documentation
  - Limit timeframe of access
- Add watermark to evidence and report documentation
- If manipulated by Investigator, document thoroughly and provide explanation (e.g. Blurring of private body parts for privacy/sensitivity)
- Sensitive evidence summarized by reliable and objective party (e.g. law enforcement)
- Thoroughly document if evidence is shared differently with the parties and Decision-Maker(s)

DATA MANAGEMENT

- Consider how the evidence is being stored and shared by the school and who may have access to it
- Consider how the report documentation and evidence can be copied, screenshotted, or screen-recorded
- File retention for large files
  - Often have many pictures or videos
  - Secure online file retention

DATA MANAGEMENT

- Ages of participants/subject in photos
- How data is shared across campus
- Metadata can be lost when saved or accessed across various apps and software programs

DATA AND FILE MANAGEMENT

- Users may need to download specific software to access data files requested from apps (Snapchat, Hinge, Instagram, etc).
- Altering file type
  - Save original
  - Save copy of original and save alternate as other file type
  - Online file converters and computer applications
    - For example, iMovie on Apple computers

SHARING EVIDENCE IN THE HEARING

- Prepare evidence in separate folder with labels reflecting evidence identification in report
- Redact evidence
- Summary of sensitive evidence by impartial individual

EVIDENCE RELEVANCE AND WEIGHT

CREDIBILITY

- Credibility
  - What are the differences between the altered evidence and unaltered evidence?
  - Is the evidence inherently plausible?
  - Did the person openly volunteer information that is prejudicial to themselves or a party?

RELIABILITY

- Reliability
  - Did the party omit material facts/information? If so, what and why?
  - Did the party admit to altering evidence? How was the altered evidence discovered?
  - If the party did not admit to altering the evidence, how did the party respond to questions about altered evidence?
  - Is the evidence corroborated by witness/party statements or other documentation?
  - Does the party have a motive to falsify?
  - Did the party alter or omit multiple pieces of evidence?
  - Did any other participating individuals have knowledge of the altered evidence?

RELEVANCE AND WEIGHT

- How does the altered evidence impact the:
  - Reliability and credibility of the party/witness's statements
  - Reliability and credibility of any other evidence submitted by the individual
  - Reliability and credibility of witness statements
    - Did they appear to have knowledge of the altered documentation?
    - Does another individual's statements corroborate the altered documentation?
  - Material facts of the allegations

WEIGHING DIGITAL EVIDENCE

- Party reliability and credibility
- Statements made in the hearing
- Statements made in the investigation
- Internal consistency

AI GENERATED PHOTOS AND VIDEOS

- Party reliability and credibility
  - Motive/ Intent
- Statements made in the investigation and hearing
- Likeness to Complainant's face and/or body parts
- Determining how/if Respondent distributed images/videos

DETERMINATION AND OUTCOME

- Consider the following in the rationale using the evidence standard:
  - How altered evidence impacted material facts of allegations
  - How altered evidence impacted party/witness credibility
  - How altered evidence impacted party/witness reliability

- May need to add opportunity for in-person review of any new evidence accepted in the hearing prior to appeal deadline

APPEALS

Procedural irregularity that affected the outcome of the matter

Newly discovered evidence that could affect the outcome of the matter

Title IX personnel had a conflict of interest or bias, that affected the outcome of the matter

NEW INFORMATION GROUND

- Remember, data requests may be responded to after a long wait
- Newly presented information in a hearing must come with an agreement to accept or an opportunity to review
- The newly available information should not have been available to be shared by the party with investigator
- May include information from a new witness to the digital evidence

LONG TERM STORAGE

- Follow your campus retention policy
- Minimally, must keep for 7 years
- How to address FERPA and FOIA requests in the future
- Ensure you secure digital evidence in a private/encrypted database or similar

APP AND DEVICE UPDATES

Device and app updates and operating systems affects

- Downloading app/device updates
  - Wait to download updates and review resources prior to downloading
- Resources
  - Review update statements from app or social media site
  - Videos posted on apps reviewing updates by social media Users

SOCIAL MEDIA/APP USE AND MENTAL HEALTH

- 69% of adults and 81% of youth use social media
- Social media use is connected to the release of dopamine in the brain
- Social media use is tied to sleep interruptions
- Increased exposure to harm, social isolation, bullying, depressive symptoms
- Decrease in in-person interactions
- Cyberbullying can increase depressive and anxiety symptoms
- Those with depressive symptoms are often targeted

SOCIAL MEDIA AND MENTAL HEALTH

- Many users who experience mental health concerns turn to social media to share experiences or seek information and support
- Can increase engagement and retention in community support
- Can increase social interaction for those normally disengaged

PREVENTION AND SELF-CARE

01

The whole community

02

Those in high-risk situations

03

Those directly impacted or harmed

PREVENTION MESSAGING

- Educate your community on issues
  - Use of AI to create images
  - Extortion over social media
  - "Outting" of dating app users
- Provide multiple avenues to report
  - Decrease barriers to reporting conduct
  - Increase avenues to connect with support
- Work with campus/local law enforcement on digital evidence issues
  - Issues involving blackmail, threats, minors
  - Limit the number of personnel retaining copies of digital evidence

SELF CARE ON SOCIAL MEDIA

- Flood the algorithm with positivity
- Self-Monitoring
  - Limit to 10 minutes a day, which can reduce loneliness and depression
  - Self-Awareness and monitoring use, even without limitations, decreases anxiety and FOMO (Fear of Missing Out)
- Deleting Apps
- Recognize that everyone has an online "persona"
- Prioritize in person connections

QUESTIONS?

COMPLIMENTARY SUBSCRIPTION

CONNECT WITH US

info@grandriversolutions.com

/Grand-River-Solutions

/GrandRiverSolutions

/GrandRiverSolutions

Grandriversolutions.com

GRAND RIVER | SOLUTIONS

WE LOVE FEEDBACK

Your Opinion Is Invaluable!

Case Management Software

Designed for you, by people like you

We are experts and practitioners working in response and resolution for discrimination, harassment, & equity concerns.

Case Tracker allows you to:

- track and manage your cases
- communicate with campus stakeholders without compromising case privacy, and
- provide parties with the ability to follow the status of their case

Schedule a Demo