



Private Until Presumed Guilty

- Or How the 4th Amendment
Doesn't Protect Your
Data in a Post-
Dobbs World



Agenda

Laws don't protect you

Digital investigations of phones

Laws still don't protect you (the cloud edition)

Digital investigations of the cloud

Conclusion

Disclaimers:

- We are not your lawyers
- We are not providing advice on which apps to use/not use
 - Some apps tested offer additional privacy protections we did not test or call out (data deletion from app, data deletion from cloud servers)
 - But again, these are optional settings and we are not providing advice on how to configure apps
- The phone and cloud data is test data (not associated with a real person or real reproductive status/cycle) or self-collected data. Several legal examples have been edited to preserve the technical language while protecting the identities of our clients.



- These methods are already being used to prosecute all kinds of crimes
- Dobbs laid the groundwork for *increased* criminalization of pregnant people
- Any increase in criminalization will always simply be an extension of the existing criminal legal system
 - low-income women are particularly vulnerable to these state actions*
 - pregnant African American women are significantly more likely to be arrested*
 - 56% of cases involved people living in poverty**
- Law enforcement learns from other law enforcement

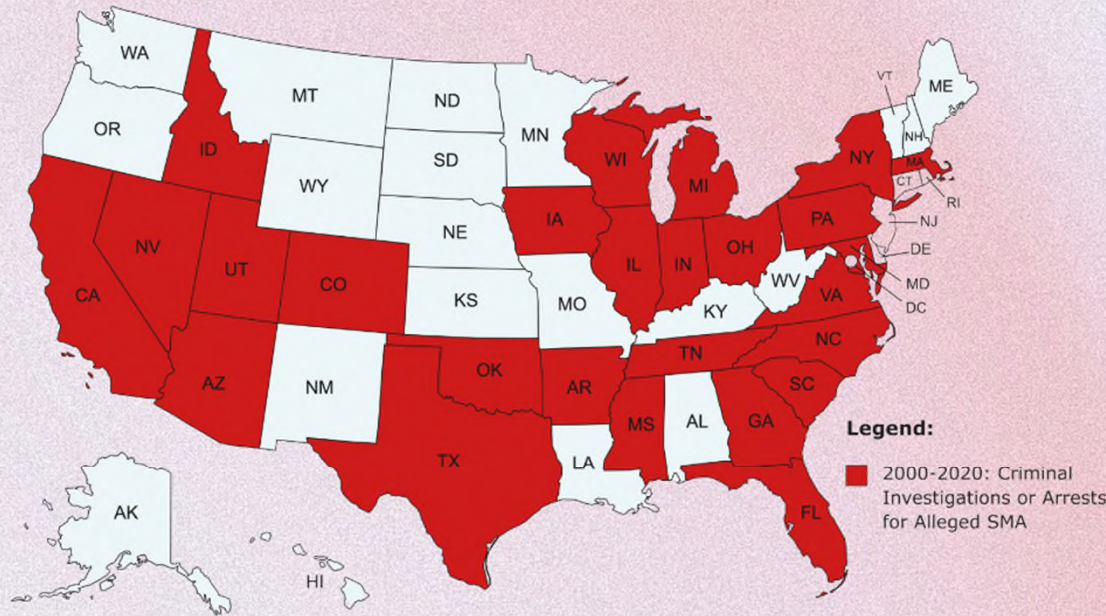


*Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal Status and Public Health, Journal of Health Politics, Policy and Law (April 1, 2013)

**Self-Care Criminalized: August 2022 Preliminary Findings, Huss et. al, available at <https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/> (August 9, 2022)

Mapping abortion criminalization.

if
when
how
Lawyering for
Reproductive
Justice



From 2000 to 2020, If/When/How identified 61 cases of people criminally investigated or arrested for allegedly ending their own pregnancy or helping someone else do so.

Self-Care Criminalized: August 2022 Preliminary Findings, Huss et. al, available at <https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/>

Pregnancy Justice has further documented approximately 1,331 such cases from 2006-2020.

- This equals more than 1,700 cases between 1973-2020.

Private until
presumed
guilty

The power of the government
to get your data when
investigating a “crime” is
unmatched.

The Health Insurance Portability and Accountability Act
(HIPAA)?

The Stored Communications Act (SCA)?

Consumer protections from the Federal Trade
Commission (FTC) (Health Breach Notification Rule?)

HOW DOES THE GOVERNMENT GET THIS DATA?

Cell Phone

1. Constitutional seizure of device
2. Valid search warrant (or exception to warrant requirement), *Riley v. California*, 573 U.S. 373
3. Technological ability to perform forensically sound extraction
 - i. May require additional hardware or software that they do not have access to
4. Can obtain data that is only stored on a device, and not stored in the cloud or by a third-party.

Cloud Data

1. Does not require physical seizure of a device
2. Does not require any special hardware or software
3. Can obtain some information without a warrant (just via subpoena)
4. May require a search warrant (pursuant to the Stored Communications Act)
5. Can potentially obtain information that is *not* stored on a device (IP logs, subscriber information).
6. Business records may be more intelligible than extracted data

Warrants for Phone Data

...and why it's so easy for the government to get them

Requirements for Warrants

Connection to Crime	Connect "thing" to crime Stolen TVs being kept in a house = probable cause why it is believed to be the "stash house"
Limited Search	Search only the places where the thing can be Can't open a drawer to look for a TV
Specificity	Describe *specifically* what areas can be searched Search cannot go beyond the parameters of the warrant
Oversight	Judge reviews and signs off on the warrant

Riley V.
California
573 U.S.
373 (2014)

These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.

While [this] categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.

We therefore hold instead that officers must generally secure a warrant before conducting such a search.

Problems with warrants

Lack of scrutiny	Search warrants are largely rubber stamped
Inability to challenge prior to search	Issued ex-parte (in secret) No legal mechanism or adversarial process
Limited avenues for post-search challenges	Who and what can be challenged is limited
Inadequate Remedies for violations	Data obtained from a search can still be used in limited ways even obtained in violation of the law (whether a constitutional violation or otherwise)

Requirements for Warrants

Connection to Crime	Connect "thing" to crime Stolen TVs being kept in a house = probable cause why it is believed to be the "stash house"
Limited Search	Search only the places where the thing can be Can't open a drawer to look for a TV
Specificity	Describe *specifically* what areas can be searched Search cannot go beyond the parameters of the warrant
Oversight	Judge reviews and signs off on the warrant

“Phones do stuff and store information” is probable cause?

- s. As detailed in the Technical Background section, below, cellular telephones commonly contain geolocation, as well as date and time information, associated with various uses of the phone, including, but not limited to, metadata associated with audio files, videos, photos or other images contained in the cellphone. In addition, cellular telephones commonly contain dates, times and IP addresses associated with the phone's Wi-Fi access, mobile internet access or use of mobile apps. Such date, time and location information will provide details and corroboration of the TARGET DEVICE's user's/possessor's location and movements at and around the time of the Subject Crimes.
- t. Based upon my training and experience, I am aware that cellular telephones are used to communicate with others, through phone calls, emails, texts, the sharing or posting of documents and audio or video files, instant messages, or through the use of Apps, including, but not limited to, Twitter, Facebook, Messenger, WhatsApp, Snapchat, Instagram, Skype, WeChat, Viber, Kik, QQ, Telegram and Signal. I am further aware that individuals who engage in describe criminal activity at issue may (i) communicate with others regarding planned future actions or past actions, (ii) research such criminal activity through mobile internet searches, and/or (iii) generate and store on their cellphones communications, images or screenshots of communications and records relating to their illegal activity and contacts with persons either involved directly in that activity or with whom they may discuss such activity. Such communications and records may be evidence of contact or association with known and unknown co-conspirators, or be statements or other indications of an intent, motive or desire to commit, or of having committed, the Subject Crimes.
- u. As further detailed in the Technical Background section, below, I am aware that cellular telephones are capable of being linked to a remote account, or "cloud" service.

Information identifying the existence of such accounts, the identifying information necessary to associate an account with a given device and/or user, and evidence that a given "cloud" account has been accessed by or electronically associated with the TARGET DEVICE, is stored within any phone linked in this manner to a remote account.

- v. I am further aware that cellular telephones commonly contain information that is evidence of the identity of the user/possessor of the TARGET DEVICE or of a person who exercised dominion or control over said device. For instance, telephone call logs, contact lists, email addresses, calendar entries, mobile app user profiles, voice messages, lists of other, Bluetooth-paired devices, and identifiers for instant messaging and social media accounts are evidence of past or potential future communications and contacts with particular persons which in turn is evidence of the identity of the person using or possessing the TARGET DEVICE, or exercising dominion or control thereover, during time periods associated with or relevant to the Subject Crimes.
- w. In addition to geolocation data and date and time information contained in the metadata of audio files, photos or videos stored on the TARGET DEVICE, the audio files, photos and videos themselves provide relevant evidence of the Subject Crimes or that a particular person used or possessed the TARGET DEVICE, at a time relevant to the investigation of said crimes. Based upon my training and experience, I am aware that it is common for individuals to store on cellphones photos or videos of themselves alone or with others or of their family and/or friends, which in turn is evidence of the identity of the person using or possessing the TARGET DEVICE during time periods associated with or relevant to the Subject Crimes.

cellular telephones commonly contain information that is evidence

s. As detailed in the Technical Background section, below, cellular telephones commonly contain geolocation, as well as date and time information, associated with the phone, including, but not limited to, metadata associated with audio files, videos, photos or other images contained in the cellphone. In addition, cellular telephones

commonly contain dates, times and IP addresses

t. Based upon my training and experience, cellular telephones are used to communicate with others, through phone calls, text messages, or through the use of Apps, including Facebook, Messenger, WhatsApp, Snapchat, Instagram, Skype, WeChat, Viber, Kik, QQ, Telegram and Signal. I am further aware that individuals who engage in describe criminal activity at issue may (i) communicate with others regarding planned future actions or past actions, (ii) research such criminal activity through mobile internet searches, and/or (iii) generate and store on their cellphones communications, images or screenshots of communications and records relating to their illegal activity and contacts with persons either involved in or who may be involved in the criminal activity, or whom they may discuss such activity. Such communications may be evidence of contact or association with known and unknown co-conspirators, or of statements or other indications of an intent, motive or desire to commit, or of having committed, the Subject Crimes.

u. As further detailed in the Technical Background section, below, I am aware that cellular telephones are capable of being linked to a remote account, or "cloud" service.

cellular telephones are capable of being linked to a remote account, or "cloud" service.

Information identifying the existence of such accounts, the identifying information necessary to associate an account with a given device and/or user, and evidence that a given "cloud" account has been accessed by or electronically associated with the TARGET DEVICE, is stored within any phone linked in this manner to a remote account.

v. I am further aware that cellular telephones commonly contain information that is evidence of the identity of the user/possessor of the TARGET DEVICE or of a person who exercised dominion or control over said device. For instance, telephone call logs, contact lists, email addresses, calendar entries, mobile app user profiles, voice messages, lists of other, Bluetooth-paired devices, and identifiers for instant messaging and social media accounts are evidence of past or potential future communications and contacts with particular persons which in turn identify the identity of the person using or possessing the TARGET DEVICE, dominion or control thereover, during time periods associated with or relevant to the Subject Crimes.

w. In addition to geolocation data and date and time information contained in the metadata of audio files, photos or videos stored on the TARGET DEVICE, the audio files, photos and videos themselves provide relevant evidence of the Subject Crimes or that a particular person used or possessed the TARGET DEVICE, at a time relevant to the investigation of said crimes. Based upon my training and experience, I am aware that it is common for individuals to store on cellphones photos or videos of themselves alone or with others or of their family and/or friends, which in turn is evidence of the identity of the person using or possessing the TARGET DEVICE during time periods associated with or relevant to the Subject Crimes.

“People like to do stuff on their phones” is probable cause?

11. I further state that based on my experience as a Police Officer and someone who uses cellular phones, I know that suspects communicate with these phones and store information on these phones which reveal their identity, for example, I know that people that use cell phones frequently take “selfies” or other photographs or videos of themselves. I know that these phones have address books which frequently contain their own name and address, as well as the names and addresses of family members and friends. Additionally, people use smart phones to communicate with other people, and these messages will also frequently reveal information of the owner/sender’s name or identity. Likewise, with regards to emails and or text messages, as well as identifying themselves in social media communications. I know that cell phones store the particular number of the cell phone, from which I would also be able to determine the owner or user’s identity. I believe that there is reasonable cause to believe obtaining this information will reveal the identity of this perpetrator.
12. I am also aware that mobile devices, such as so-called “smart phones,” such as the **subject mobile telephone**, function as small computers, with Internet, email and messaging capabilities that are augmented by various mobile applications. I am aware that a forensic search of a “smart phone” may provide evidence of electronic communications, files or other data which were once on the device and have been subsequently deleted. I am also aware that this type of examination may take an extended period of time.

“Criminals” use phones and social media

6. I know from prior training and experience, and conversations with other seasoned criminal investigators, that people involved in criminal activity frequently have conversations regarding their criminal activities through various social networking sites, i.e. Facebook.

Getting warmer

I was advised by [REDACTED] major crimes

Sgt. [REDACTED] that there was surveillance video of the suspect holding a phone right after the assault. Sgt. [REDACTED] explained you can see a glow of the cellular device.

On [REDACTED] [REDACTED] was taken into custody for one the pending charges related to the above mentioned investigation. When [REDACTED] was taken into custody he had two phones on him. A blue Iphone in a teal case and a black Iphone in a black case.

In regards to the black Iphone with the black case, While [REDACTED] was in custody, text messages started popping up on his home screen.

Requirements for Warrants

Connection to Crime	Connect "thing" to crime Stolen TVs being kept in a house = probable cause why it is believed to be the "stash house"
Limited Search	Search only the places where the thing can be Can't open a drawer to look for a TV
Specificity	Describe *specifically* what areas can be searched Search cannot go beyond the parameters of the warrant
Oversight	Judge reviews and signs off on the warrant

The only factual allegation linking the phone to the incident:

I observed, via the TARU video surveillance that depicted what I believe to be a robbery and an individual that appeared to be the defendant – he was dressed in the same clothing, carried the same bag, and appeared to have a beard – walking in close proximity to the incident location around 5:20 AM.

I further observed that, when the unknown individual began to quickly approach the victim, the defendant pulled out what appears to be a cellphone and points it in the direction of the robbery in a manner consistent with recording a video or taking a photograph.

I also believe the phone, based on my observations detailed above, would contain images or videos of the unknown perpetrator.

r. Further, I believe evidence contained within THE TARGET DEVICE would assist in discovering the defendant's motive.

Why the officer wants to search the phone:

Because phones have stuff on them, I guess?

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

- a. Evidence of the identifying numbers assigned, registered, or associated with the TARGET DEVICE, including the telephone number, International Mobile Station Equipment Identity (IMEI) number, Electronic Serial Number (ESN) number, Mobile Equipment Identifier (MEID) number, Subscriber Identity Module (SIM) card number, media access control address(es) (MAC address) and/or any other serial or unique identifying number;
- b. Evidence of the identity of the owner and/or user of, or individual who exercised dominion or control over, the TARGET DEVICE, at or around the time of the commission of the Subject Crimes, including:
 - i. Telephone call logs, contact lists, email addresses, mobile app user profiles, voice messages, lists of devices paired by Bluetooth to the TARGET DEVICE, and identifiers for instant messaging and social media accounts;
 - ii. Communications, whether by phone, text, email, the sharing or posting of documents or audio or video files, instant messages, mobile Apps, images or screenshots of communications, or communications in some other form, sent by or received by the TARGET DEVICE, at or around the time of the Subject Crimes;
 - iii. Audio files, photos, videos or other images, and their associated metadata, of [REDACTED] or of others who are his family, friends or associates;
 - iv. Calendar entries, and any linked communications or files, sent by or received by the TARGET DEVICE, at or around the time of the Subject Crimes; and
 - v. Evidence of mobile access to websites, Apps, or social media accounts, e.g., Facebook, Twitter, Snapchat, etc., associated with [REDACTED] or others who are his family, friends or associates;

Makes it look like a limited search, but amounts to the whole phone.

- c. Evidence relating to the location of the owner or user of the TARGET DEVICE, including dates, times and geolocation data contained in metadata associated with audio files, videos or images, as well as IP addresses associated with the TARGET DEVICE's Wi-Fi access, mobile internet access or use of mobile Apps (including, but not limited to, Uber, Lyft, Google Maps, Waze, Belly, Level Up, etc.), at or around the time of the commission of the Subject Crimes;
- d. Communications, records, internet history, audio files, videos, images, screenshots or other images of communications, or other data which evidence or tend to show the commission of, or tend to connect a person to, the Subject Crimes, including:
 - i. Audio files, photos, videos or other images, and their associated metadata, of [REDACTED] whether alone or with others, at or around the time of the Subject Crime;
 - ii. Communications, records, images or other evidence of contact or association with others involved in the planning, commission or concealment of the Subject Crimes;
 - iii. Statements, including texts, emails or other communications, and internet searches or other indications of an intent, motive or desire of committing, or of having committed, the Subject Crimes;
- e. Information demonstrating the existence of a remote backup account, or "cloud" service, linked to the TARGET DEVICE and any of the user accounts associated with the TARGET DEVICE, including the names of "cloud" account service providers, account names, account addresses, account passwords, account settings, account activity logs, and evidence that a given "cloud" account has been accessed by or electronically associated with the TARGET DEVICE.

Remember, they said they are looking for photos/videos, and evidence of motive.

- a. Evidence of the identifying numbers assigned, registered, or associated with the TARGET DEVICE, including the telephone number, International Mobile Station Equipment Identity (IMEI) number, Electronic Serial Number (ESN) number, Mobile Equipment Identifier (MEID) number, Subscriber Identity Module (SIM) card number, media access control address(es) (MAC address) and/or any other serial or unique identifying number;
- b. Evidence of the identity of the owner and/or user of, or individual who exercised dominion or control over, the TARGET DEVICE, at or around the time of the commission of the Subject Crimes, including:

Telephone call logs, contact lists, email addresses, mobile app user profiles, messages, lists of devices paired by Bluetooth to the TARGET DEVICE, and identifiers for instant messaging and social media accounts;

Communications, whether by phone, text, email, the sharing or posting of documents or audio or video files, instant messages, mobile Apps, images or screenshots of communications, or communications in some other form, sent by or received by the TARGET DEVICE, at or around the time of the Subject Crimes;

- iii. Audio files, photos, videos or other images, and their associated metadata, of [REDACTED] or of others who are his family, friends or associates;
- iv. Calendar entries, any linked communications or files, sent by or received by the TARGET DEVICE, at or around the time of the Subject Crimes; and
- v. Evidence of mobile access to websites, Apps, or social media accounts, e.g.,

mobile access to websites, Apps, or social media accounts, e

- c. Evidence relating to the location of the owner or user of the TARGET DEVICE, including dates, times and geolocation data contained in metadata associated with audio files, videos or images, as well as IP addresses associated with the TARGET DEVICE's Wi-Fi access, mobile internet access or use of mobile Apps (including, but not limited to, Uber, Lyft, Google Maps, Waze, Belly, Level Up, etc.), at or around the time of the commission of the Subject Crimes;
- d. Communications, records, internet history, audio files, videos, images, screenshots or other images of communications, or other data which evidence or tend to show the commission of, or tend to connect a person to, the Subject Crimes, including:
 - i. Audio files, photos, videos or other images, and their associated metadata, of [REDACTED] whether alone or with others, at or around the time of the Subject Crime;
 - ii. Communications, records, images or other evidence of contact or association with others involved in the planning, commission or concealment of the Subject Crimes;
 - iii. Statements, including texts, emails or other communications, and internet searches or other indications of an intent, motive or desire of committing, or of having committed, the Subject Crimes;
- e. Information demonstrating the existence of a remote backup account, or "cloud" service, linked to the TARGET DEVICE and any of the user accounts associated with the TARGET DEVICE, including the names of "cloud" account service providers, account names, account addresses, account passwords, account settings, account activity logs, and evidence that a given "cloud" account has been accessed by or electronically associated with the TARGET DEVICE.

Your victim indicated that the girlfriend of [REDACTED] [REDACTED] was attempting to sell the stolen Iphone 6s Plus on her 'FACEBOOK.COM' account. Your victim referred to the 'FACEBOOK.COM' account, under the moniker of [REDACTED] It is your affiant's intention to download and inspect the contents of all of the above involved Facebook records in order to try and obtain further evidence of the aforementioned crimes.

3. You are hereby authorized and directed to search for and seize the following property; the property sought to be seized consists of:

- A. **IMSI and MSN numbers** associated with the described phones and affixed to them within the battery compartment and also contained inside the case of the phone and accessible by disassembly of the phone and also embedded in the memory of the phone or associated and attached SIM cards.
- B. **Records kept electronically or digitally** within the telephones' memory to include a log of recent incoming and outgoing phone calls, a list of contacts or phonebook, text and picture messages, photographs, videos, internet history, search history, applications and information that tends to identify the user or subscriber of the phone including telephone number, private ID number and I.P. addresses.

c) the area to be searched includes the entire phone and all data to include but not

limited to information that tends to identify the owner/user of said cellular telephone devices, IMSI and MSN numbers associated with said cellular telephone devices, affixed to it within the battery compartment or accessible by disassembly of the phone or embedded in the memory of the phone or associated and attached SIM cards, any information regarding web connectivity including web searches and website history, and records kept electronically or digitally within the telephone's memory, to include: a log of recent incoming and outgoing calls, a list of contacts or phone book, any text messages, any e-mail messages, any pictures, picture messages, any videos, video-messages, any information gleaned from applications present on the phone such as social networking sites, any information relative to location information, and any information that tends to identify the user or subscriber of the phone, including telephone number, private ID number, and IP address; all in violation of Section 220.16 and Section 125.25 of the New York State Penal Law or that a particular person participated in the commission of such offense, pursuant to Section 690.10.(2)(3)(4) of the New York State Criminal Procedure Law.

Not even trying to act like the search is limited.

Problems with warrants

Lack of scrutiny	Search warrants are largely rubber stamped
Inability to challenge prior to search	Issued ex-parte (in secret) No legal mechanism or adversarial process
Limited avenues for post-search challenges	Who and what can be challenged is limited
Inadequate Remedies for violations	Data obtained from a search can still be used in limited ways even obtained in violation of the law (whether a constitutional violation or otherwise)

Can you stop the search from happening?

From: **Records** <records@records.facebook.com>

Date: Wed, Feb 1, 2017 at 3:09 PM

Subject: Your Facebook account

To: [REDACTED]

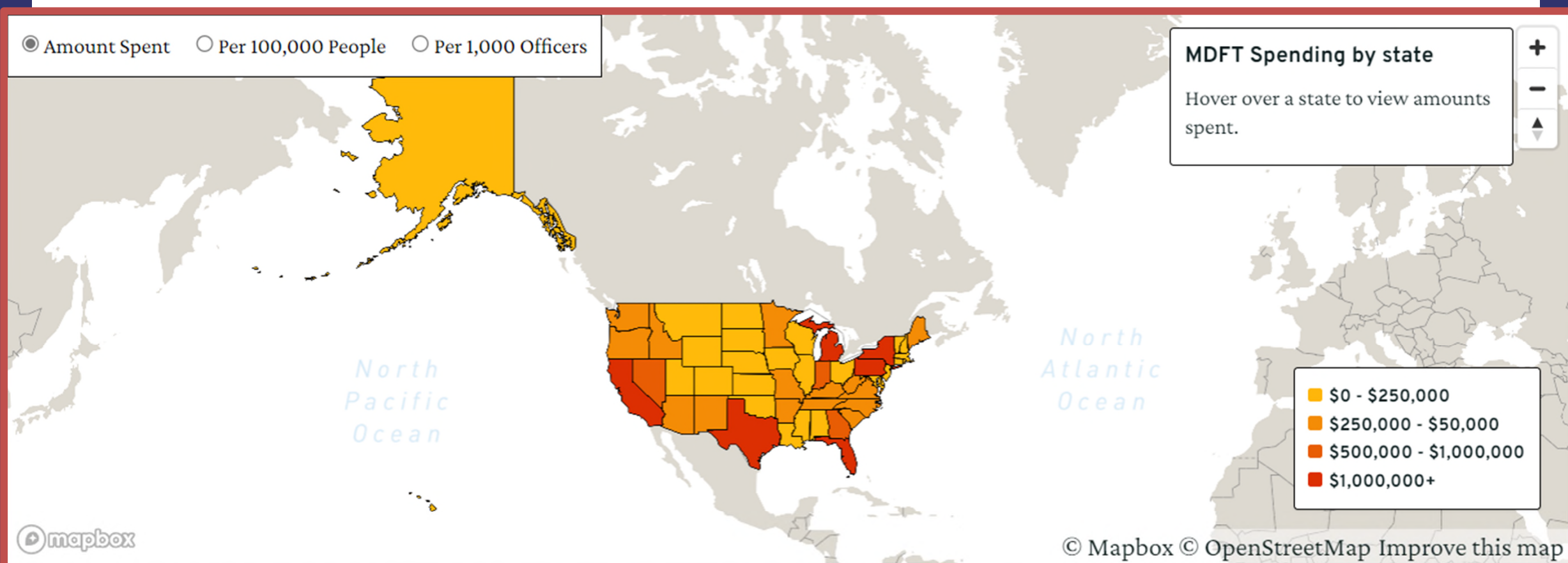
Hello,

We have received legal process from law enforcement seeking information about your Facebook account. If we do not receive a copy of documentation that you have filed in court challenging this legal process within ten (10) days, we will respond to the requesting agency with information about the requested Facebook account. We may need to respond to this legal request within less than ten (10) days if we have a reasonable belief that we are legally required to do so. Please respond to this message with a copy of any documents you file with the court. If you would like additional information about the legal process, please let us know as soon as possible.

Thank you,
Law Enforcement Response Team



Phone Investigations



Map 2 shows the total amount of money spent on MDFTs in each state since 2015. Using the toggle alternately shows the amount spent in each state per 100,000 residents, and per 1,000 sworn officers. Total amounts come from our records requests and from our records requests and from financial transparency websites that states offer. Given this, the total amounts shown are likely underestimates.

For-profit, for the government

Certain tools to unlock phones and access data sold to:

- ✓ Criminal Prosecution
- ✓ Government Agencies
- ✓ Computer forensics businesses serving Civil Plaintiffs (sometimes)
- ✓ Computer forensics businesses serving Civil Defense (sometimes)
- ✓ Corporate Cybersecurity Teams (sometimes)

But not to:

- ✗ Criminal Defense



Evidence + Bias = Inconsistent Conclusions

The results suggest what is considered a low/inadequate ($\alpha < 0.667$) consistency between DF examiners who examined the same evidence file based on the same contextual information. The low consistency was found on all the examined levels: observations of traces, interpretations of observed traces, and conclusions. The results suggest that if a DF examiner performs an analysis of an evidence file, and another DF examiner would do a re-analysis of the same evidence file, the chances of reaching consistent results are low.

This finding is of great importance, since it indicates, quite contrary to the perception of digital evidence as objective and credible, that digital evidence may be affected by the human examiner in all the stages we have examined – during the observation, the interpretation of observation and when forming a conclusion. The low reliability would thus not only have implications for reporting opinion evidence but also for factual/technical reporting.

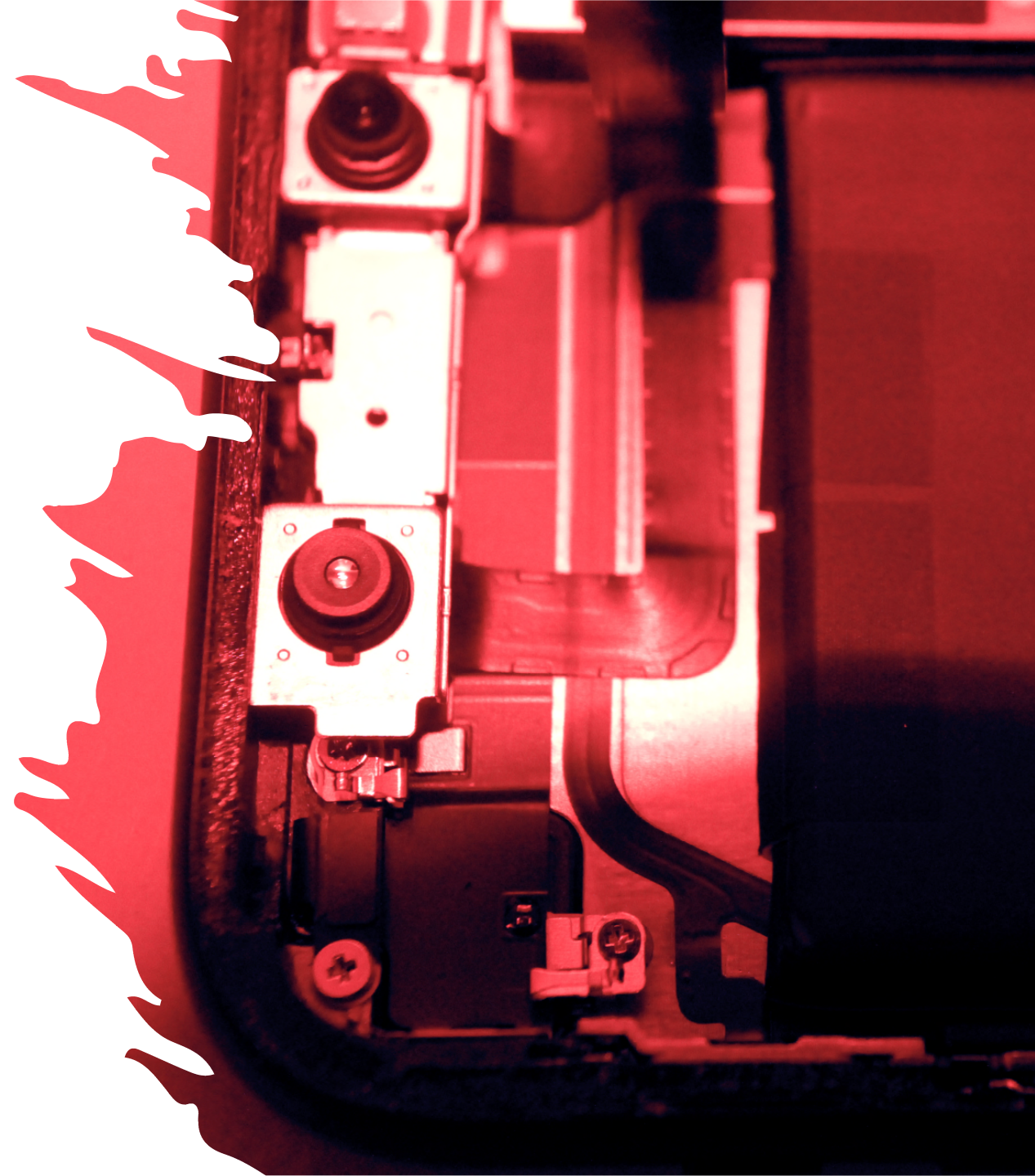
Nina Sunde, Itiel E. Dror, *A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making*, Forensic Science International: Digital Investigation, Volume 37, 2021, 301175, ISSN 2666-2817, <https://doi.org/10.1016/j.fsidi.2021.301175>.

(Accessed from <https://www.sciencedirect.com/science/article/pii/S2666281721000834> on July 2nd, 2023)

What is a phone extraction?

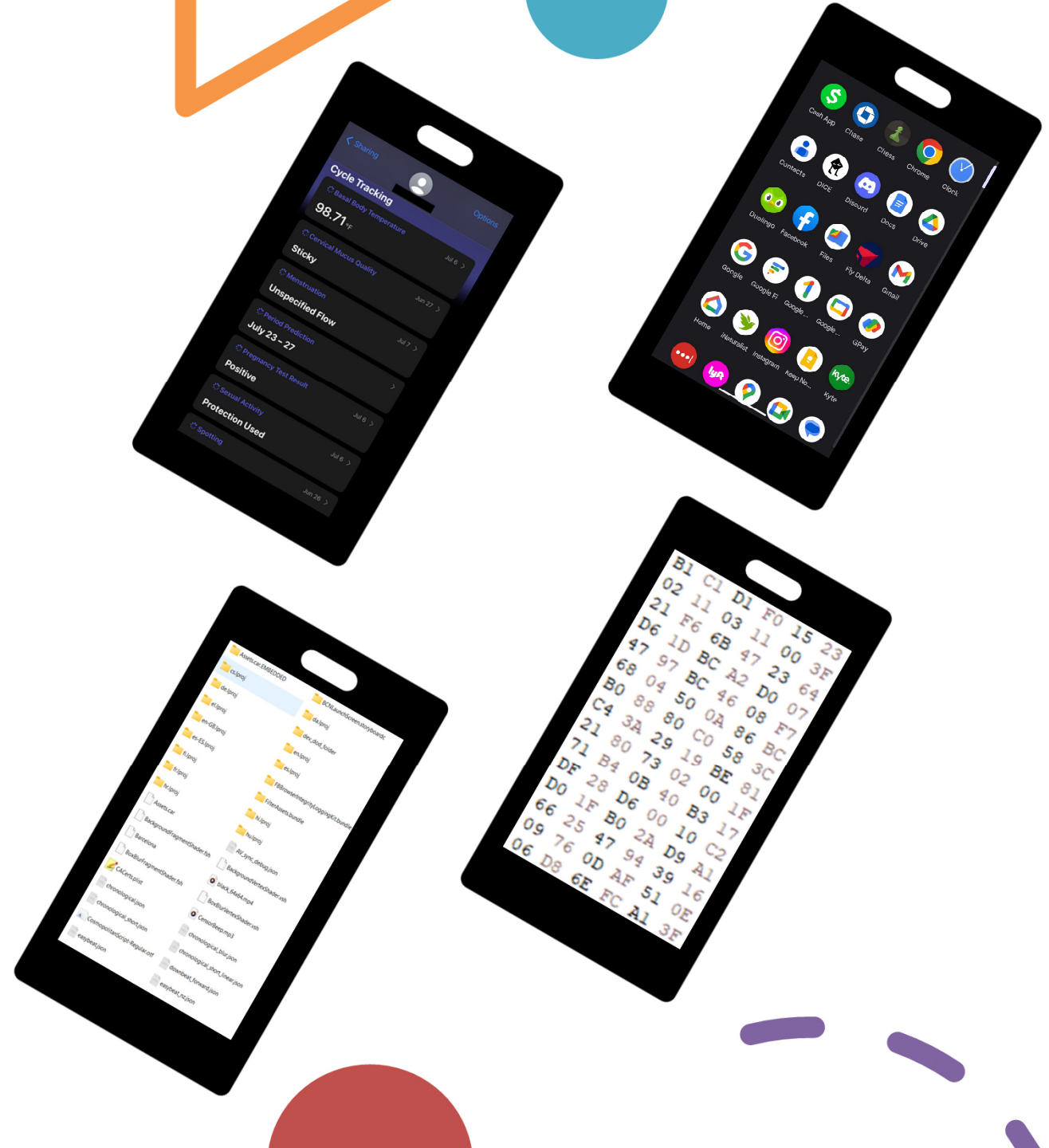
Copy of the phone (to a point)

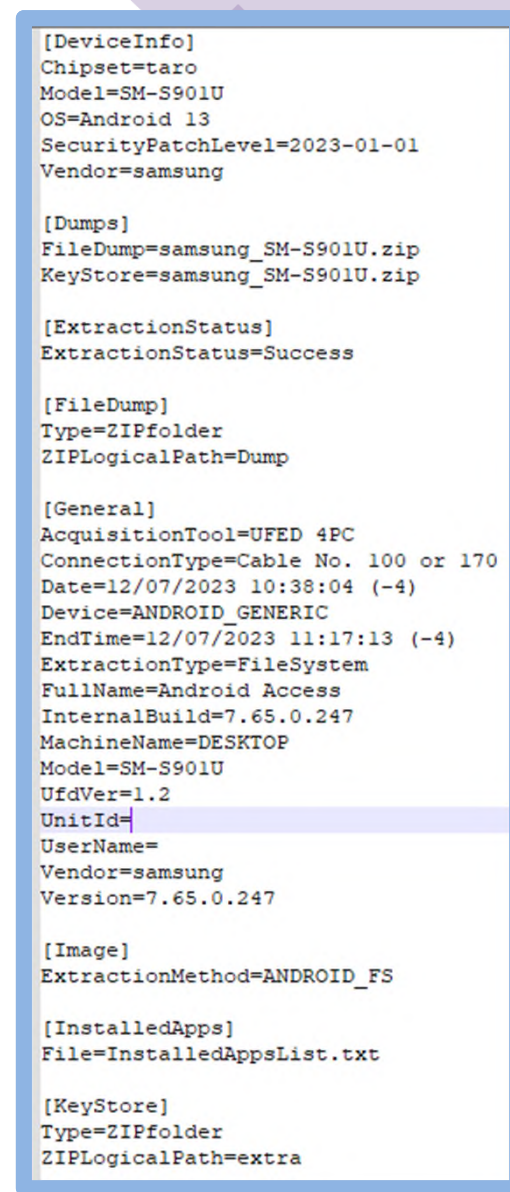
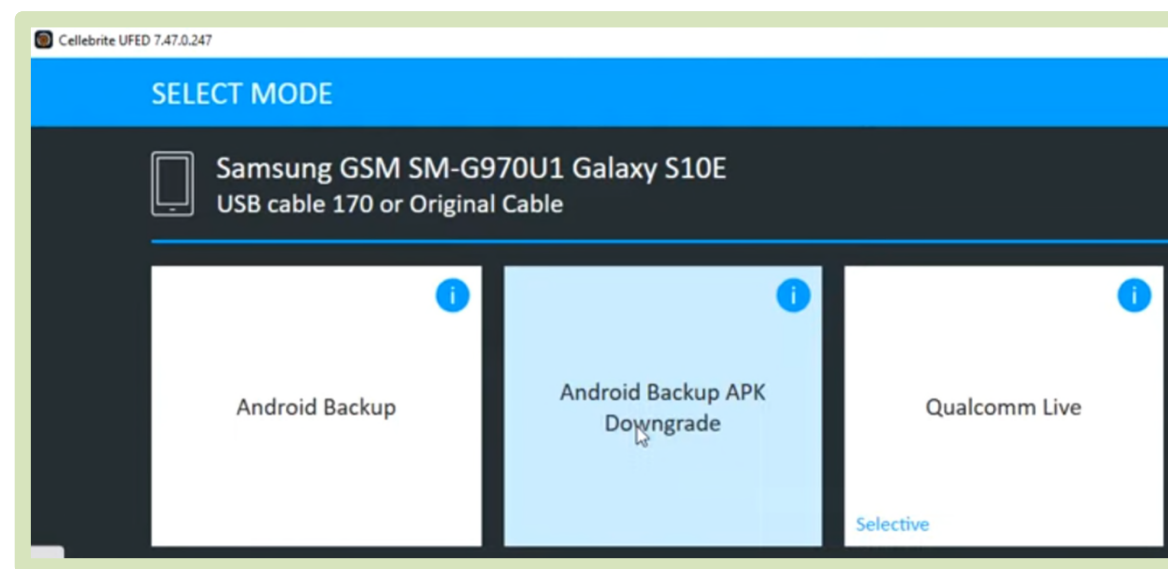
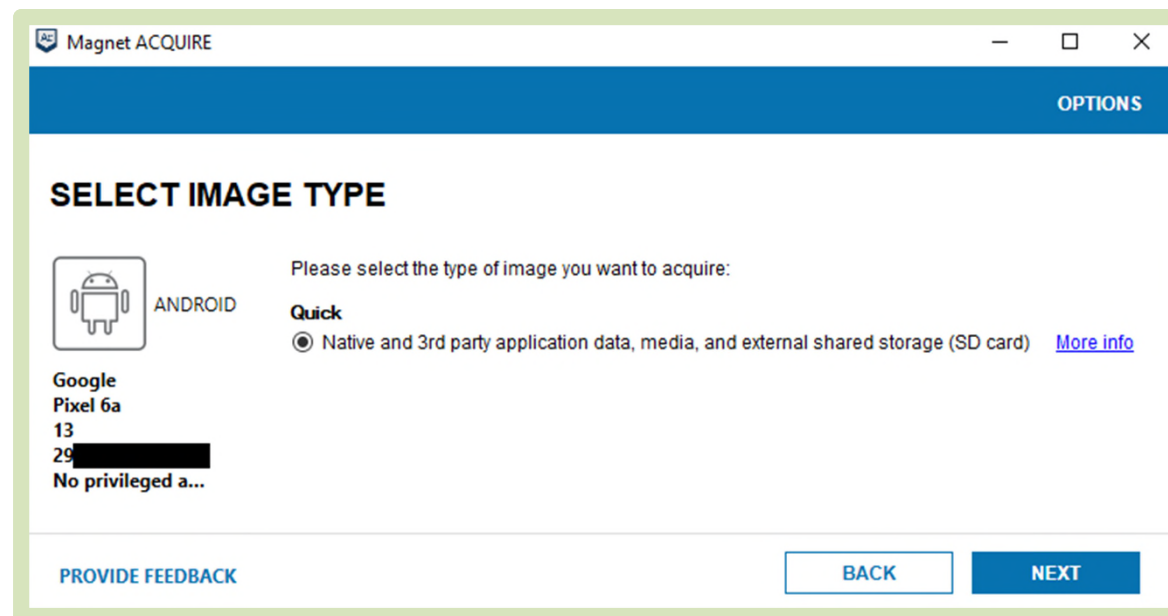
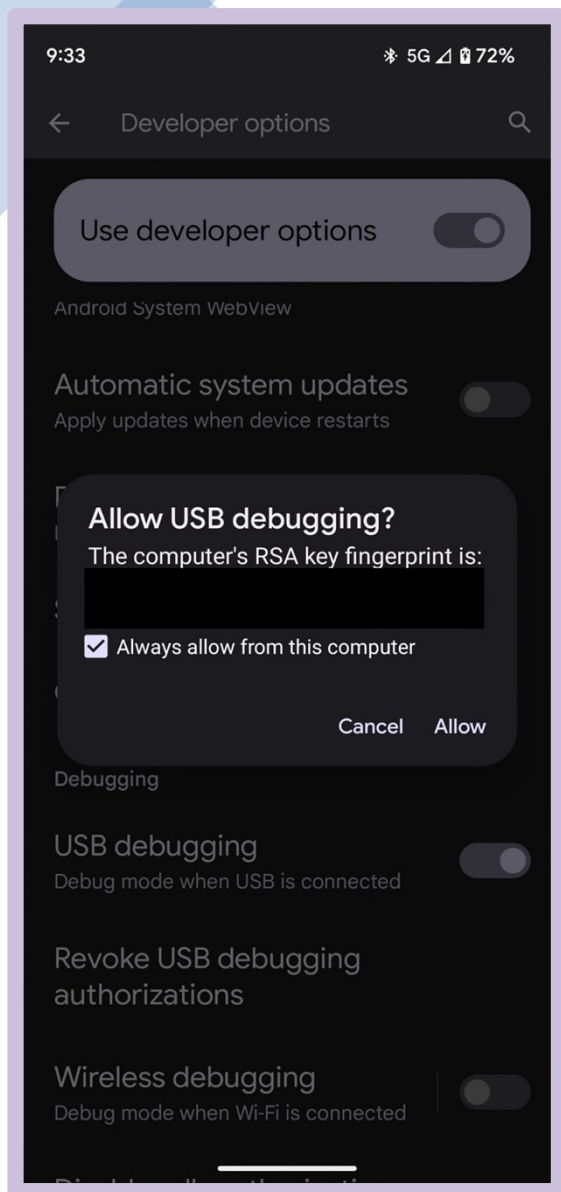
- **Commercial software** used by the government and private companies uses ADB, AFC, built in backup tools, bootloaders, sideloaded apps, and jailbreaks to bypass protections like SEP (Secure Enclave processor) and copy data for use in court
- Don't have to be a hacker, just need government **budget** and a **tool license**
- **Security is great but:**
 - Brute force - it's only a matter of time
 - Consent and social engineering - it's only a matter of pressure



Extraction types:

- **Live screenshots** saved by an investigator
- **"Logical"** information categories supported by transfer protocols on the device (backups, SMS/MMS, media, calendars)
- **Partial file system** copy
- **Full file system** copy (including keychains)
- **Physical** copy of phone's flash memory (on older devices)





(c) 2011-2023 Elcomsoft Co. Ltd.

Device connected: none
Please select an action:

Logical acquisition

- | | | |
|---|---------------|---|
| I | DEVICE INFO | - Get basic device information |
| R | RECOVERY INFO | - Get information on device in Recovery/DFU mode |
| B | BACKUP | - Create iTunes-style backup of the device |
| M | MEDIA | - Copy media files from the device |
| S | SHARED | - Copy shared files of the installed applications |
| L | LOGS | - Copy crash logs |

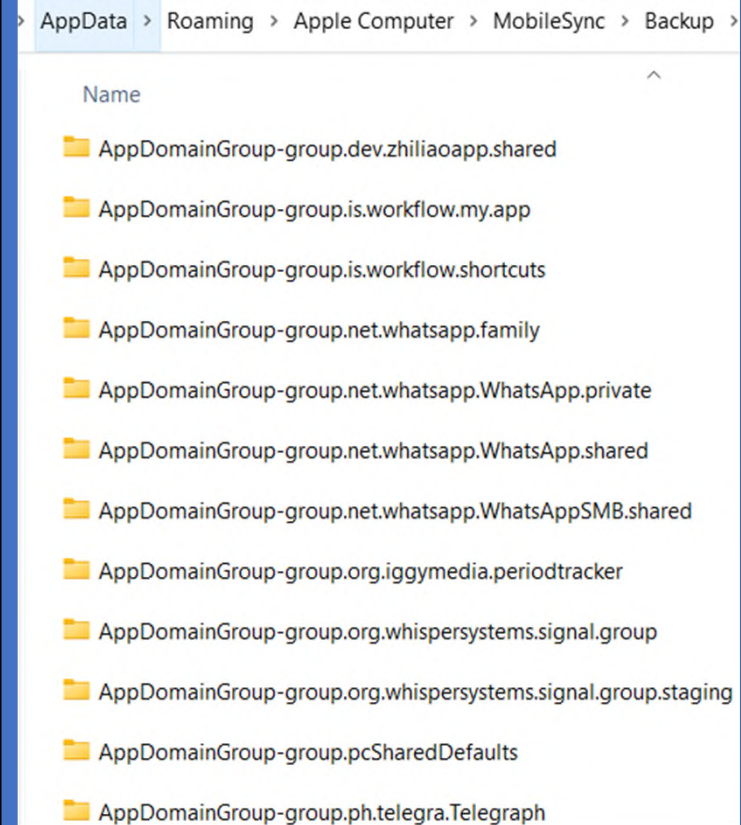
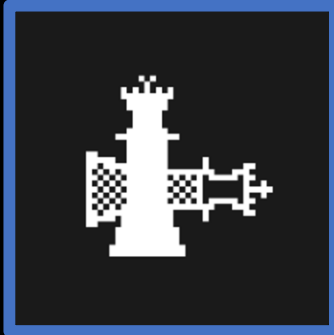
Physical acquisition (for jailbroken devices)

- | | | |
|---|--------------|---|
| D | DISABLE LOCK | - Disable screen lock (until reboot) |
| K | KEYCHAIN | - Decrypt device keychain |
| F | FILE SYSTEM | - Acquire device file system (as TAR archive) |

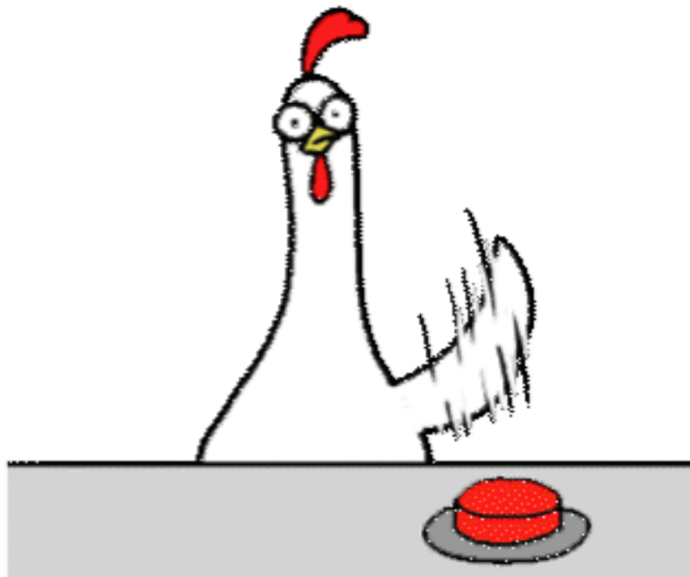
Acquisition agent (limited compatibility)

- | | | |
|---|--------------------|---|
| 1 | INSTALL | - Install acquisition agent on device |
| 2 | KEYCHAIN | - Acquire device keychain |
| 3 | FILE SYSTEM | - Acquire device file system (as TAR archive) |
| 4 | FILE SYSTEM (USER) | - Acquire user files only (as TAR archive) |
| 5 | UNINSTALL | - Uninstall acquisition agent on device |
| X | EXIT | |

>:



Push Button Forensics



- **Why can it be good? (if you know what you're doing)**
 - Less effort to keep up with the large volume of devices that need to be analyzed
 - Faster to analyze/process
- **Why can it be bad? (if you don't know what you're doing)**
 - Analysts may not even know how to look for relevant data without the aid of tools (which are not always correct) 🐛
 - Analysts may misinterpret reports (bias)
 - Wrong decisions can result in having to re-preserve... and ephemeral data may have been lost in the meantime



Apple iPhone

Search

Analyzed Data

Application (226)

Calendar (136)

Calls (3)

Contacts (31)

Devices & Networks (1119) (67)

Device Connectivity (1067) (67)

Device Events (44)

Wireless Networks (8)

Location Related (1)

Manual Evidence

Media (19368)

Messages (16)

Chats (11) (19 messages)

Instant Messages (5)

Physical Activities (706)

Search & Web (354)

Cookies (101)

Searched Items (4)

Web Bookmarks (7)

Web History (242)

System & Logs (1182)

User Accounts & Details (340)

Mobile Cards (1)

Passwords (320)

User Accounts (19)

Timeline (21139) x

2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025



Clear



2020 - 2029

5/20/2023 - 7/30/2023

3 Filters applied Clear filters

Timeline settings



Export

Filters

Actions

Search



[Icon]	[Icon]	[Icon]	Type	Timestamp	Description	Source	Source file information
			Log Entries	7/10/2023 5:39:09 PM(UTC-4)	com.apple.datausage.media: Wifi In:0 Wifi Out:0 Wan In:18304 Wan Out:4986	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20C5E DataUsage.sqlite-wal : 0x23E9C
			Log Entries	7/10/2023 6:03:31 PM(UTC-4)	com.apple.MobileSMS: incoming sms from E25F4CAA-7FF1-4465-82E6-0E71F9814CAE:ABPerson	InteractionC	interactionC.db-wal : 0x248D08
			Log Entries	7/10/2023 6:03:32 PM(UTC-4)	com.apple.datausage.appleid: Wifi In:0 Wifi Out:0 Wan In:15303 Wan Out:3262	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20CC4 DataUsage.sqlite-wal : 0x24543
			Log Entries	7/10/2023 6:03:46 PM(UTC-4)	Hey, can you help me out with something?	Native Messages	sms.db : 0x49900
			Log Entries	7/10/2023 6:03:46 PM(UTC-4)	Hey, can you help me out with something?	InteractionC	interactionC.db-wal : 0x248C41
			Log Entries	7/10/2023 6:04:21 PM(UTC-4)	com.apple.datausage.icloud: Wifi In:0 Wifi Out:0 Wan In:94064 Wan Out:26453	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20C5E DataUsage.sqlite-wal : 0x244F2
			Log Entries	7/10/2023 6:04:21 PM(UTC-4)	com.apple.datausage.icloud: Wifi In:0 Wifi Out:0 Wan In:94064 Wan Out:26453	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20C81 DataUsage.sqlite-wal : 0x244A4
			Log Entries	7/10/2023 6:04:22 PM(UTC-4)	com.apple.datausage.diagnostics: Wifi In:0 Wifi Out:0 Wan In:130774 Wan Out:20232	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20CA3 DataUsage.sqlite-wal : 0x23EEA
			Log Entries	7/10/2023 6:04:23 PM(UTC-4)	com.apple.datausage.general: Wifi In:0 Wifi Out:0 Wan In:263719 Wan Out:226275	iPhoneNetworkDataUsage	DataUsage.sqlite : 0x20C38 DataUsage.sqlite-wal : 0x23E96
			Instant Messages	7/10/2023 6:04:32 PM(UTC-4)			Recents-wal : 0x7580A
			Instant Messages	7/10/2023 6:04:32 PM(UTC-4)	Sure! What do you need?	Native Messages	sms.db : 0x496F7
			Instant Messages	7/10/2023 6:04:32 PM(UTC-4)	com.apple.MobileSMS: outgoing sms	InteractionC	interactionC.db-wal : 0x248AB4
			Instant Messages	7/10/2023 6:04:32 PM(UTC-4)	Can we move to signal?	Native Messages	sms.db : 0x49508

Location Related (1)

User Accounts & Details (340)

Mobile Cards (1)

Passwords (320)

User Accounts (19)

MATCHING RESULTS (77,875 of 148,851)

MATCHING RESULTS 77,875

REFINED RESULTS 2,073

WEB RELATED 7,589

iOS Safari Cache Records 4
Potential Browser Activity 2,001
Safari History 118
WebKit Browser Web History (Carved) 5,466

COMMUNICATION 81

Apple Contacts - iOS 12
Facebook Messenger Groups 1
Facebook Messenger Users Contacted 2
iOS Call Logs 54
IP Addresses - Audio/Video Calls 6
LINE Messages 1
Textfree Messages / C 1
TextPlus Messages 1
WeChat Friends 1

SOCIAL NETWORK

Instagram Media
Instagram Profiles
iOS Instagram Posts
TikTok Contacts
TikTok Videos
Twitter Tweets

MEDIA

AMR Files
Audio
Carved Audio
iOS Snapshots
Photos Media Informa
Photoshop Files
Pictures
Videos

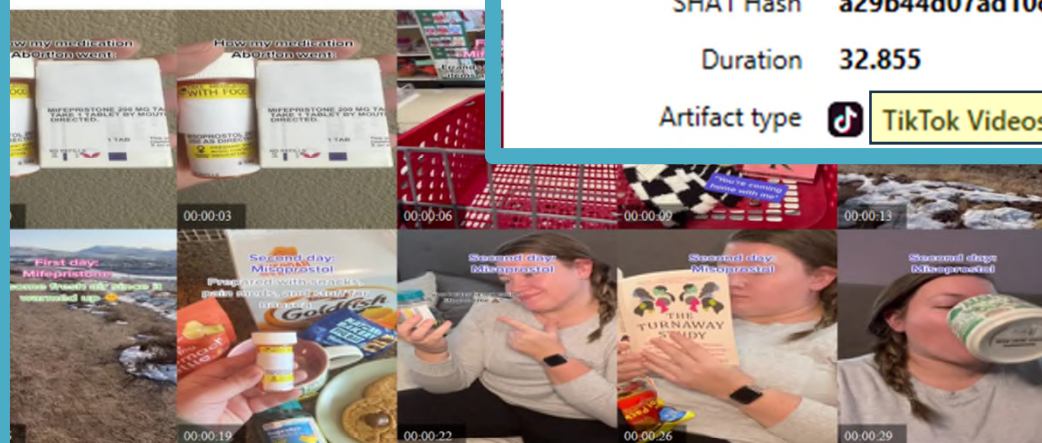
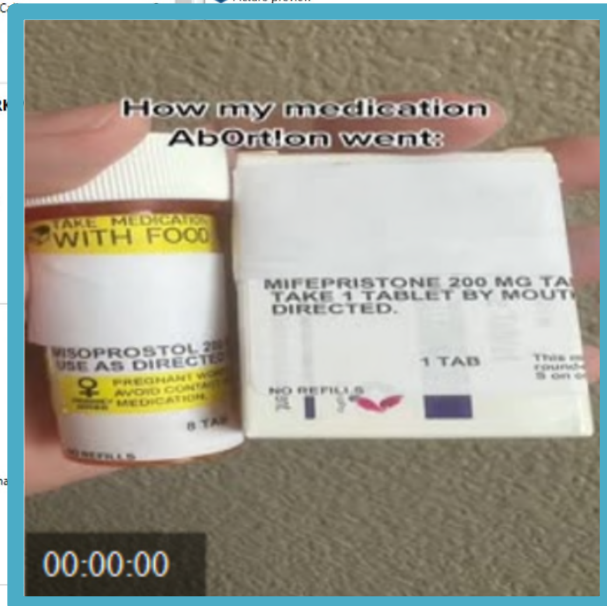
DOCUMENTS

APPLICATION USAGE 2,001

Application Install States 608
Installed Applications 102
Interactive Content

Item ID	Item	Artifact type	Artifact...	Date and time
119003	image/jpeg	Instagram Media	Social Networ...	7/7/2023 1:42:31 PM
119004	image/jpeg	Instagram Media	Social Networ...	7/7/2023 2:28:58 PM
119005	image/jpeg	Instagram Media	Social Networ...	7/7/2023 4:32:07 PM
119006	image/jpeg	Instagram Media	Social Networ...	7/7/2023 2:29:01 PM
119007	image/jpeg	Instagram Media	Social Networ...	7/7/2023 4:32:09 PM
119008	image/jpeg	Instagram Media	Social Networ...	7/6/2023 12:42:53 PM
119009	image/jpeg	Instagram Media	Social Networ...	7/6/2023 12:42:32 PM
119011	image/jpeg	Instagram Media	Social Networ...	7/7/2023 4:32:09 PM
119031	1688753153	iOS Instagram Posts	Social Networ...	7/7/2023 2:05:53 PM
119560	v09044g40000chlmkajc77u7dkom0...	TikTok Videos	Social Networ...	7/6/2023 2:02:42 PM
119561	v12044gd0000cib18jc77u5puqim1fg...	TikTok Videos	Social Networ...	7/6/2023 1:59:59 PM
119562	-1792676417.mdl	TikTok Videos	Social Networ...	7/6/2023 2:01:58 PM
119565	v12044gd0000ch79hvj77ueki2vnn0...	TikTok Videos	Social Networ...	7/6/2023 2:00:51 PM
119566	v12044gd0000chv2jhr77ubnb38vth...	TikTok Videos	Social Networ...	7/6/2023 1:59:59 PM
119567	258759743.mdl	TikTok Videos	Social Networ...	7/6/2023 2:00:51 PM
119568	1459528805.mdl	TikTok Videos	Social Networ...	7/6/2023 2:02:25 PM

Picture preview



ZOOM 86%

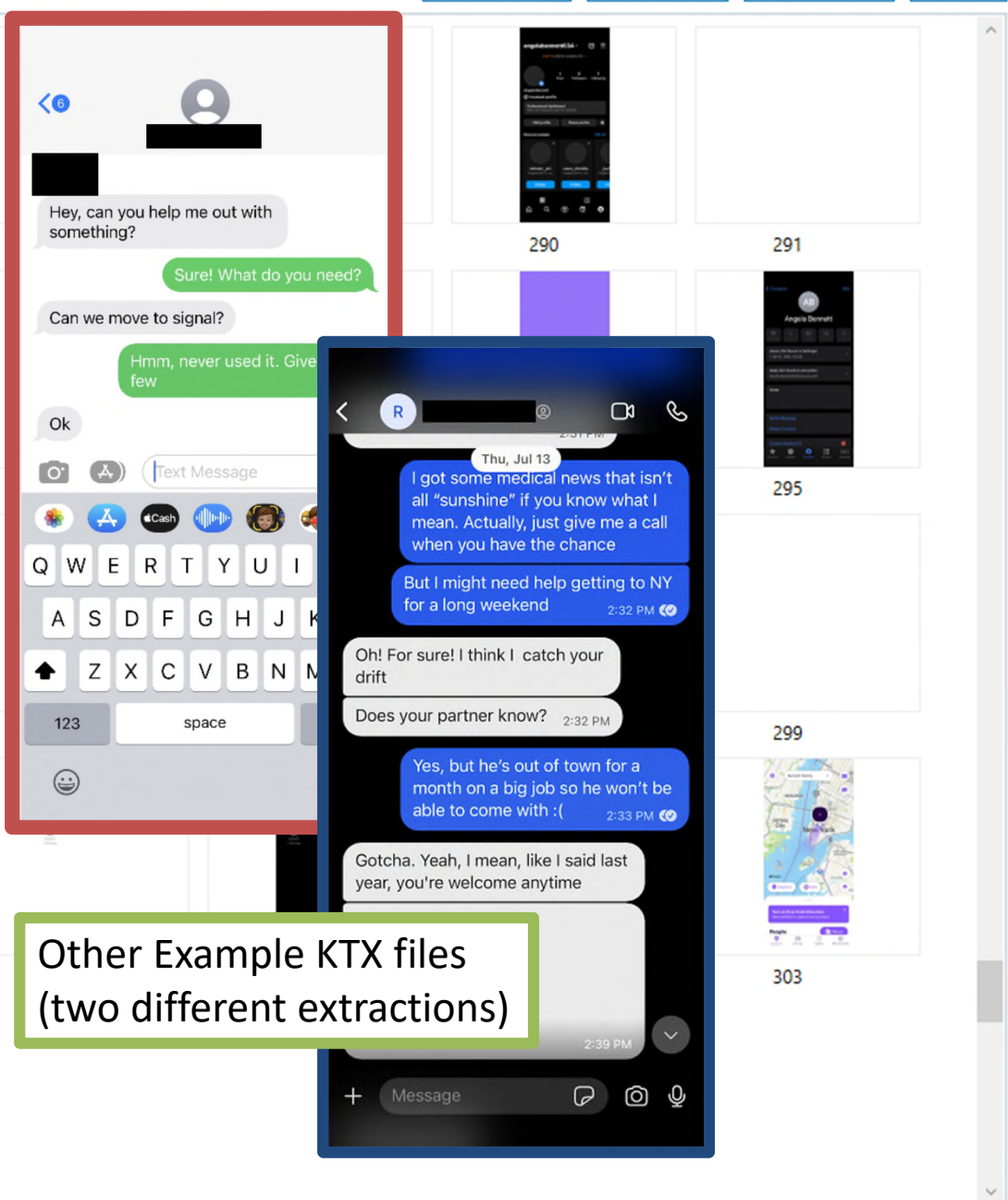
ARTIFACT INFORMATION

File Name v12044gd0000cegu6dbc77u71h71djag_bytevc1_540p_597733.mdl
File Extension .mdl
Last Modified Date/Time 7/6/2023 2:02:41 PM
Type Watched Video
Skin Tone Percentage 54.1
File Size (Bytes) 2454817
MD5 Hash d53cc1af203616b697e2af952e9056a1
SHA1 Hash a29b44d07ad10c3aa0d817193581e283ecbb86eb
Duration 32.855
Artifact type TikTok Videos

Skin Tone Percentage 54.1
File Size (Bytes) 2454817
MD5 Hash d53cc1af203616b697e2af952e9056a1
SHA1 Hash a29b44d07ad10c3aa0d817193581e283ecbb86eb
Duration 32.855
Artifact type TikTok Videos
Item ID 119573

EVIDENCE INFORMATION

Source 00008110-00094C410CDA401E_20230712T152640.tar/private/var/mobile/Containers/Data/Application/803C6783-8AF3-4E29-BAE8-A41CD6486E75/Library/Caches/TTPlayerCache/v12044gd0000cegu6dbc77u71h71djag_bytevc1_540p_597733.mdl
Recovery method Parsing
Deleted source
Location n/a
Evidence number 00008110-00094C410CDA401E_20230712T152640.tar



Other Example KTX files (two different extractions)

00008110-00094C410CDA401E_20230712T152640.tar

PREVIEW

DETAILS

ARTIFACT INFORMATION

Application Package Name	com.zhilioapp.musically
File Name	454E8ABF-749E-40A3-B795-9ADF86776189@3x
File Extension	.ktx
Last Modified Date/Time	7/6/2023 2:03:26 PM
Size (Bytes)	85713
Skin Tone Percentage	0.2
MD5 Hash	681d82335c67f4c143a54b7e06009752
SHA1 Hash	3adc87da38a180be2c33a44eee2ad8033e890673
Potential Original Media	Yes
Artifact type	iOS Snapshots
Item ID	125787

EVIDENCE INFORMATION

Source	00008110-00094C410CDA401E_20230712T152640.tar\private\var\mobile\Containers\Data\Application\803C67B3-8AF3-4E29-BAE8-A41CD6486E75\Library\SplashBoard\Snapshots\sceneID:com.zhilioapp.musically-default\454E8ABF-749E-40A3-B795-9ADF86776189@3x.ktx
Recovery method	
Deleted source	
Location	n/a
Evidence number	00008110-00094C410CDA401E_20230712T152640.tar

alexgerber

Search

abortion medical pill

You may like

- mifepristone cvs - Just watched
- surgical abortion procedure experience
- how much are abortions pill
- Spirit Airlines Flight
- 15 Minute Meals
- Medical Careers
- las libres abortion
- The Viral Ghost Blanket From HomeGo...
- Brown Eyed Girl Trend

Give feedback

< Back

[REDACTED] iPhone

[Device info](#)

Health



Filter OFF Hide



Export... ▲



User Info



Activity

Body
Measurements

Heart



Mindfulness



Nutrition



Reproductive



Results



Sleep



Vitals



Hearing

Birthdate: 25.06.1993

Blood Type: O+

Body Mass: 47.31 kg

Fitzpatrick Skin Type: III

Height: 1.68 m

Name: [REDACTED]

Sex: Female

User entered menstrual cycle length: 21

User entered period cycle length: 5

Wheelchair: No

cardio_fitness_medications_use 0

17.07.2023 12:17:23 (UTC -4)

17.07.2023 14:51:02 (UTC -4)

Active Energy

Flights Climbed

Resting Energy

Steps

Walking and running distance

End Date	Date Added	Source	Device	Details	Active Energy	Was User Entered
17.07.2023 12:09:10 (...)	17.07.2023 12:17:23 (...)	[REDACTED]	iPhone14,4	Hardware v...	1.07 kcal	No
17.07.2023 12:06:27 (...)	17.07.2023 12:13:48 (...)	[REDACTED]	iPhone14,4	Hardware v...	1.79 kcal	No
17.07.2023 12:02:43 (...)	17.07.2023 12:06:53 (...)	[REDACTED]	iPhone14,4	Hardware v...	10.62 kcal	No
17.07.2023 09:42:55 (...)	17.07.2023 09:53:18 (...)	[REDACTED]	iPhone14,4	Hardware v...	14 kcal	No
17.07.2023 09:35:34 (...)	17.07.2023 09:36:13 (...)	[REDACTED]	iPhone14,4	Hardware v...	9.14 kcal	No
17.07.2023 09:23:09 (...)	17.07.2023 09:25:09 (...)	[REDACTED]	iPhone14,4	Hardware v...	0.11 kcal	No
17.07.2023 09:12:41 (...)	17.07.2023 09:14:42 (...)	[REDACTED]	iPhone14,4	Hardware v...	20.2 kcal	No
17.07.2023 08:47:05 (...)	17.07.2023 08:55:59 (...)	[REDACTED]	iPhone14,4	Hardware v...	19.2 kcal	No
17.07.2023 08:38:05 (...)	17.07.2023 08:47:05 (...)	[REDACTED]	iPhone14,4	Hardware v...	0.71 kcal	No

Basal Body Temperature

Cervical Mucus Quality

Menstruation

Sexual Activity

Spotting

Start Date ▼	End Date	Date Added	Source	Device	Details	Menstruation	Was User Entered	
10.07.2023 00:00:00 (...)	10.07.2023 00:00:00 (...)	06.07.2023 10:35:12 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	No
09.07.2023 00:00:00 (...)	09.07.2023 00:00:00 (...)	06.07.2023 10:35:12 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	No
08.07.2023 00:00:00 (...)	08.07.2023 00:00:00 (...)	06.07.2023 10:35:12 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	No
07.07.2023 00:00:00 (...)	07.07.2023 00:00:00 (...)	06.07.2023 10:35:12 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	No

Basal Body Temperature

Cervical Mucus Quality

Menstruation

Sexual Activity

Spotting

Date ▼	Date Added	Source	Device	Details	Was User Entered	Protection Used
06.07.2023 12:00:00 (...)	06.07.2023 13:53:11 (...)	Health	iPhone14,4	Hardware v...	Yes	Yes
26.06.2023 12:00:00 (...)	26.06.2023 18:28:41 (...)	Health	iPhone14,4	Hardware v...	Yes	Yes

22.06.2023 00:00:00 (...)	22.06.2023 00:00:00 (...)	06.07.2023 10:33:47 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	No
21.06.2023 00:00:00 (...)	21.06.2023 00:00:00 (...)	06.07.2023 10:33:47 (...)	Flo	iPhone14,4	Hardware v...	Unspecified	No	Yes
12.06.2023 12:00:00 (...)	12.06.2023 12:00:00 (...)	26.06.2023 18:28:23 (...)	Health	iPhone14,4	Hardware v...	Unspecified	Yes	No
11.06.2023 12:00:00 (...)	11.06.2023 12:00:00 (...)	26.06.2023 18:28:23 (...)	Health	iPhone14,4	Hardware v...	Unspecified	Yes	No
10.06.2023 12:00:00 (...)	10.06.2023 12:00:00 (...)	26.06.2023 18:28:23 (...)	Health	iPhone14,4	Hardware v...	Unspecified	Yes	No
09.06.2023 12:00:00 (...)	09.06.2023 12:00:00 (...)	26.06.2023 18:28:23 (...)	Health	iPhone14,4	Hardware v...	Unspecified	Yes	No
08.06.2023 12:00:00 (...)	08.06.2023 12:00:00 (...)	26.06.2023 18:28:23 (...)	Health	iPhone14,4	Hardware v...	Unspecified	Yes	Yes

Beyond the button...

Changes



Open Project



Save Project



Attach Database



Close Databases

Table: key_value_secure



Filter in any column

	ROWID	category	domain	key	value
	Filter	Filter	Filter	Filter	Filter
22	577	101		user_entered_menstrual_cycle_length	21.0
23	578	101		user_entered_period_cycle_length	5.0
24	589	105	com.apple.Health.favorites	FavoriteIdentifiers	BLOB
25	590	105	com.apple.Health.favorites	UserUpdatedFavorites	1
26	830	101		body_mass	47.3096484375
27	856	105	com.apple.private.health.menstrual-cycles	LastLoggedInCycleTrackingDate	710358818.693455
28	1405	100	com.apple.Safety	HealthChecklistFeatureStatusSnapshot	BLOB
29					
30					
31					

◀ Hide

com_samsung_health_cycle_note

com_samsung_health_cycle_profile

com_samsung_health_cycle_sexual_activity

com_samsung_health_cycle_symptom

com_samsung_health_device_profile

com_samsung_health_cycle_note (1)

com_samsung_health_cycle_note...

com_samsung_health_cycle_note_update_time

Taking test

7/10/2023 10:24:35 PM



July 10

Cycle day 20



Search



Sensual touch



Sex toys



Orgasm



High sex drive



Neutral sex drive



Low sex drive

Mood



Calm



Happy



Energetic



Frisky



Mood swings



Irritated



Sad



Anxious



Depressed



Feeling guilty



Obsessive thoughts



Low energy



Apathetic



Flo Ovulation & Period Tracker

Flo Health Inc.

In-app purchases

4.6★

3.1M reviews

100M+

Downloads

E

Everyone

3:15



Month

Year

S

M

T

W

T

21

22

23

24

25

28

29

30

31

June

1

4

5

6

7

8

11

12

13

14

15

18

19

20

21

22

25

26

27

28

29

July

Edit period dates

Total: 13 Deduplication: 0 Items: 13/840 Selected: 13 Path: samsung_SM-S901U.zip/data/data/org.iggymedia.periodtracker/files/DataModel.realm

Hide

class_NCycle

class_NDeletedC

class_NInstallati

class_NJsonObject

class_NNote

class_NPointEve

class_NPreferen

class_NProfile

class_NRealmDo

class_NRepeatat

class_NSchedule

class_NUser

class_ServerCycleEstimation

class_UserDataSynInfo

metadata

(1)

(2)

(0)

(1)

Mood

Neutral

Mood

Panic

Mood

FeelingGuilty

PregnancyTest

Disturber

Travel

70c07737-38fa-4ee1-af72-fafb189095a

404833a6-d309-4ec9-afb2-e7a0d08c35f8

additionalFields	category	date	subCategory	fValue
class_NJsonObject	Symptom	7/11/2023 4:00:00 AM	Backache	0
class_NJsonObject	Sex	7/10/2023 4:00:00 AM		6
class_NJsonObject	Mood	7/10/2023 4:00:00 AM	Neutral	0
class_NJsonObject	Mood	7/10/2023 4:00:00 AM	Panic	0
class_NJsonObject	Mood	7/10/2023 4:00:00 AM	FeelingGuilty	0
class_NJsonObject	PregnancyTest	7/10/2023 4:00:00 AM		-1
class_NJsonObject	Disturber	7/10/2023 4:00:00 AM	Travel	0
class_NJsonObject	Sport	7/10/2023 4:00:00 AM	Yoga	0
class_NJsonObject	Sport	7/10/2023 4:00:00 AM	Running	0
class_NJsonObject	Water	7/10/2023 4:00:00 AM		1.65592002868652
class_NJsonObject	Fluid	7/10/2023 4:00:00 AM	Sticky	0

G:\Test Data\UFED Apple A2481 iPhone 13 mini 2023_07_13 (001)\AdvancedLogical File System 01\estimations.realm

File Edit View Window Help

CLASSES

EstimationCycleInfoImpl

EstimationCycleServerImpl

EstimationExplanationAnimationImpl

EstimationExplanationCardInfoImpl

EstimationExplanationElementImpl

EstimationExplanationImpl

EstimationExplanationSubElementImpl

EstimationIntervalImpl

realmStartDate

date?

2023-07-06T04:00:00.000Z

2023-07-23T04:00:00.000Z

2023-06-21T04:00:00.000Z

2023-06-08T04:00:00.000Z

2023-05-28T04:00:00.000Z

(SQL) to filter the list

realmT...	realmStartDate	realmLength
int	date?	int
1	2023-07-06T04:00:00.000Z	17
3	2023-07-23T04:00:00.000Z	14
0	2023-06-21T04:00:00.000Z	15
0	2023-06-08T04:00:00.000Z	13
0	2023-05-28T04:00:00.000Z	11
0	2023-05-12T04:00:00.000Z	16
0	2023-04-29T04:00:00.000Z	13
0	2023-04-01T04:00:00.000Z	28



samsung_SM-S901U

File Systems

- com.android.wifi.dialog (0 files, 0 KB)
- com.android.wifi.resources (0 files, 0 KB)
- com.clue.android (88 files, 1,773 KB)
 - cache (18 files, 642 KB)
 - code_cache (0 files, 0 KB)
 - databases (17 files, 956 KB)
 - categories.db
 - categories.db-shm
 - categories.db-wal
 - com.google.android.datatransport.events
 - com.google.android.datatransport.events-journal
 - google_app_measurement_local.db
 - google_app_measurement_local.db-journal
 - LocalCurrentCycleDatabase
 - LocalCurrentCycleDatabase-shm
 - LocalCurrentCycleDatabase-wal
 - snowplowEvents-clue-android.sqlite
 - snowplowEvents-clue-android.sqlite-journal
 - snowplowEvents-clue-android.sqlite-shm
 - snowplowEvents-clue-android.sqlite-wal
 - tracking.db
 - tracking.db-shm
 - tracking.db-wal
 - files (13 files, 20 KB)
 - no_backup (4 files, 144 KB)
 - shared_prefs (36 files, 9 KB)

LocalCurrentCycleDatabase x

Database View

Hex View

File Info

Hide

android_metadata	(1)
LocalCycle	(1)
LocalDailyCategoryGroups	(3)
LocalPhase	(4)
room_master_table	(1)
sqlite_master	(8)

LocalDailyCategoryGroups (3)

date	categoryGroups	cycleId
2023-07-06	Bleeding_Activities	CurrentCycleId
2023-07-11	Bleeding_Activities	CurrentCycleId
2023-06-12	Bleeding	CurrentCycleId

- open-sessions (3 files, 16 KB)
 - 64ADD2140278000114E7552DB29817D9 (3 files, 16 KB)
 - report
 - start-time
 - userlog

NULNULNULË55932

```
$A$:{ "name": "change mode", "parameters": { "mode_change_trigger": "user initiated", "previous_mode": "pregnancy", "o": "app", "sc": "MainActivity", "si": -7694514163121430285, "new_mode": "period_tracking" }}
```

NULNULNULÿ81254

```
$A$:{ "name": "exit_option_modal", "parameters": { "category_option": "[withdrawal]", "previous_category_option": "[]", "o": "app", "sc": "MainActivity", "si": -7694514163121430285, "category": "sex_life", "numeric_category": "false", "relative_date_tracked": "0" }}
```

NULNULNULÿ107458

```
$A$:{ "name": "open_topic", "parameters": { "slot_number": "0", "topic_name": "trying_to_conceive", "o": "app", "sc": "MainActivity", "si": -7694514163121430285 }}
```

NULNUL(SOHE)B135943

```
$A$:{ "name": "exit_option_modal", "parameters": { "category_option": "[unprotected, painfulintercourse]", "previous_category_option": "[]", "o": "app", "sc": "MainActivity", "si": -7694514163121430285, "category": "sex_life", "numeric_category": "false", "relative_date_tracked": "-26" }}
```



Clue Period Tracker & Calendar

Clue Period Tracker by BioWink

In-app purchases

4.4★

1.2M reviews

10M+

Downloads

E

Everyone ⓘ

Install


```
1 select datetime(ZOCCURREDAT+978307200,'unixepoch') from ZMENSTRUATIONLOG
```

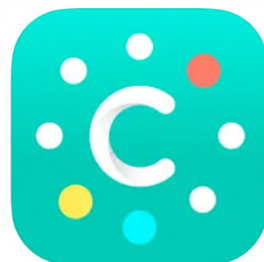
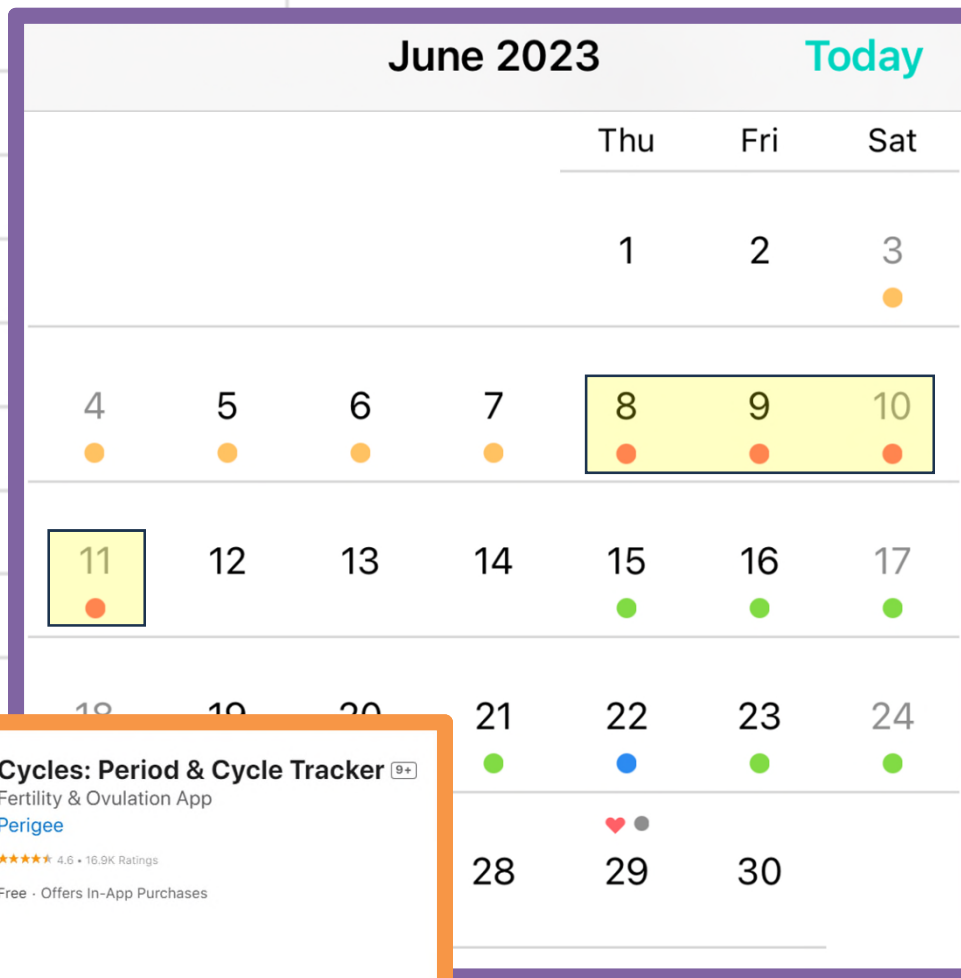
2:49



Enter Passcode

Enter your passcode

	datetime(ZOCCURREDAT+978307200,'unixepoch')
1	2023-05-14 04:00:00
2	2023-05-13 04:00:00
3	2023-05-12 04:00:00
4	2023-06-08 04:00:00
5	2023-05-11 04:00:00
6	2023-06-09 04:00:00
7	2023-06-11 04:00:00
8	2023-05-16 04:00:00
9	2023-05-15 04:00:00
10	2023-06-10 04:00:00
11	2023-07-06 04:00:00
12	2023-07-07 04:00:00
13	2023-07-10 04:00:00



Cycles: Period & Cycle Tracker 9+
Fertility & Ovulation App
[Perigee](#)
★★★★★ 4.6 • 16.9K Ratings
Free · Offers In-App Purchases

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
0		⌫

	start	uid	period	date_str	createDate	pregnancy_date	ID	dueDateSelect	cycle	synced	pregnancy	update_time
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1678939200000	0	2	2023-03-16	1688652983879	NULL	1	0	25	0 0		1688652983879
2	1681099200000	0	4	2023-04-10	1688652983879	NULL	2	0	33	0 0		1688652983879
3	1683950400000	0	4	2023-05-13	1688652983879	NULL	3	0	30	0 0		1688652983879
4	1686542400000	0	4	2023-06-12	1689610514885	NULL	5	0	35	0 1		
5	1689566400000	0	-4	2023-07-17	1689610514886	NULL	6	0	24	0 0		

```
1 select date_str, pregnancyTest, pill, note from note
```

	date_str	pregnancyTest	pill	note
1	2023-07-06	0	NULL	Looked into travel cost for clinics in ...
2	2023-07-14	1	NULL	Get mifepristone

cloud.db

fake.db

LKDB.db

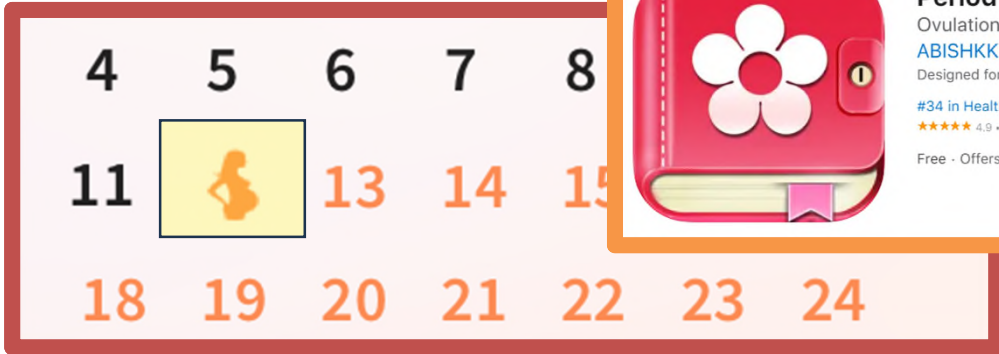
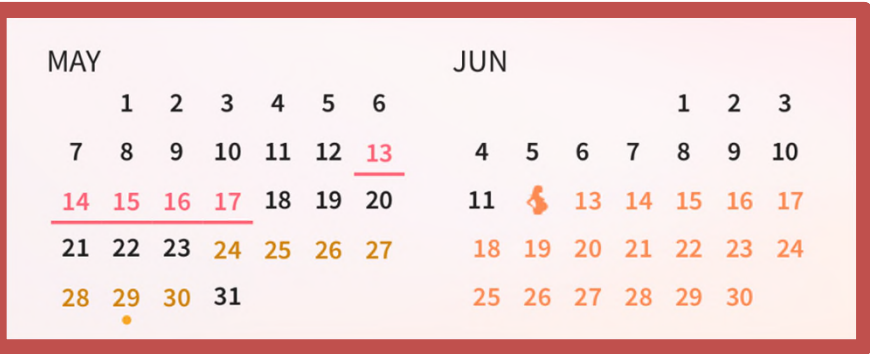
Please input password

Forget password?

2 ABC3 DEF

5 JKL6 MNO

7 PGRS8 TUV9 WXYZ

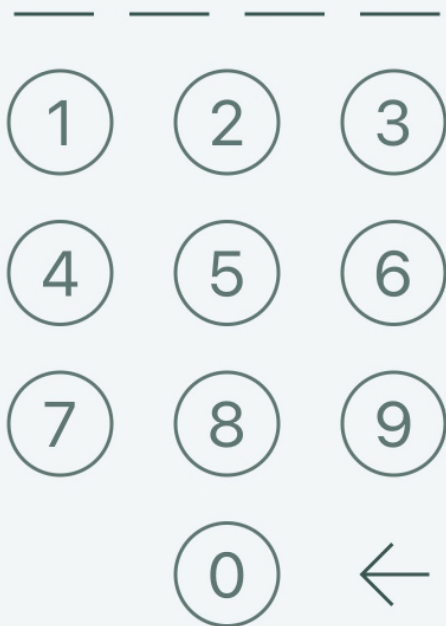


Period Tracker Period Calendar 12+
Ovulation & Cycle My Calendar
[ABISHKKING LIMITED](#).
Designed for iPhone
#34 in Health & Fitness
★★★★★ 4.9 • 128K Ratings
Free · Offers In-App Purchases

3:11



Enter your code



Go

Lite - C:\Users\Allison Young\AppData\Roaming\Apple Computer\MobileSync\Backup\decrypted\AppDomain-com.euki\Library\Application Support\Euki.sqlite

Help

Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Browse Data Edit Pragmas Execute SQL Edit Database Cell

ARIT Filter in... Mode: Binary

ZNOTE	ZAPPOINTMENTS
	Filter
BLOB	
BLOB	
BLOB	
BLOB	
BLOB	

Euki ¹⁷⁺
Sexual health info & tracking
[Women Help Women International Foundation](#)
Designed for iPhone
★★★★★ 4.5 • 62 Ratings
Free

```

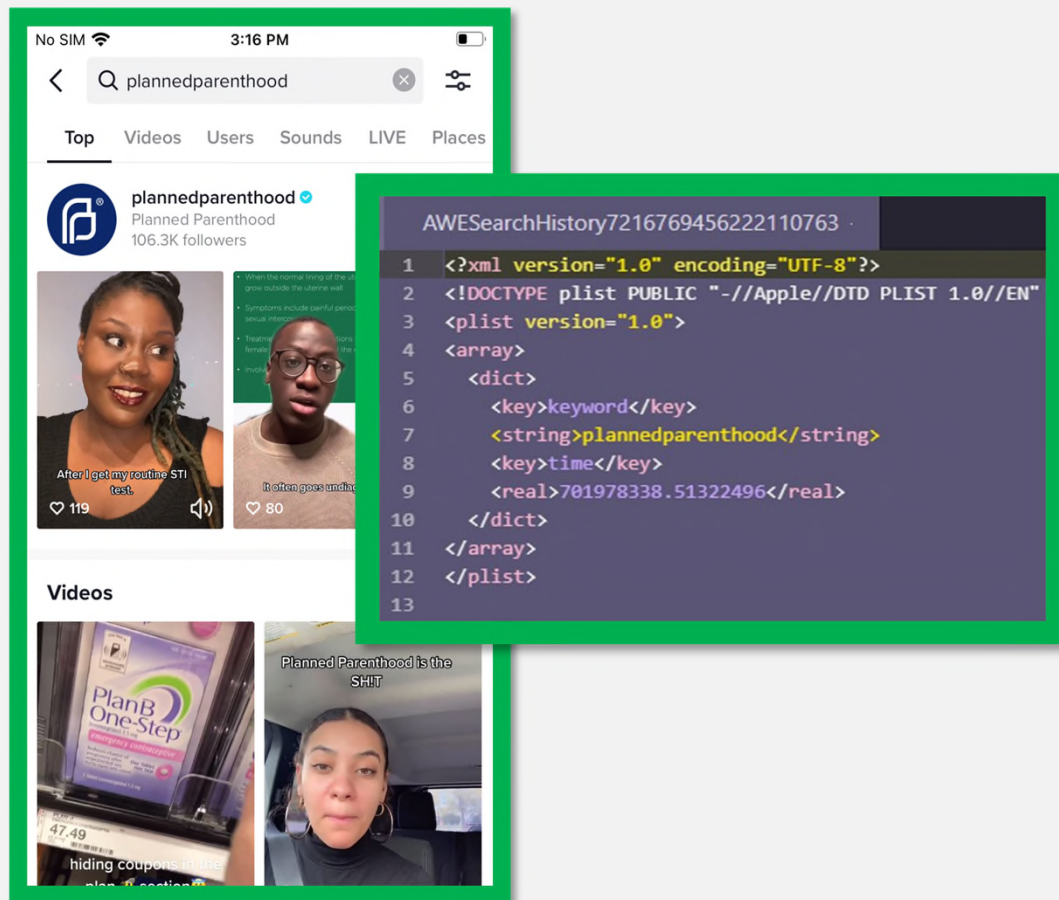
0000 62 70 6c 69 73 74 30 30 d4 01 02 03 04 05 06 07 bplist00.....
0010 0a 58 24 76 65 72 73 69 6f 6e 59 24 61 72 63 68 .X$versionY$arch
0020 69 76 65 72 54 24 74 6f 70 58 24 6f 62 6a 65 63 iverT$topX$objec
1 86 a0 5f 10 0f 4e 53 4b 65 79 65 ts..... ..NSKeye
8 69 76 65 72 d1 08 09 54 72 6f 6f dArchiver...Troo
b 0c 12 20 21 25 2b 2f 55 24 6e 75 t..... !%+/U$nu
e 0f 11 5a 4e 53 2e 6f 62 6a 65 63 ll.....ZNS.objec
3 6c 61 73 73 a1 10 80 02 80 07 d7 tsV$class.....
6 17 18 19 1a 19 19 1d 1e 19 5a 61 .....Za
3 68 6f 77 6e 58 6c 6f 63 61 74 69 lertShownXlocati
4 55 74 69 74 6c 65 54 64 61 74 65 onRidUtitleTdate
0030 5b 61 6c 65 72 74 4f 70 74 69 6f 6e 80 00 80 06 [alertOption....
00c0 80 00 80 00 80 03 80 04 80 00 5f 10 12 44 6f 63 ..... ..Doc
00d0 74 6f 72 20 4b 61 72 65 6e 20 53 6d 69 74 68 d tor Karen Smith.
00e0 22 0e 23 24 57 4e 53 2e 74 69 6d 65 23 41 25 09 ".#$WNS.time#A..
00f0 9b a0 00 00 00 80 05 d2 26 27 28 29 5a 24 63 6c .....&'()Z$cl
0100 61 73 73 6e 61 6d 65 58 24 63 6e 61 73 73 65 73 assnameX$classes
0110 56 4e 53 44 61 74 65 a2 28 5a 58 4e 53 4f 62 6a VNSDate.(*XNSObj
0120 65 62 74 4e 26 27 28 29 5a 24 63 6c ect.&',- ..Euki.
65 6e 74 a2 2e 2a 5f 10 Appointment..* .
70 6f 69 6e 74 6d 65 6e .Euki.Appointmen
53 41 72 72 61 79 a2 30 t.'&'01WNSArray.0
24 00 29 00 32 00 37 00 *.....$.).2.7.
5c 00 62 00 67 00 72 00 I.L.Q.S.\.b.g.r.
2e 00 00 00 a2 00 a5 00 .....
50 01 20 01 02 01 00 00 .....#.(.;>.
00 00 00 02 01 00 00 00 Q.V.^.....
00 00 00 00 00 00 00 00 .....2.....
01e0 00 00 00 01 61 ....a
  
```

```

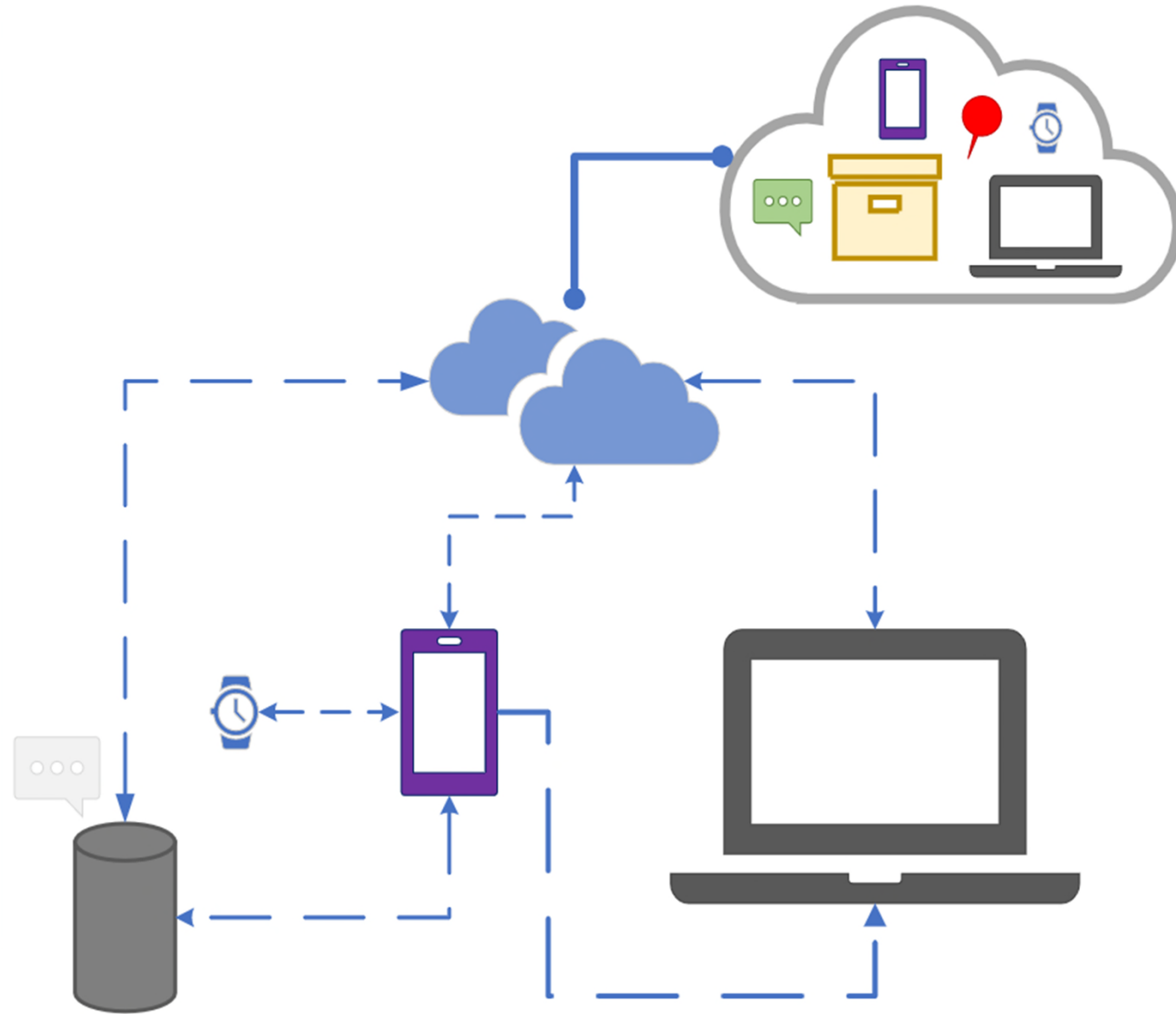
<string>Doctor Karen Smith</string>
<dict>
  <key>NS.time</key>
  <real>705902400.000000<
  <key>$class</key>
  
```

Apple Absolute Time 2023-05-16

Summary of Phone Analysis



- Data artifacts understood by forensic tools included (not limited to):
 - Cached videos (TikTok "watched" content)
 - IOS Snapshots (KTX files)
 - Communications (calls, chat messages)
 - Installed applications, wireless networks, locations (sometimes), photos/videos, search history, device information
 - Health data, including menstrual dates and sexual activity
- Data identified with additional analysis and software:
 - Sqlite databases, Plists, and timestamp values corresponding to...
 - Logged moods, flows, symptoms, notes, medication, appointments, activities, etc. tracked by apps (even where a passcode was set to open the app on the phone)



Cloud Device

- The data can be everywhere
- The data can be nowhere
- If the data exists, there may be multiple full or partial copies
- If the data is deleted, it may be deleted for good... or deleted only from one location and not another

Cloud Data

...why it's even easier for the government to get and harder for you to fight.

Problems with warrants

Lack of scrutiny	Search warrants are largely rubber stamped
Inability to challenge prior to search	Issued ex-parte (in secret) No legal mechanism or adversarial process
Limited avenues for post-search challenges	Who and what can be challenged is limited
Inadequate Remedies for violations	Data obtained from a search can still be used in limited ways even obtained in violation of the law (whether a constitutional violation or otherwise)

Stored Communications Act 18 U.S.C. § 2702(a)

Non-Content

- Subscriber Name
- Contact information
 - Telephone number, address, email
- Account activation date
- Usage information
 - Log in information (IP Addresses)
- Billing information

Content

- Private messages
- “posts”
- Photos
- Documents

When I conducted the interview with C. Burgess I wanted to try and figure out when the miscarriage occurred. C. Burgess scrolled through her messages on her Facebook Messenger account. She showed me where she was trying to message J. Burgess to get her attention. The message showed it was sent on 04-22-22 at 0338 hrs.

I identified the URL of the Facebook account associated with Celeste Burgess (AKA Celeste Kerr) as; [https://www.facebook.com/profile.php?id=100009\[REDACTED\]](https://www.facebook.com/profile.php?id=100009[REDACTED])

I identified the URL of the Facebook account associated with Jessica Burgess (AKA Jessica Kerr) as; [https://www.facebook.com/\[REDACTED\]](https://www.facebook.com/[REDACTED])

- a. Neoselect, or Basic Subscriber Information, for username <https://www.facebook.com/██████████> including, but not limited to, the user identification number, e-mail address, date and time stamp of account creation date, most recent logins, and verification on whether the account was publicly viewable.
- b. Neoprint, or Expanded Subscriber Content, for username <https://www.facebook.com/██████████>, including, but not limited to, profile contact information, wall postings, and friend listing, with Facebook ID's, for dates ranging from April 15th, 2022 through current.
- c. Photoprint of for username <https://www.facebook.com/██████████>, including, but not limited to, all photos uploaded by the user that have not been deleted, along with all photos uploaded by any user which have the requested user tagged in them, for dates ranging from April 15th, 2022 through current..
- d. Private Messages for username <https://www.facebook.com/██████████> for dates ranging from April 15th, 2022 through current.
- e. IP log for username <https://www.facebook.com/██████████>, for dates ranging from April 15th, 2022 through current.

June 7, 2022

a & e can be obtained
without a warrant.

Challenging Cloud Data

In spite of the SCA creating an implicit (or explicit) privacy expectation, there is still no universally recognized reasonable expectation of privacy in cloud data – including social media, email, etc...

Courts have been slow to acknowledge both the expectation of privacy in digital data and the limitations of the third-party doctrine in the modern world. Riley v. California, 573 U.S. 373 (2014); U.S. v. Jones, 565 U.S. 400 (2012); Carpenter v. U.S. 138 S. Ct. 2206 (2018); United States v. Warshak, 631 F.3d 266 (6th Cir., 2010).

The Founders didn't know about the Cloud

“More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.

U.S. v. Jones, 565 U.S. 400 (2012)(Sotomayor, J. concurrence)

Easy for them

Law Enforcement Online Requests



Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

[Request Access](#)

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).

[About](#) [Create Ad](#) [Create Page](#) [Developers](#) [Careers](#) [Privacy Policy](#) [Cookies](#) [Ad choices](#) [Terms](#) [Help](#)

Meta © 2023

[English \(US\)](#) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [Italiano](#) [한국어](#) [Deutsch](#) [हिन्दी](#) [日本語](#) [+](#)



Hard for us

Re: Subpoena: The People of the State of New York v. [REDACTED]

Dear [REDACTED]

We represent Facebook, Inc. ("Facebook"), the provider of the Facebook and Instagram services, and write in response to the subpoena you issued on behalf of a criminal defendant in the above-referenced matter. At the onset, Facebook tried to contact you via email, [REDACTED] by sending their objections, but the email was erroneously sent to [REDACTED]. Regardless, for the reasons stated below, Facebook cannot fulfill the subpoena. Please contact me directly to meet and confer if you disagree with any of our objections.

Facebook is headquartered in California, and the custodians who have control over Facebook's data are located out of state. Therefore, any subpoena in a New York criminal matter must comply with the Uniform Act to Secure the Attendance of Witnesses from Without a State in Criminal Proceedings ("Uniform Act"), which applies to the production of documents as well as demands for the attendance of live witnesses. Pursuant to the Uniform Act, a criminal litigant cannot compel the production of documents from Facebook's out-of-state records custodians without presenting the appropriate certification to the San Mateo County Superior Court, scheduling a hearing, and obtaining an order from the California court for production. *See* CPL § 640.10; Cal. Penal Code §§ 1334, *et seq.*; *In re Codey*, 82 N.Y.2d 521, 525-26 (1993) ("The Uniform Act provides detailed and constitutionally valid procedures whereby a party to a criminal proceeding in one State can either obtain the presence of a witness residing in another State or can compel the production of evidence located in another State."). While we understand New York has historically exercised subpoena power over corporations "doing business" in state, the Supreme Court's decision in *Daimler AG v. Bauman* limited the "doing business" doctrine to those places in which a corporation is "at home," which the Court identified as its "place of incorporation and principal place of business." 134 S. Ct. 746, 760 (2014). As a

Cloud Investigations

Cloud Data

```
"placeVisit": {
  "location": {
    "latitudeE7": 4[REDACTED]
    "longitudeE7": -7[REDACTED]
    "placeId": "C[REDACTED]",
    "address": "[REDACTED] NY",
    "name": "GYN [REDACTED]",
    "sourceInfo": {
      "deviceTag": 987676980
    },
    "locationConfidence": 95.0402,
    "calibratedProbability": 82.679184
  },
  "duration": {
    "startTimestamp": "2023-02-[REDACTED].316",
    "endTimestamp": "2023-02-[REDACTED].006Z"
  },
  "placeConfidence": "HIGH_CONFIDENCE",
  "centerLatE7": 4[REDACTED],
  "centerLngE7": -7[REDACTED],
  "visitConfidence": 92,
  "otherCandidateLocations": [{
    "latitudeE7": 4[REDACTED],
    "longitudeE7": -7[REDACTED],
    "placeId": "C[REDACTED]",
    "address": "[REDACTED] NY",
    "name": "[REDACTED] Healthcare",
    "locationConfidence": 2.2561026,
    "calibratedProbability": 1.9626719
  }]
```

Search

Searched for [abortion law in new york state](#)

Mar 31, 2023, 2:43:10 PM EDT

Products:

Search

Locations:

At [this general area](#) - Based on your past activity

Why is this here?

This activity was saved to your Google Account because the following settings

Takeout > Google Fi > Content > Voicemails V1



Voicemail.2023.0
2.-- 13.47.58
Z.mp3

+1 917-[REDACTED]
Feb [REDACTED], 8:48 AM • 00:13

Hello, good morning. My name is M [REDACTED]. I'm calling from [REDACTED] GYN [REDACTED]. I'm calling regarding [REDACTED].

Thank you and have a great day.

0:00 0:13

▶ 🔊 🔗 🗑️

```
"usage_timestamp": [
  [REDACTED] 13320184042000000,
  [REDACTED] 13320184237000000
],
"name": "practice_visit_reason_id",
"value": "REDACTED"
```

"alexa is abortion legal in my state"

Yesterday 6:47 PM Allison Allison's Echo Dot

▶ "alexa how do i get abortion pills at home"

"Here's something I found on Reference.com: "

"According to Planned Parenthood, it is possible to end a pregnancy at home by having a medication abortion. This method relies on two different medications to terminate the pregnancy first and then cause the uterus to empty."

Allison

🗑️ Delete recording

Yesterday 6:47 PM Allison Allison's Echo Dot

You searched Facebook

"Planned Parenthood"

Apr 11, 2023 10:13:33am

You searched Facebook

"brooklyn abortion clinic"

Apr 11, 2023 10:15:13am

Your Data Request



Notes

- 2023-06-29: Close call with partner.

Sexual Activities

- 2023-06-29: Used Protection
- 2023-07-01: Did Not Use Protection
- 2023-07-06: Did Not Use Protection

2. The Personal Data we process about you

Natural Cycles may process the following kinds of personal data about you (collectively referred to as “Personal Data”):

Account Data	includes registration date, payment plan and whether you have an active subscription or not.
Contact Data	includes address, billing address, delivery address, email address and telephone number.
Device Data	includes device identifier, your mobile operating system, the type of mobile browser you use and time zone setting.
IP Data	includes your approximate position based on your IP address.
Identity Data	includes first name, last name, username and date of birth.

Personal Data We Collect

We collect the following categories of personal data in connection with our Services:

Category	Examples of Data We Collect In this Category
Identifiers	Name, email address, postal address Device identifiers such as IP address, AdID, IDFA For Enterprise members, employer ID
General personal information including health information	Date of birth, date of last period, due date, and other fertility, pregnancy, health, sex life and life circumstances information you input into the apps or discuss as part of health coaching services In the Parenting app, health and milestone information for your child For Enterprise members, health insurance information

Activity on this account

This feature provides information about the last activity on this account.

This account does not seem to be open in any other location. Here's why:

Visit [Security Checkup](#) for more details

Providers log info like IP address, times, device info

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser (Chrome) Show details	* United States (NJ) (173.██████████)	4:31 pm (0 minutes ago)
Browser (Chrome) Show details	* United States (NJ) (173.██████████)	4:08 pm (23 minutes ago)
Authorized Application (██████████) Show details	United States (NJ) (71.██████████)	Jul 11 (6 days ago)
Authorized Application () Show details	United States (NJ) (71.██████████)	Jul 9
Authorized Application () Show details	United States (NY) (204.██████████)	Jul 7
Authorized Application (██████████) Show details	United States (NY) (2600:██████████)	Jul 2
Authorized Application () Show details	United States (NJ) (71.██████████)	Jun 26
Authorized Application (██████████) Show details	United States (NY) (2600:██████████)	Jun 23
Authorized Application (██████████) Show details	United States (NJ) (71.██████████)	Jun 19

Active sessions

July 17, 2023



██████████ was logged in on Windows PC.

Created Jul 8, 2022, 12:24 PM Updated Jul 17, 2023, 4:15 PM IP address 173.██████████ Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

4:15 PM

July 12, 2023



██████████ was logged in on Windows PC.

Created Jun 30, 2022, 9:56 AM Updated Jul 12, 2023, 11:09 AM IP address 204.██████████ Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

11:09 AM

May 19, 2023



██████████ was logged in on Windows PC.

Created Oct 26, 2022, 12:27 PM Updated May 19, 2023, 12:26 PM IP address 204.██████████ Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

12:26 PM

April 11, 2023



██████████ was logged in on Windows PC.

Created Feb 6, 2023, 11:55 AM Updated Apr 11, 2023, 9:26 AM IP address 71.██████████ Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

9:26 AM

March 31, 2023



██████████ was logged in on Windows PC.

Created Feb 9, 2023, 3:41 PM Updated Mar 31, 2023, 1:37 PM IP address 204.██████████ Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

1:37 PM

Service Instagram
Target [REDACTED]
Generated 2018-[REDACTED]
Date Range 2004-[REDACTED] UTC to 2018-[REDACTED] UTC
Name [REDACTED] First [REDACTED]

Registered [REDACTED]@gmail.com
Email
Addresses

Vanity Name [REDACTED]

Registration 2017-[REDACTED]
Date

Registration Ip [REDACTED]

Account Account Still true
Closure Date Active

Phone
Numbers

Logins IP Address [REDACTED]
Time 2017-[REDACTED]
IP Address [REDACTED]
Time 2017-[REDACTED]
IP Address [REDACTED]
Time 2017-[REDACTED]

Service Facebook
Target [REDACTED]
Generated 2018-[REDACTED]
Date Range 2004-[REDACTED] UTC to 2018-[REDACTED] UTC
Name [REDACTED] First [REDACTED]
Middle [REDACTED]
Last [REDACTED]

Registered [REDACTED]
Email
Addresses

Vanity Name [REDACTED]

Registration 2017-[REDACTED]
Date

Registration Ip [REDACTED]

Account Account Still true
Closure Date Active

Phone [REDACTED] Cell Verified on 2017-[REDACTED]
Numbers [REDACTED] Other Unverified

Logins IP Address [REDACTED]
Time [REDACTED]
Location WWW
IP Address [REDACTED]
Time [REDACTED]
Location WWW

Data returned by a
subpoena (not a warrant)

Summary of Cloud Analysis

- **Data can still be in the cloud:**
 - Google Location History (sensitive locations should be removed, but other information may be used for building a timeline)
 - Search history across Google, Facebook, Alexa, etc
 - Voicemails (sometimes) and voice recordings
 - Autofill data with surprising contents (ex. form field to make an appointment at a medical office)
 - Synced reproductive data for certain lifestyle apps/services
- **Subscriber information doesn't need a warrant**
 - Account information & dates and times of service access provided for other services without a warrant

Updating the 4th Amendment for the digital age

Application for search warrants should not be done ex-parte (in secret)

- traditional concerns about destruction of evidence are inapplicable in this context

Provide opportunity to object to a warrant for a phone or other digital data prior to execution

- make it an adversarial process, just like everything else, with findings by a judge on the record.

Acknowledge a constitutional expectation of privacy in cloud and digital data generally

- Do away with the Third-Party Doctrine

Create best practices and protocols for limiting searches – either technologically or via “taint teams.”

- Puts a stop to overbroad and unbridled searches of data “search everything because it can be anywhere”

Any post-execution litigation of a warrant must be in front of a different judge, de novo, and not be given a presumption of validity

- Increases the level of scrutiny at all steps of the process

Get rid of the Good Faith Exception

- An easter egg for the fellow defense attorneys in the room

Conclusion:

Defending the Digital Body

- Data is collected and retrievable to show you've committed a crime regardless of whether you have committed a crime
 - Flawed security in technology
 - Flawed security (of your privacy) in the law
- Legal privacy protections are lacking, especially when being "tough on crime"
- *Dobbs* has extended the umbrella of people who may be investigated using private, personal digital information

References

- > United States v. Jones, 565 U.S. 400 (2012)
- > Riley v. California, 573 U.S. 373 (2014)
- > Carpenter v. United States, 138 S. Ct. 2206
- > United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)
- > Stored Communications Act 18 U.S. Code Â§ 2703
- > Aziz Z. Huq & Rebecca Wexler, Digital Privacy for Reproductive Choice in the Post-Roe Era, 98 NYUL Rev 555 [2023]
- > Congressional Research Service, "Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview", (July 8, 2022 Update), Available at: <https://crsreports.congress.gov/product/pdf/LSB/LSB10786>
- > Conti-Cook, Cynthia, "Surveilling the Digital Abortion Diary" (October 28th, 2020). University of Baltimore Law Review: Vol. 50: Iss. 1, Article 2. Available at: <https://scholarworks.law.ubalt.edu/ublrvol50/iss1/2>
- > Downing, Andrea, "Health Advertising on Facebook: Privacy and Policy Considerations," (August 15th, 2022). Patterns. Available at <https://doi.org/10.1016/j.patter.2022.100561>
- > Fowler, Leah R. and Ulrich, Michael R., Femtechnodystopia (May 3, 2022). Stanford Law Review, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=4099764> or <http://dx.doi.org/10.2139/ssrn.4099764>
- > Gallagher, William, "What Apple surrenders to law enforcement when issued a subpoena," (January 21st, 2020). Apple Insider. Available at: <https://appleinsider.com/articles/20/01/21/what-apple-surrenders-to-law-enforcement-when-issued-a-subpoena>
- > Huss et. al, "Self-Care Criminalized: August 2022 Preliminary Findings," If/When/How. Available at <https://www.ifwhenhow.org/resources/self-care-criminalized-preliminary-findings/>
- > Koepke, Logan and Emma Weil, Urmila Janardan, Tinuola Dada, Harlan Yu, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones" (October 20th, 2020). Upturn. Available at <https://www.upturn.org/work/mass-extraction/>
- > Paltrow LM, Flavin J. "Arrests of and forced interventions on pregnant women in the United States, 1973-2005: implications for women's legal status and public health." J Health Polit Policy Law. 2013 Apr;38(2):299-343. doi: 10.1215/03616878-1966324. Epub 2013 Jan 15. PMID: 23262772.
- > "Pregnancy Justice, Arrests and Prosecutions of Pregnant People, 1973-2020." Available at <https://www.pregnancyjusticeus.org/arrests-and-prosecutions-of-pregnant-women-1973-2020/>
- > Rajesh, Ananya Mariam and Jeffrey Dastin, "Google to delete location history of visits to abortion clinics," (July 1st, 2022). Reuters. Available at <https://www.reuters.com/world/us/google-delete-location-history-visits-abortion-clinics-2022-07-01/>
- > Sunde, Nina and Itiel E. Dror, "A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making," Forensic Science International: Digital Investigation, Volume 37, 2021, 301175, ISSN 2666-2817, <https://doi.org/10.1016/j.fsidi.2021.301175>. (Accessed from <https://www.sciencedirect.com/science/article/pii/S2666281721000834> on July 2nd, 2023)
- > Wexler, Rebecca, "Privacy As Privilege: The Stored Communications Act and Internet Evidence" (August 13, 2020). 134 Harv. L. Rev. 2721 (2021). Available at SSRN: <https://ssrn.com/abstract=3673403>

Further Reading

> Cole, Samantha, "Apple Health Data Is Being Used as Evidence in a Rape and Murder Investigation," (January 11th, 2018). Vice Media Group. Available at: <https://www.vice.com/en/article/43q7qq/apple-health-data-is-being-used-as-evidence-in-a-rape-and-murder-investigation-germany>

> Cuthbertson, Anthony. "Amazon ordered to give Alexa evidence in double murder case," (November 14th, 2018). The Independent. Available at: <https://www.independent.co.uk/tech/amazon-echo-alexa-evidence-murder-case-a8633551.html>

> Feathers, et. Al. "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," (June 16th, 2022). The Markup. Available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

> Federal Trade Commission, "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others," (June 22, 2021). Available at: <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

> Federal Trade Commission: In the Matter of Flo, Inc., Case Summary and Timeline, available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>

> Germain, Thomas, "FTC Fines GoodRx \$1.5M for Sending Your Medication Data to Facebook and Google for Ads," (February 9th, 2021). Gizmodo. Available at <https://gizmodo.com/ftc-fines-goodrx-prescription-data-facebook-google-1850059096>.

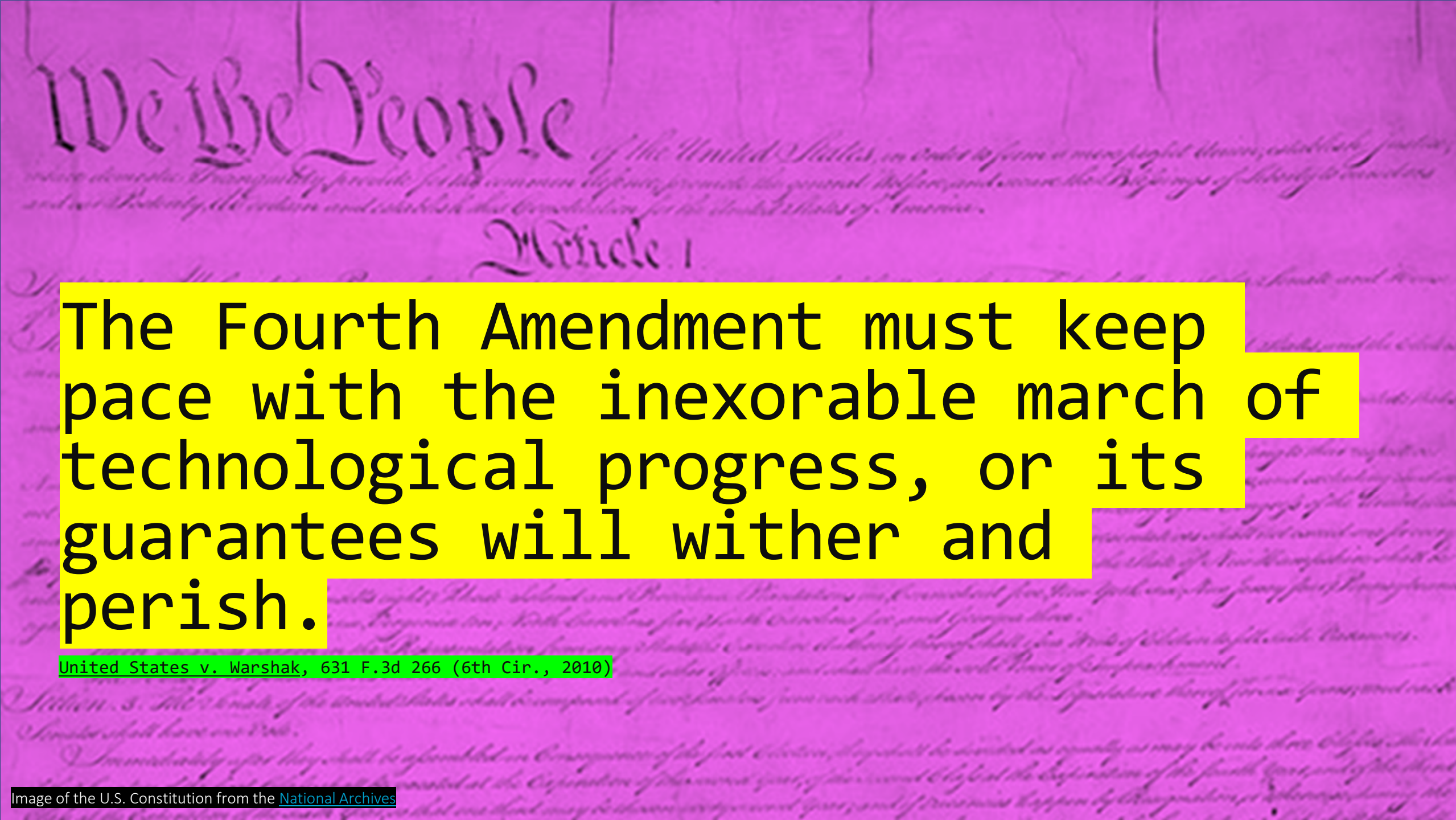
> Guide to Abortion Privacy, available at <https://digitaldefensefund.org/ddf-guides/abortion-privacy>

> "How to turn on Advanced Data Protection for iCloud," (January 19th, 2023). Apple Support. Available at: <https://support.apple.com/en-us/HT212520>

> Joyce, Stephen, "Court Allows Use of Facebook Live, Internet Searches as Evidence," (December 20th, 2022). Bloomberg Industry Group, Inc. Available at: <https://news.bloomberglaw.com/us-law-week/court-allows-use-of-facebook-live-internet-searches-as-evidence>

> Peterson, M., "Apple Health data used to convict man in wife's death," (February 9th, 2021), AppleInsider. Available at: <https://appleinsider.com/articles/21/02/09/apple-health-data-used-to-convict-man-in-wifes-death>

> Pratt, Mark. "Google searches to be key in prosecuting Brian Walshe's murder trial, experts say (January 27th, 2023). CBS News. Available at: <https://www.cbsnews.com/boston/news/ana-walshe-murder-case-brian-walshe-google-internet-searches-cohasset-massachusetts/>



The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.

United States v. Warshak, 631 F.3d 266 (6th Cir., 2010)