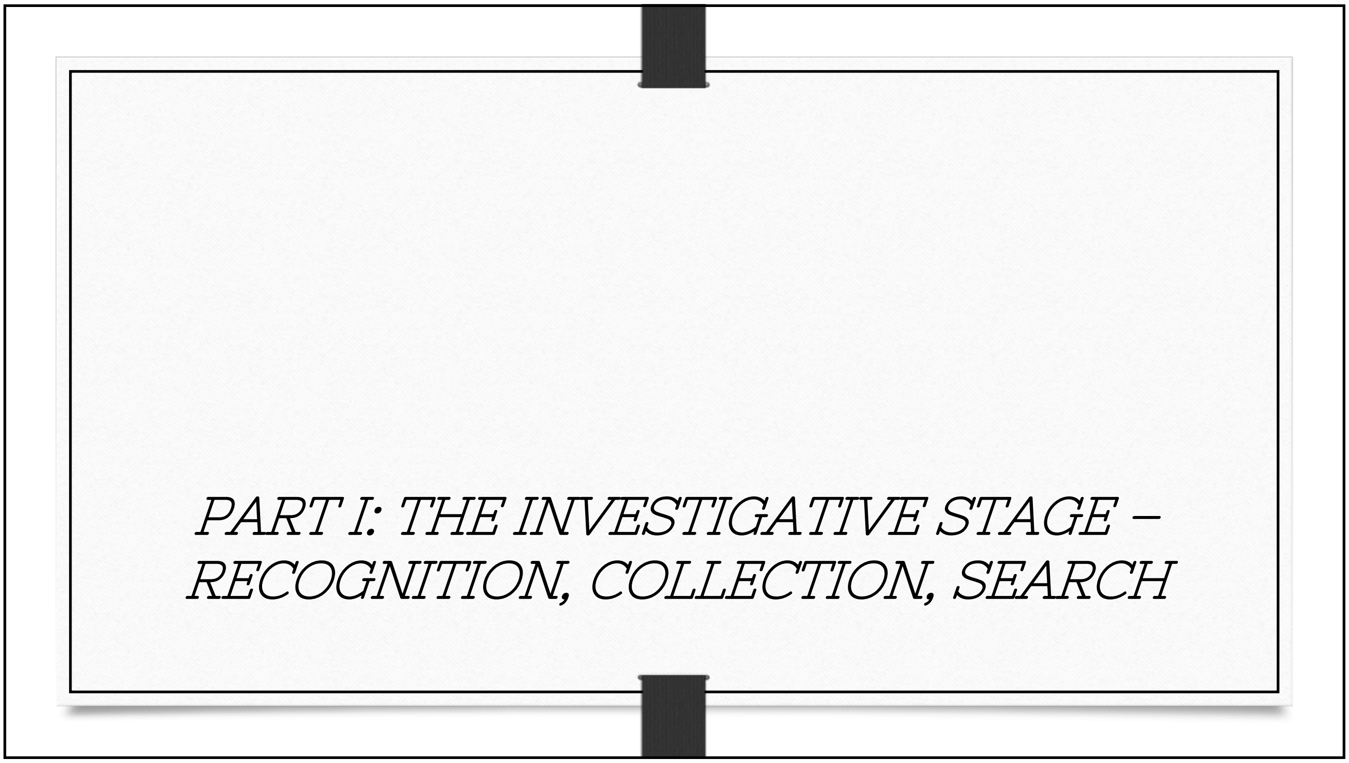
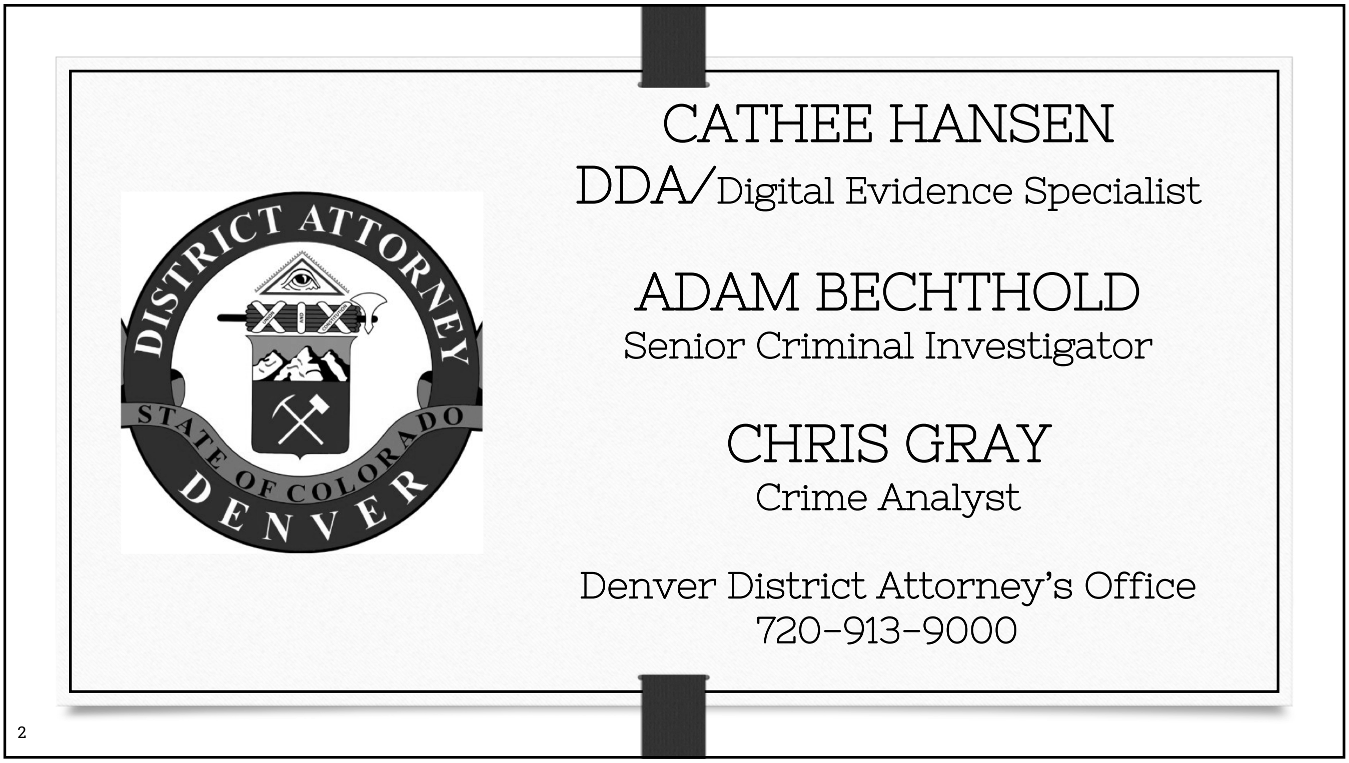


PART I: THE INVESTIGATIVE STAGE – RECOGNITION, COLLECTION, SEARCH



CATHEE HANSEN
DDA/Digital Evidence Specialist

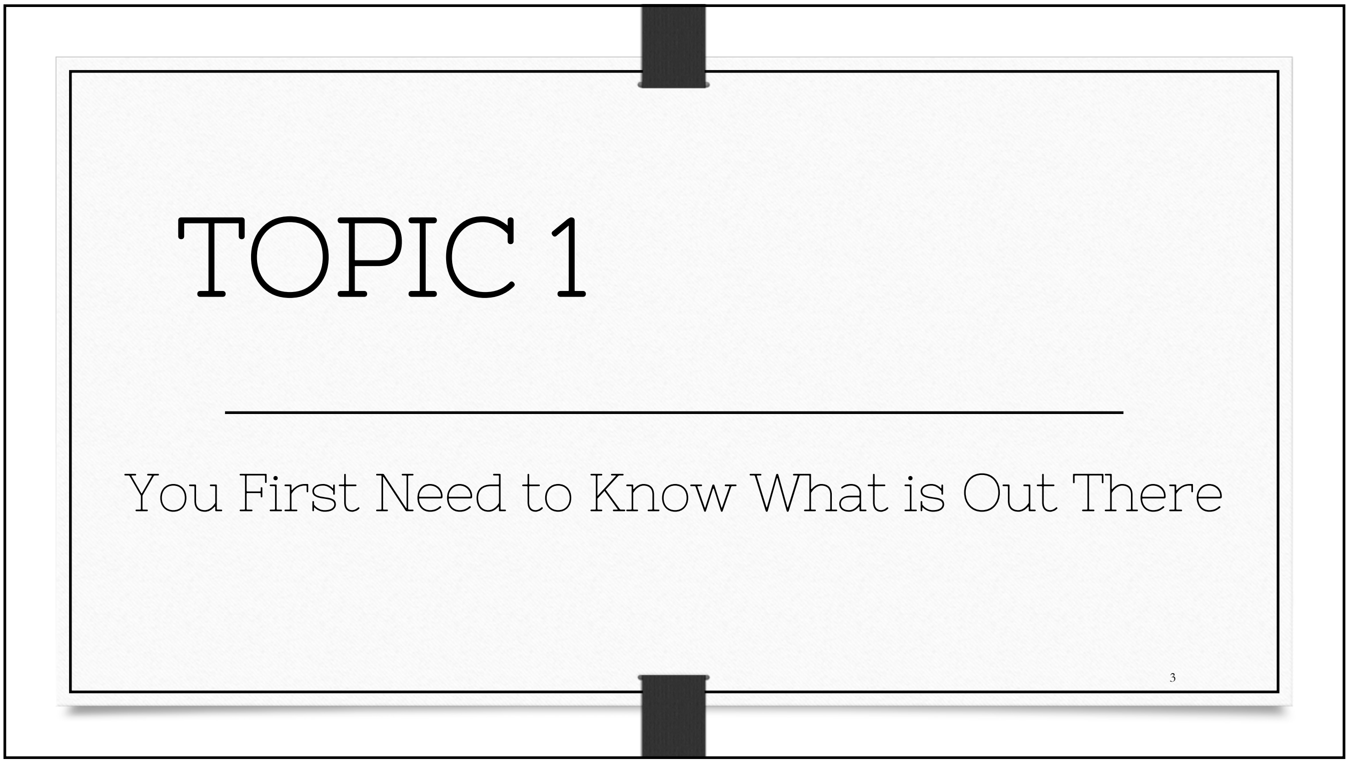
ADAM BECHTHOLD
Senior Criminal Investigator

CHRIS GRAY
Crime Analyst

Denver District Attorney's Office
720-913-9000

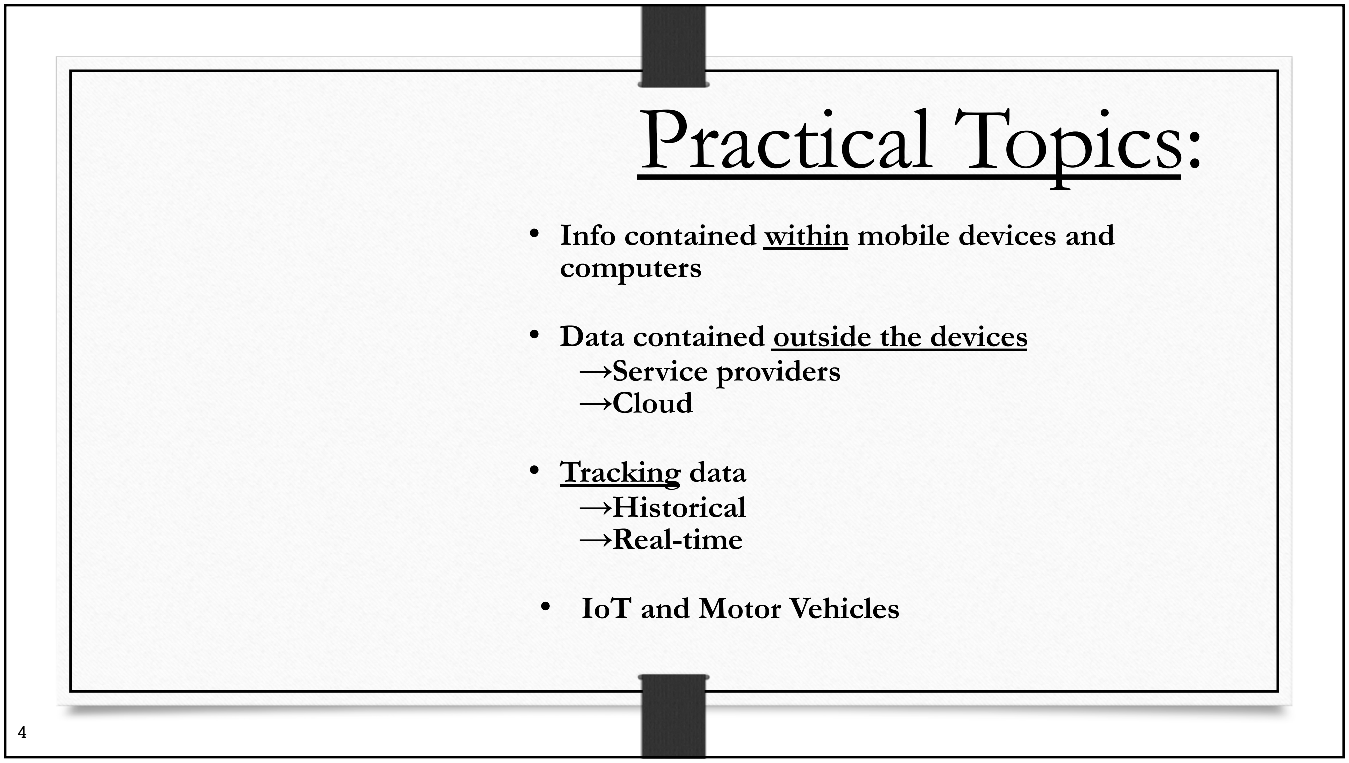
2

© Denver District Attorney's Office



TOPIC 1

You First Need to Know What is Out There



Practical Topics:

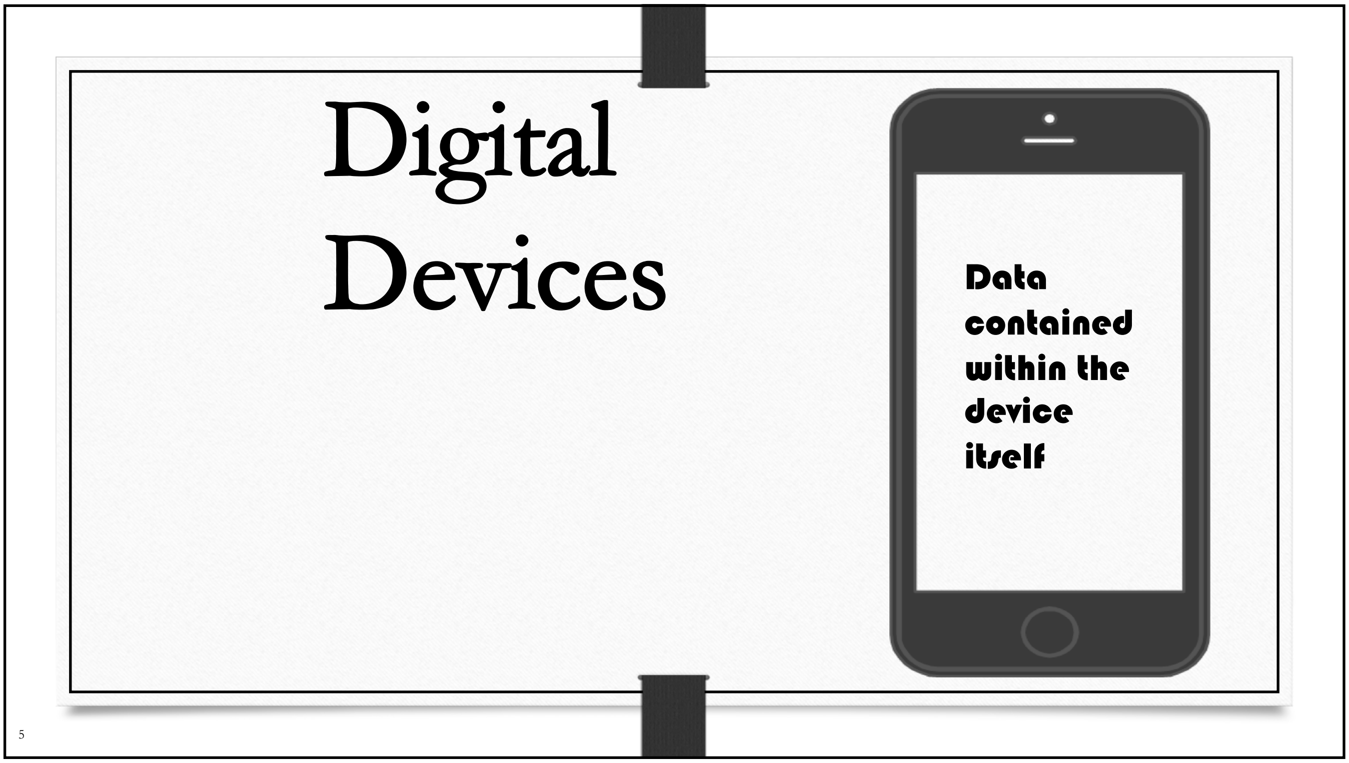
- **Info contained <u>within</u> mobile devices and computers**

- **Data contained <u>outside the devices</u>**
  →Service providers
  →Cloud

- **<u>Tracking</u> data**
  →Historical
  →Real-time

- **IoT and Motor Vehicles**

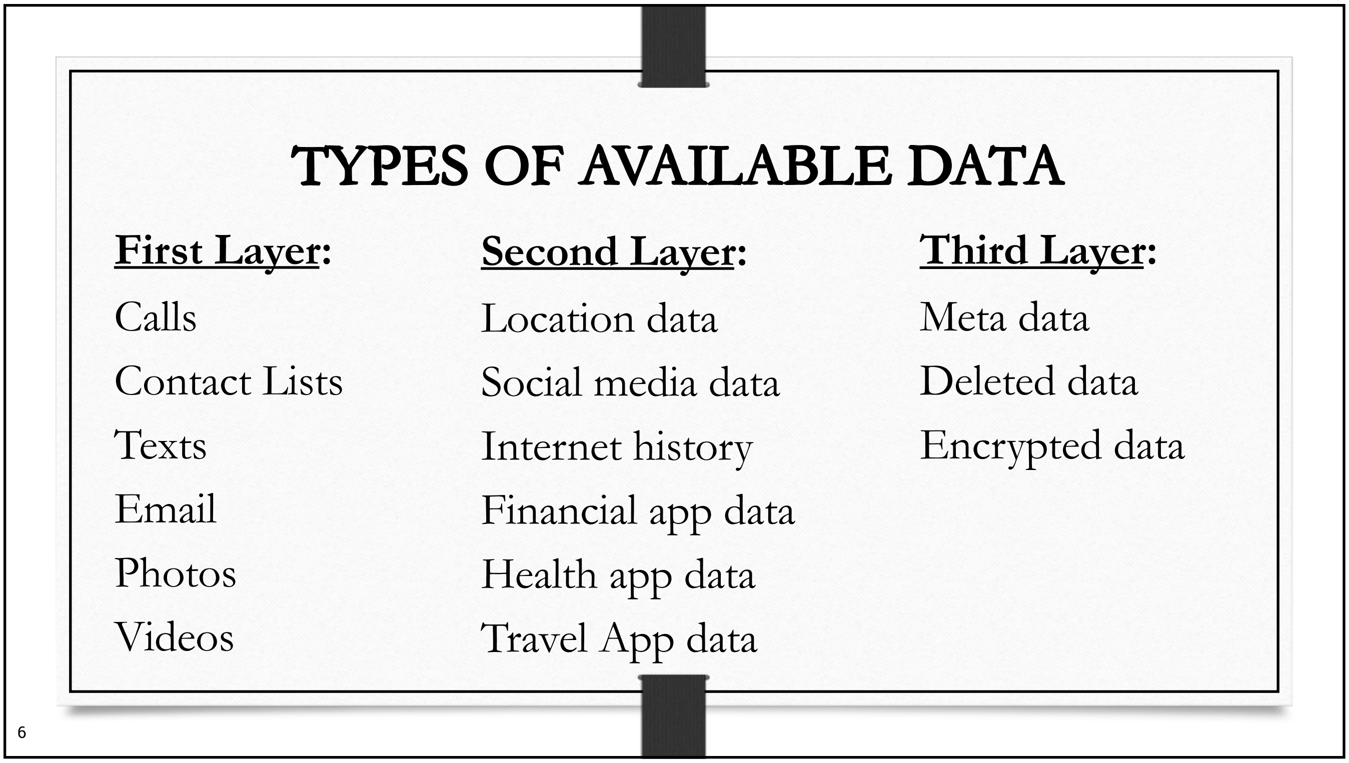
© Denver District Attorney’s Office



Digital Devices

Data contained within the device itself

5



TYPES OF AVAILABLE DATA

First Layer:

Calls

Contact Lists

Texts

Email

Photos

Videos

Second Layer:

Location data

Social media data

Internet history

Financial app data

Health app data

Travel App data

Third Layer:

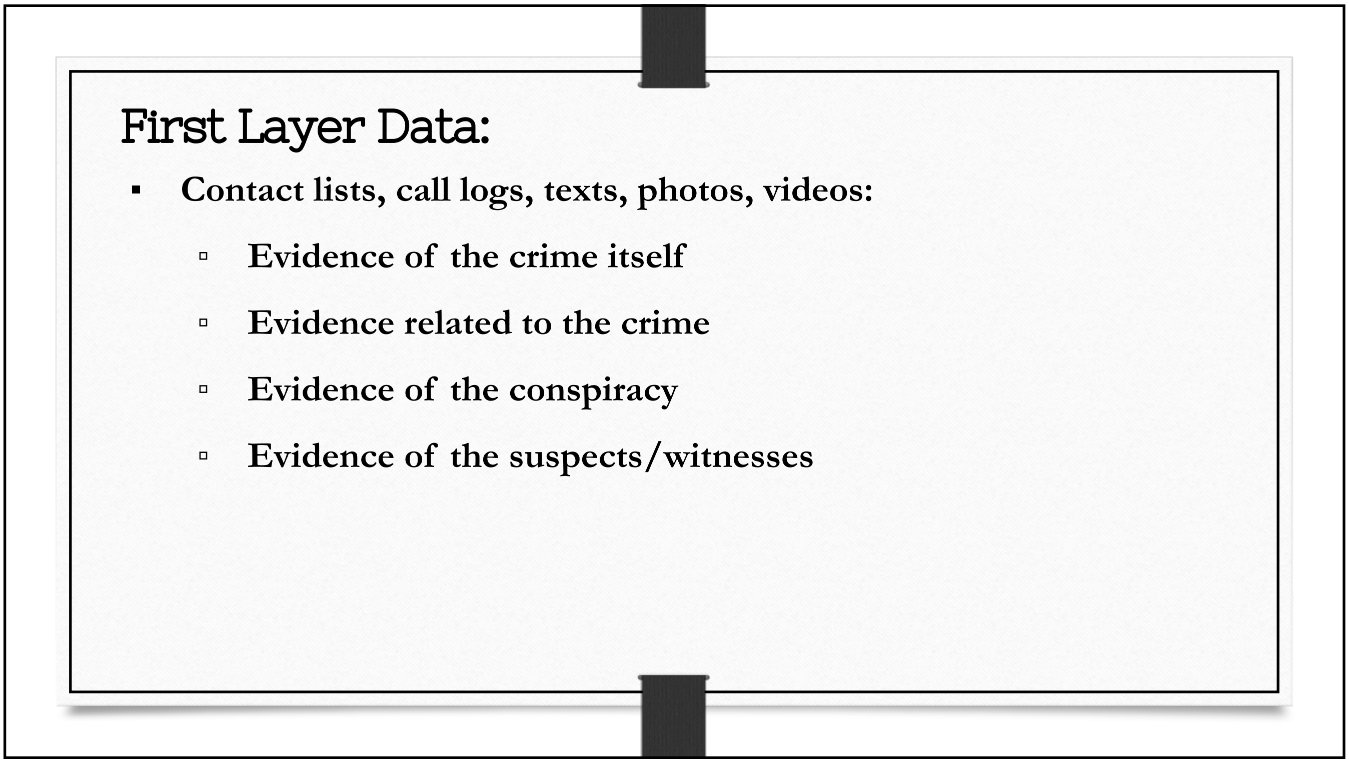
Meta data

Deleted data

Encrypted data

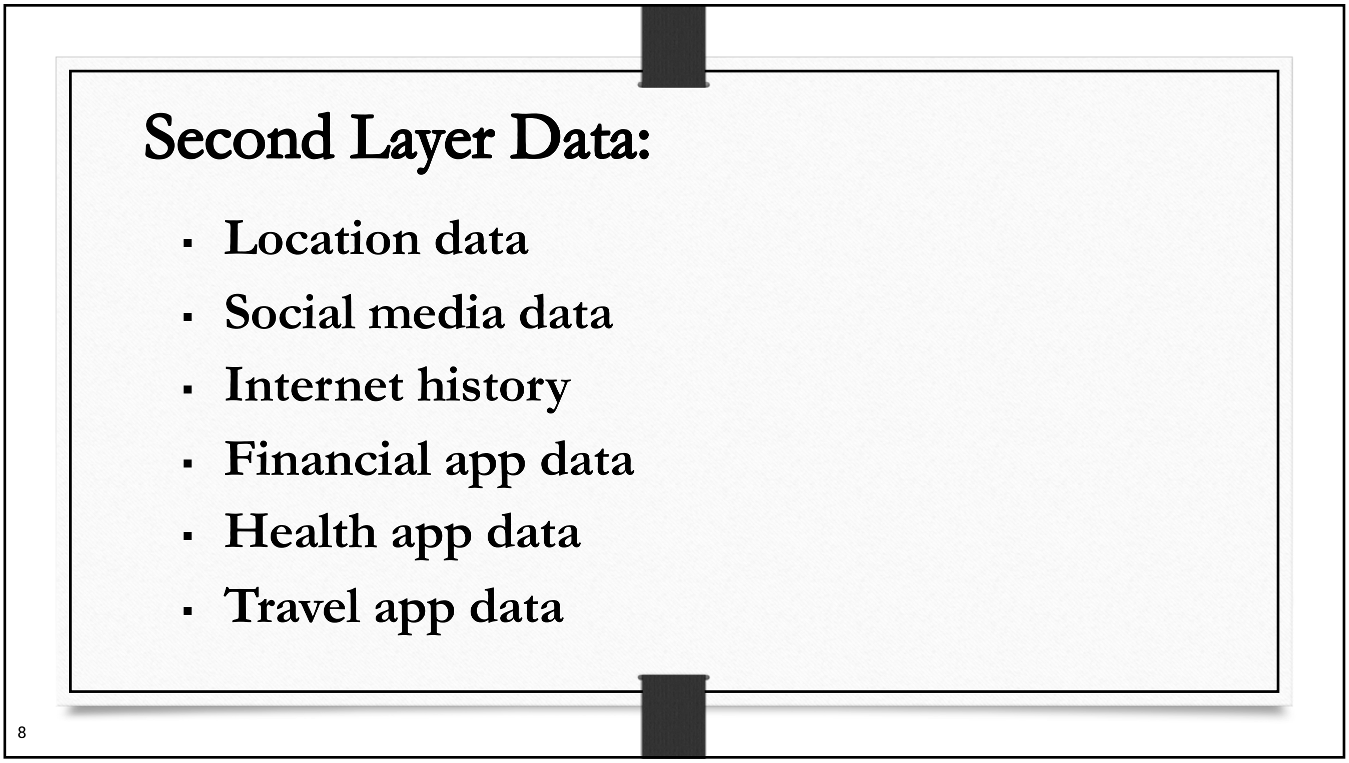
6

© Denver District Attorney's Office



First Layer Data:

- Contact lists, call logs, texts, photos, videos:
  - Evidence of the crime itself
  - Evidence related to the crime
  - Evidence of the conspiracy
  - Evidence of the suspects/witnesses

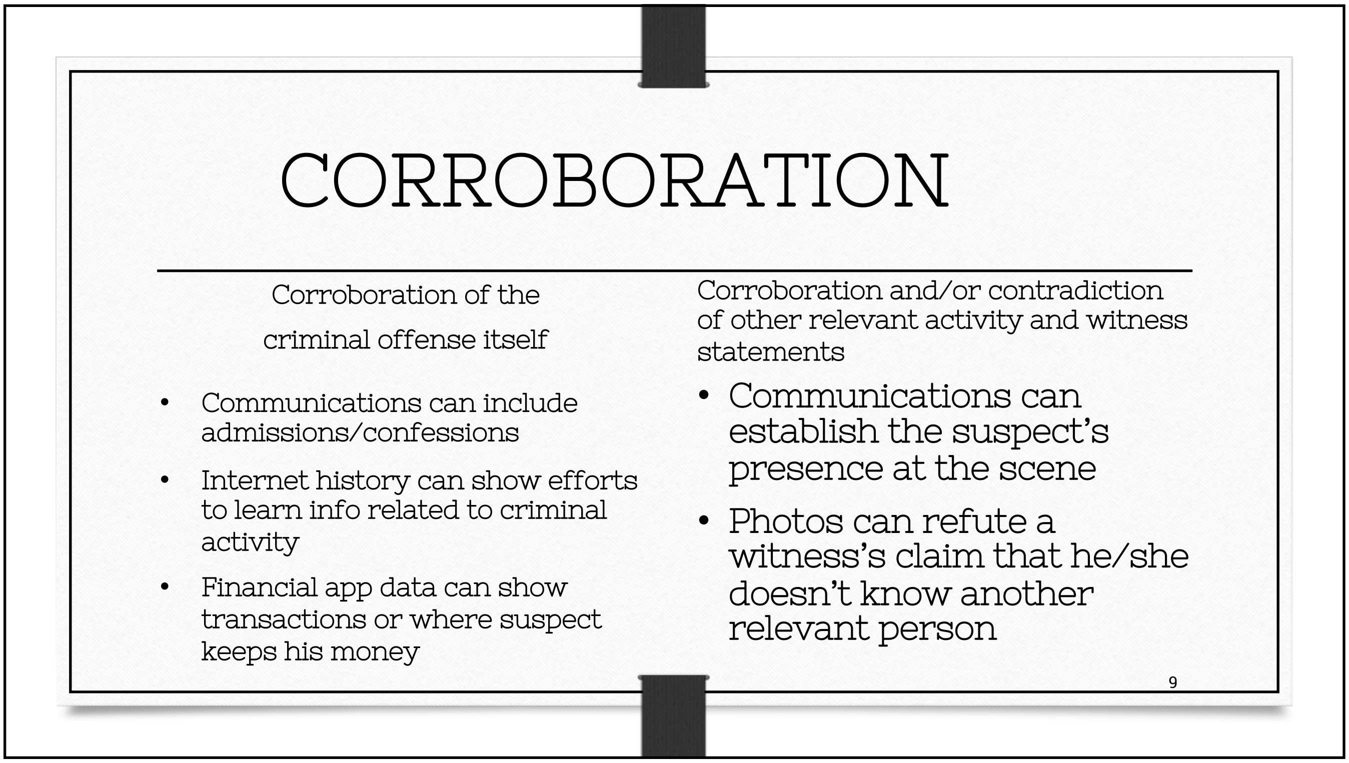


Second Layer Data:

- Location data
- Social media data
- Internet history
- Financial app data
- Health app data
- Travel app data

8

© Denver District Attorney's Office



CORROBORATION

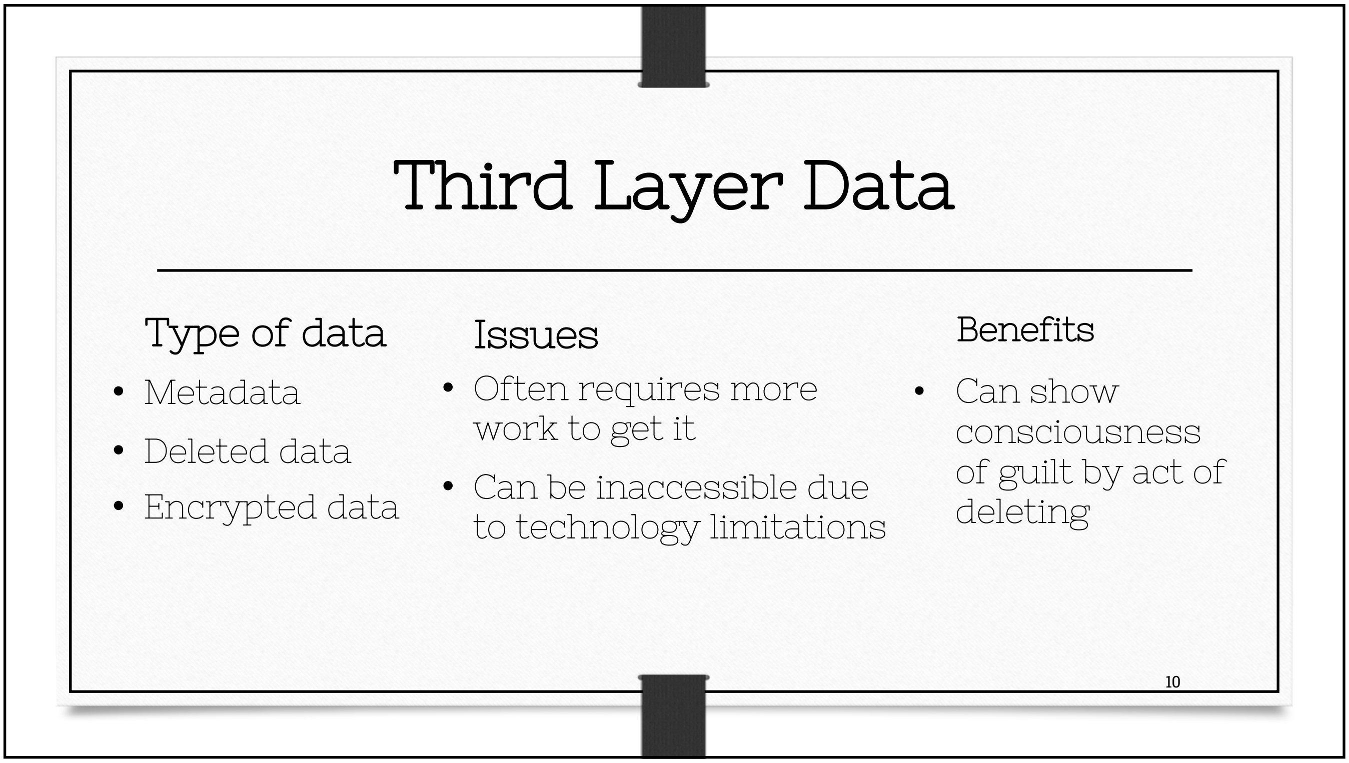
Corroboration of the criminal offense itself

- Communications can include admissions/confessions
- Internet history can show efforts to learn info related to criminal activity
- Financial app data can show transactions or where suspect keeps his money

Corroboration and/or contradiction of other relevant activity and witness statements

- Communications can establish the suspect's presence at the scene
- Photos can refute a witness's claim that he/she doesn't know another relevant person

9



Third Layer Data

Type of data

- Metadata
- Deleted data
- Encrypted data

Issues

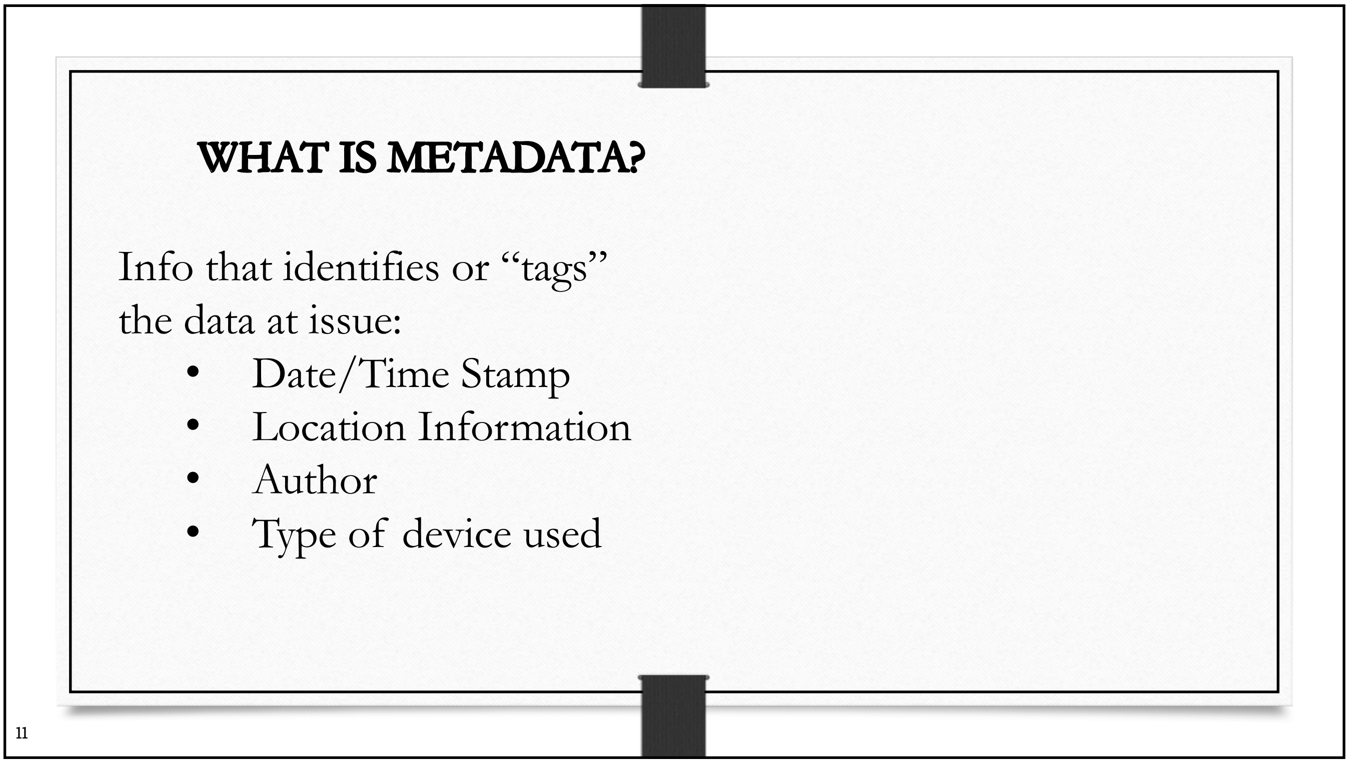
- Often requires more work to get it
- Can be inaccessible due to technology limitations

Benefits

- Can show consciousness of guilt by act of deleting

10

© Denver District Attorney's Office

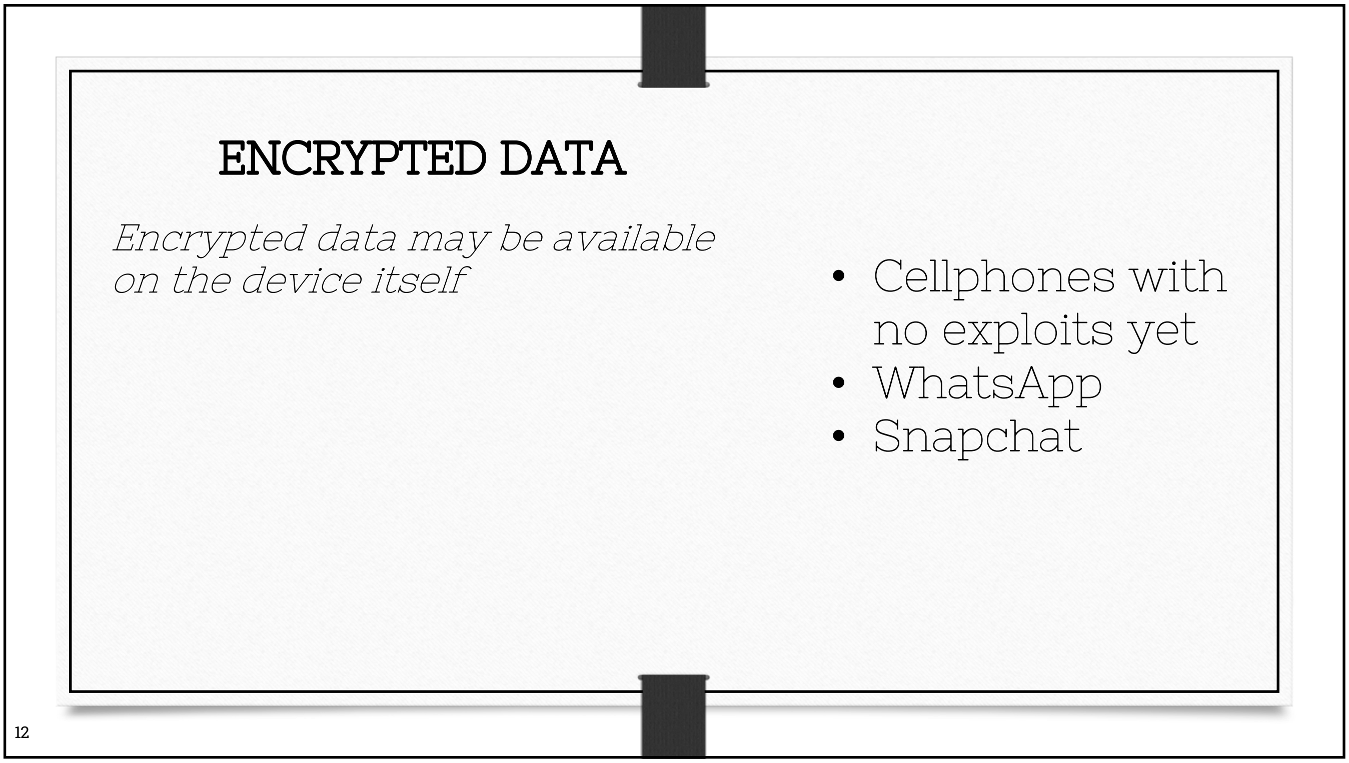


WHAT IS METADATA?

Info that identifies or "tags" the data at issue:

- Date/Time Stamp
- Location Information
- Author
- Type of device used

11

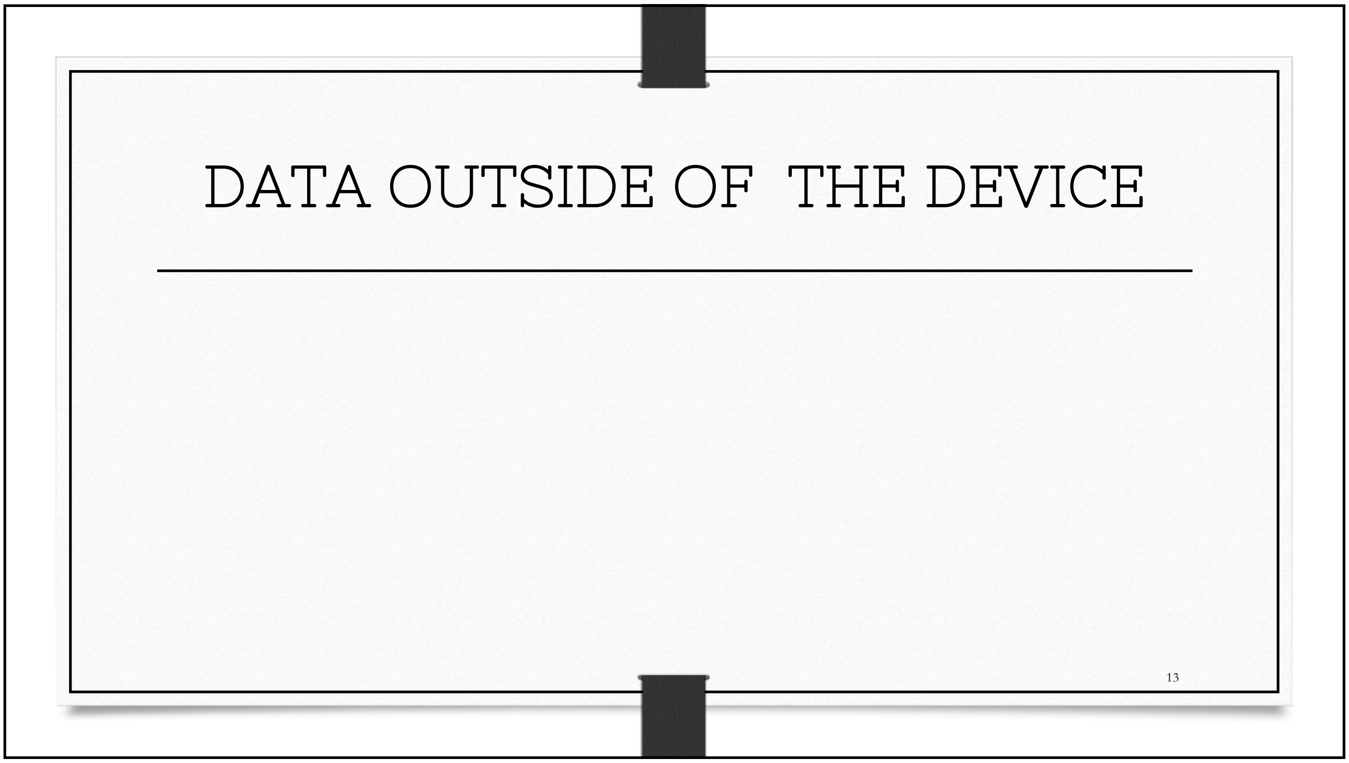


ENCRYPTED DATA

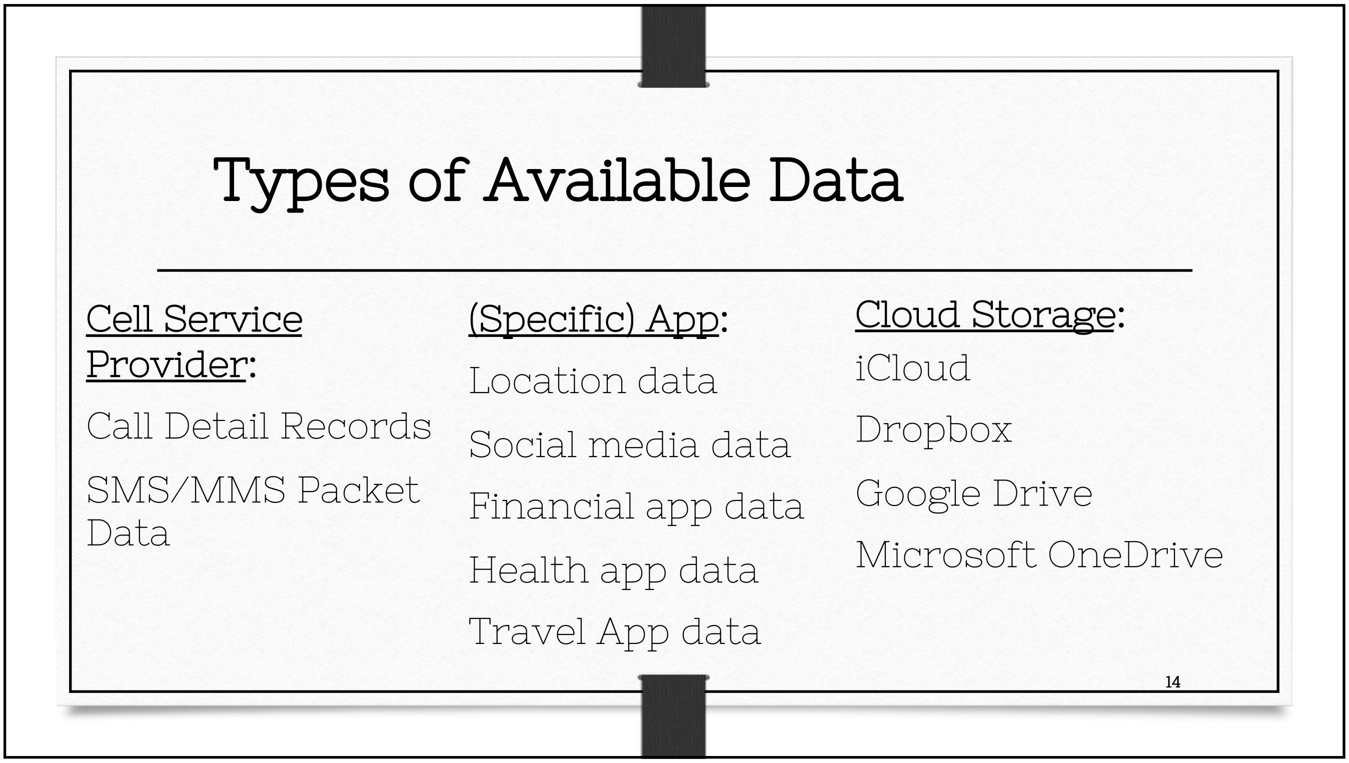
Encrypted data may be available on the device itself

- Cellphones with no exploits yet
- WhatsApp
- Snapchat

12



DATA OUTSIDE OF THE DEVICE



Types of Available Data

Cell Service Provider:

- Call Detail Records
- SMS/MMS Packet Data

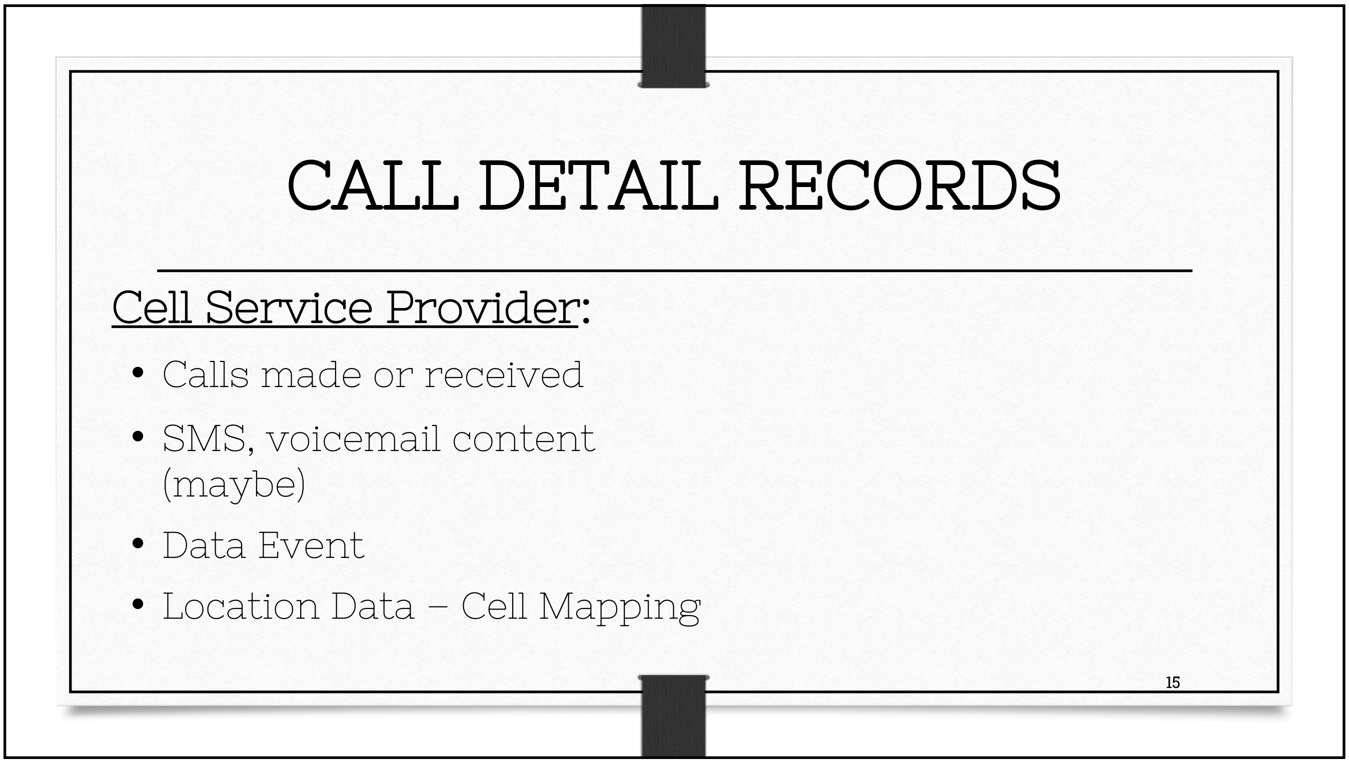
(Specific) App:

- Location data
- Social media data
- Financial app data
- Health app data
- Travel App data

Cloud Storage:

- iCloud
- Dropbox
- Google Drive
- Microsoft OneDrive

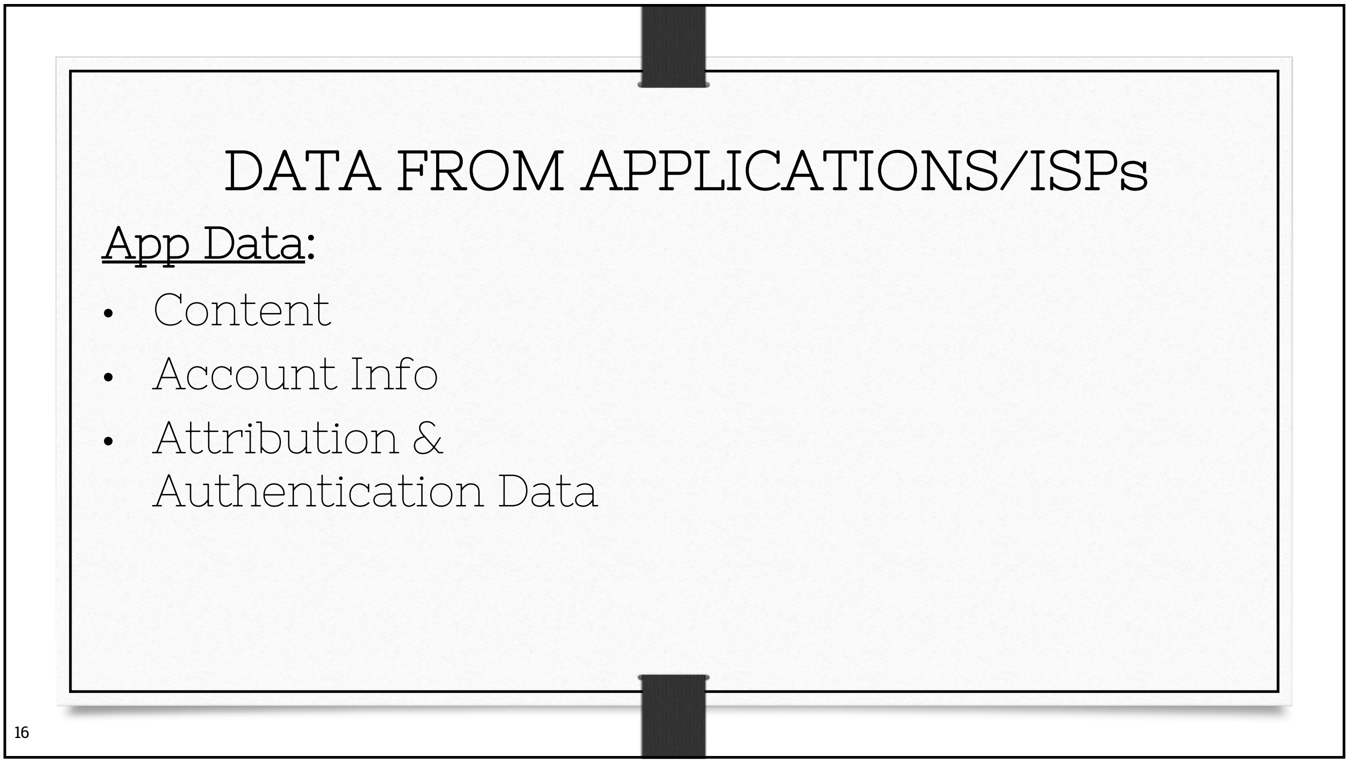
© Denver District Attorney's Office



CALL DETAIL RECORDS

Cell Service Provider:

- Calls made or received
- SMS, voicemail content (maybe)
- Data Event
- Location Data – Cell Mapping

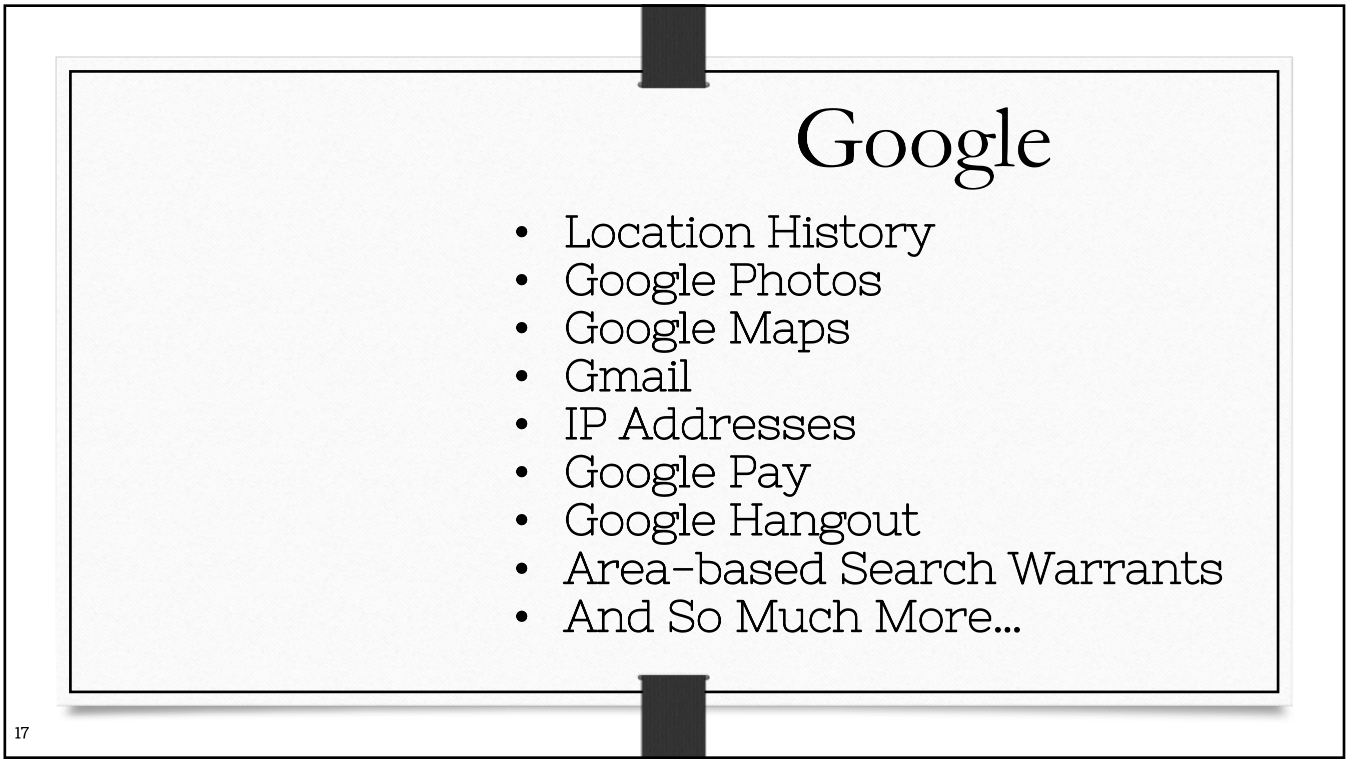


DATA FROM APPLICATIONS/ISPs

App Data:

- Content
- Account Info
- Attribution & Authentication Data

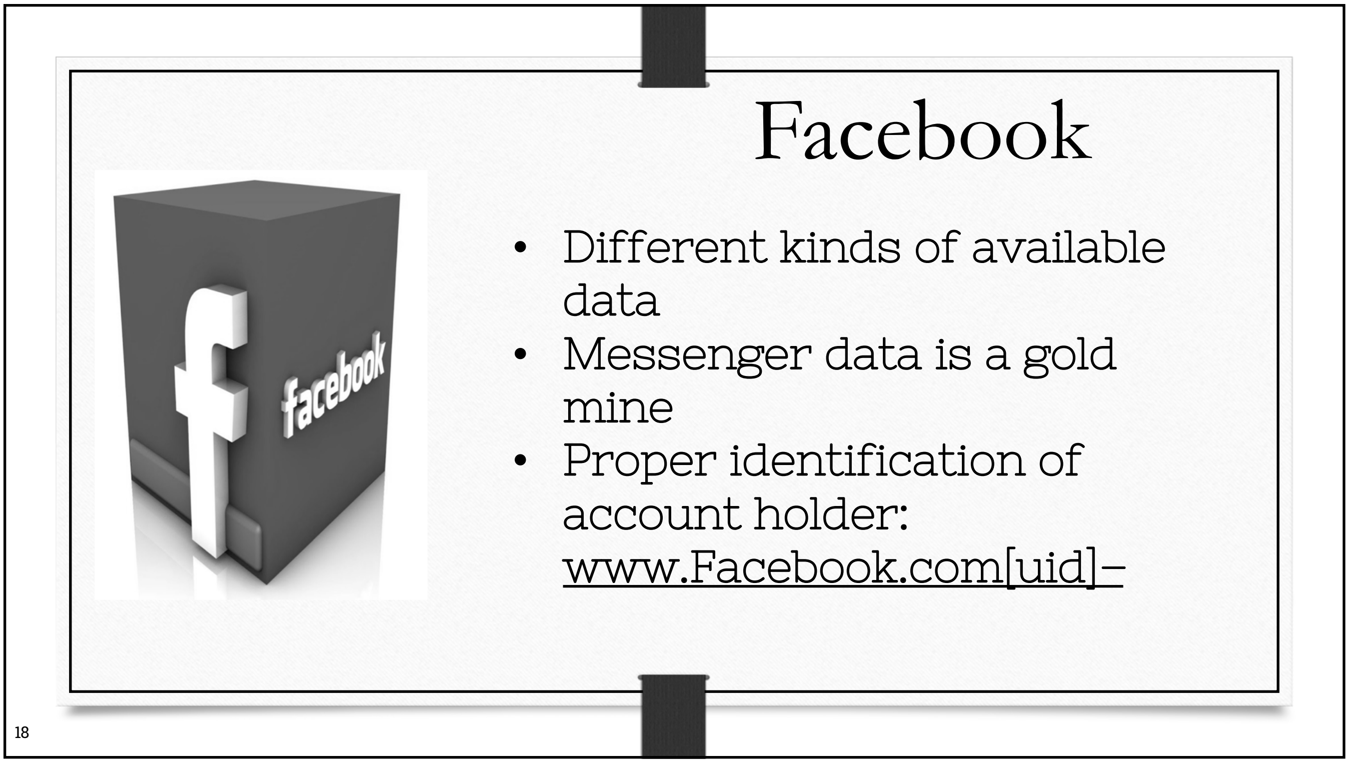
© Denver District Attorney’s Office



Google

- Location History
- Google Photos
- Google Maps
- Gmail
- IP Addresses
- Google Pay
- Google Hangout
- Area-based Search Warrants
- And So Much More…

17

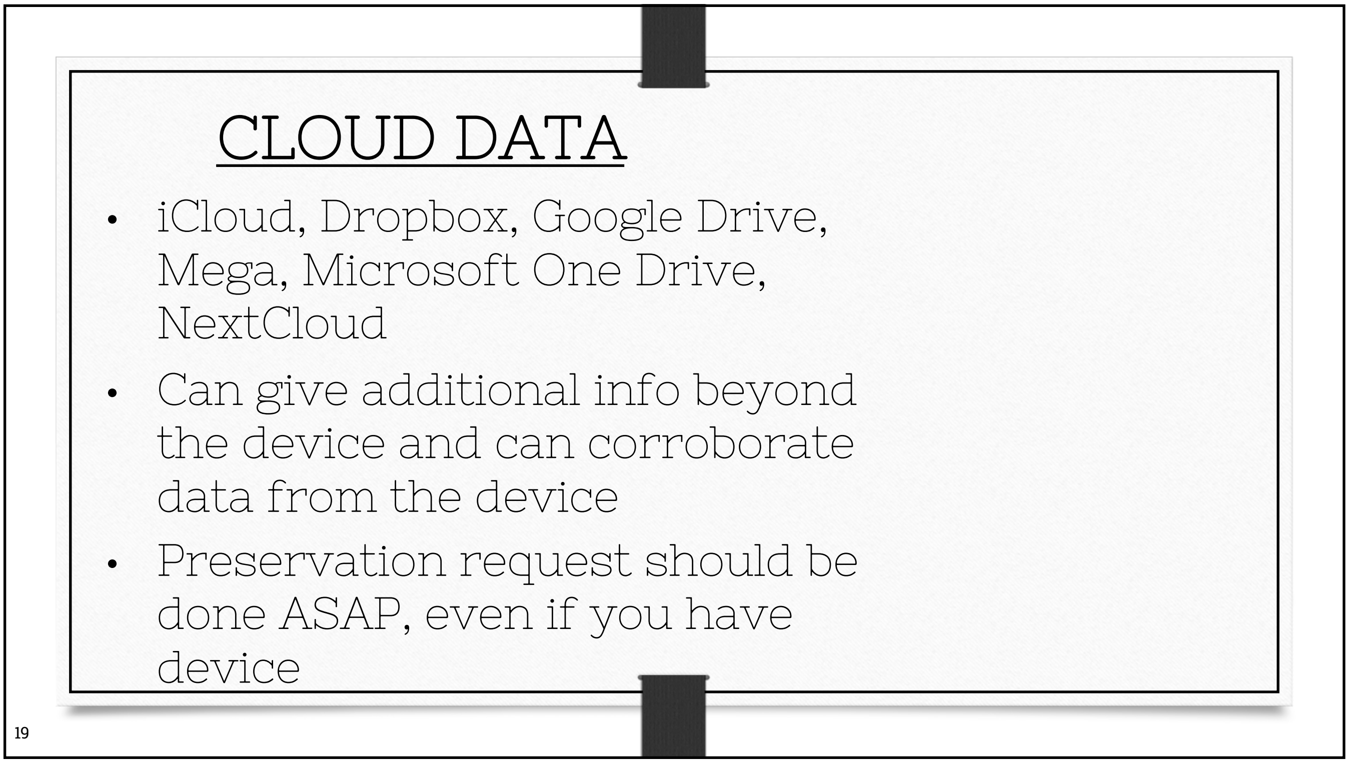


Facebook

- Different kinds of available data
- Messenger data is a gold mine
- Proper identification of account holder: www.Facebook.com[uid]-

18

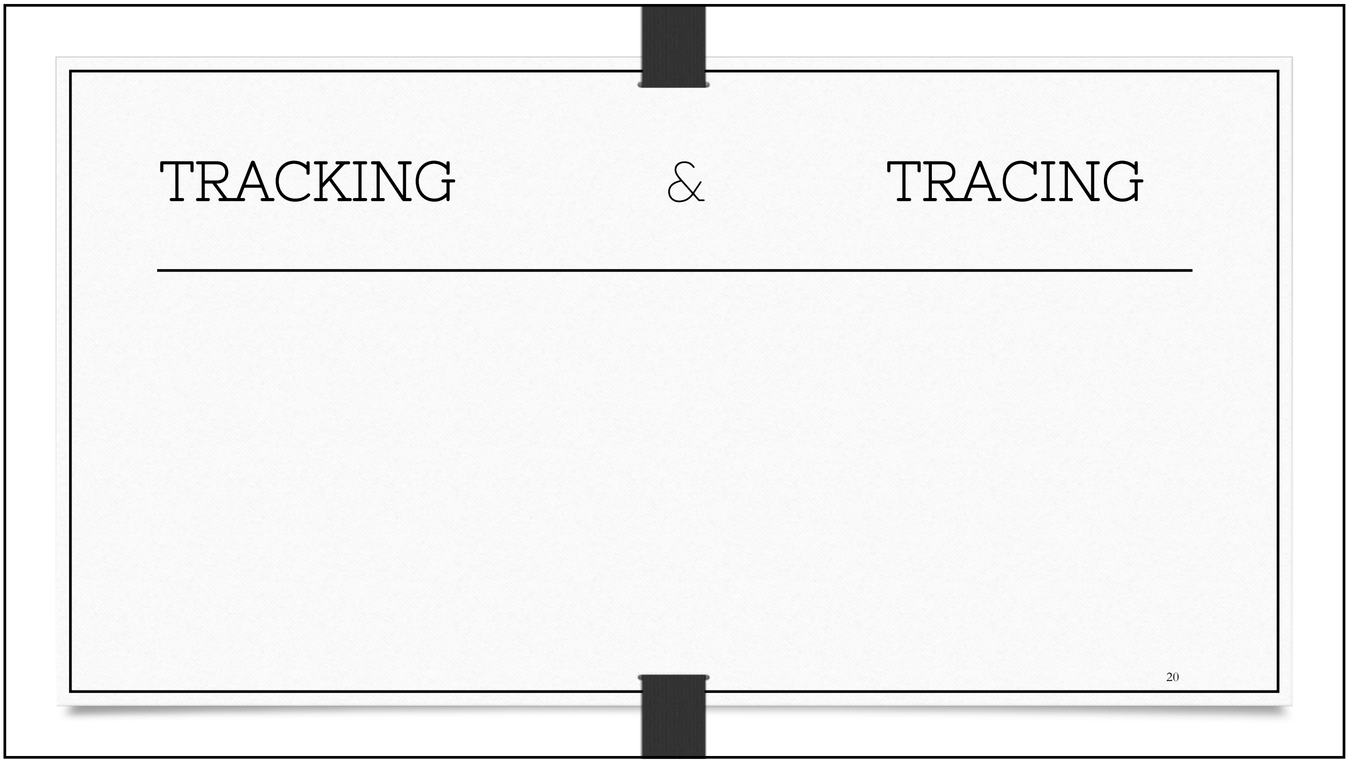
© Denver District Attorney's Office



CLOUD DATA

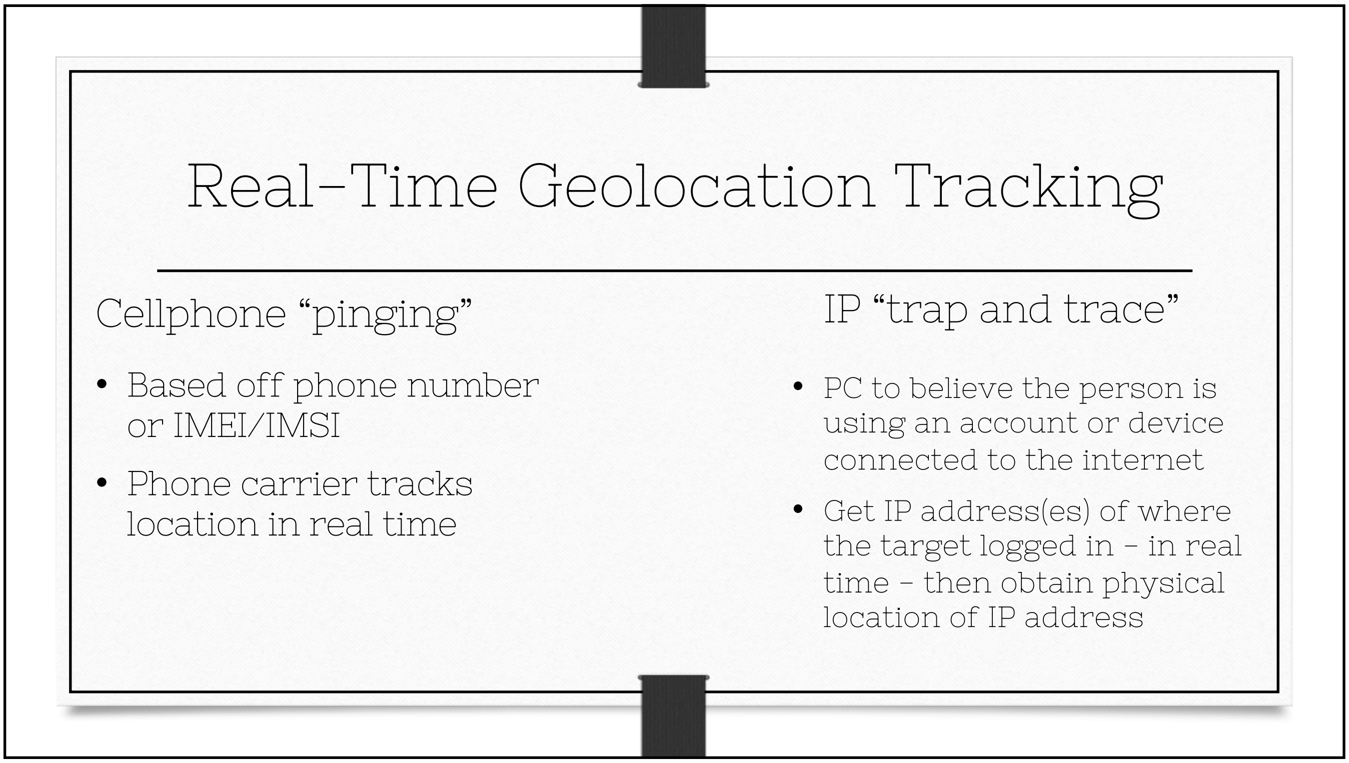
- iCloud, Dropbox, Google Drive, Mega, Microsoft One Drive, NextCloud
- Can give additional info beyond the device and can corroborate data from the device
- Preservation request should be done ASAP, even if you have device

19



TRACKING & TRACING

20



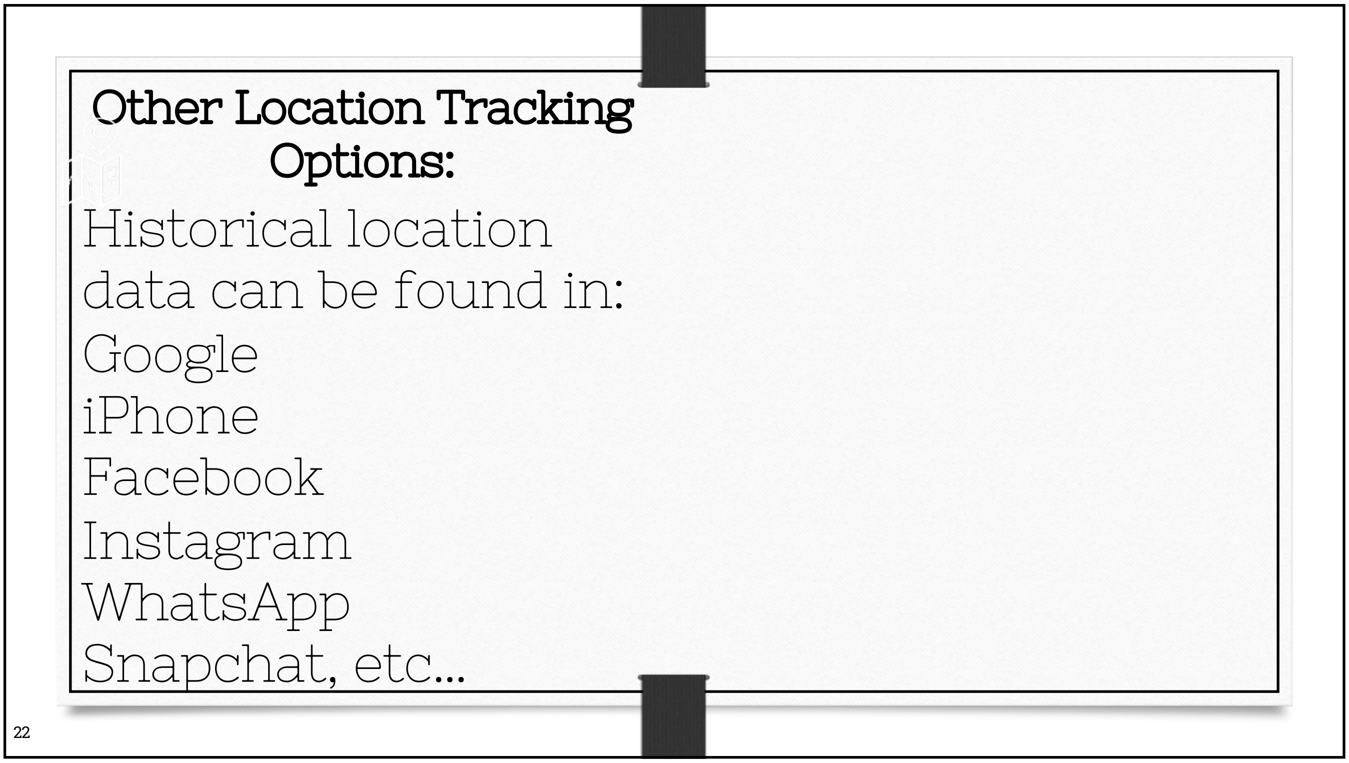
Real-Time Geolocation Tracking

Cellphone "pinging"

- Based off phone number or IMEI/IMSI
- Phone carrier tracks location in real time

IP "trap and trace"

- PC to believe the person is using an account or device connected to the internet
- Get IP address(es) of where the target logged in – in real time – then obtain physical location of IP address



Other Location Tracking Options:

Historical location data can be found in:

Google

iPhone

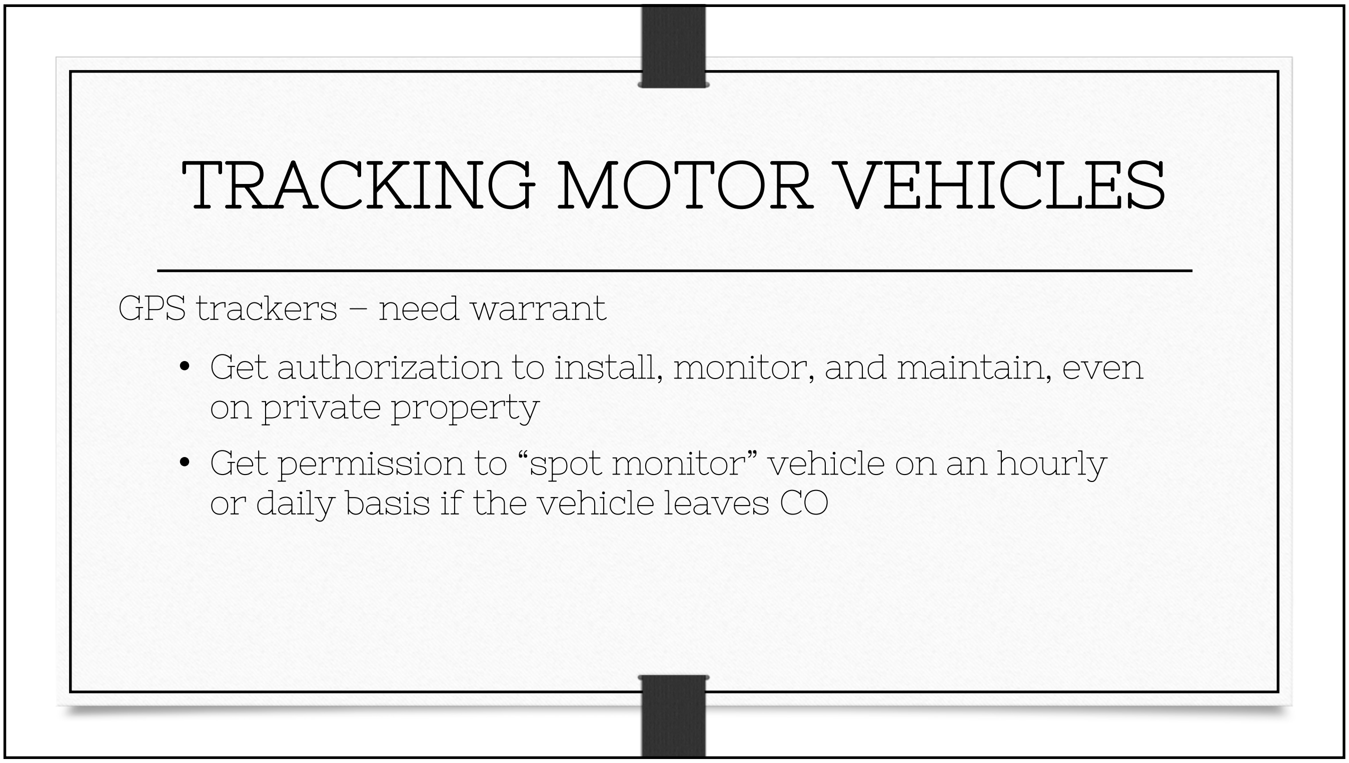
Facebook

Instagram

WhatsApp

Snapchat, etc...

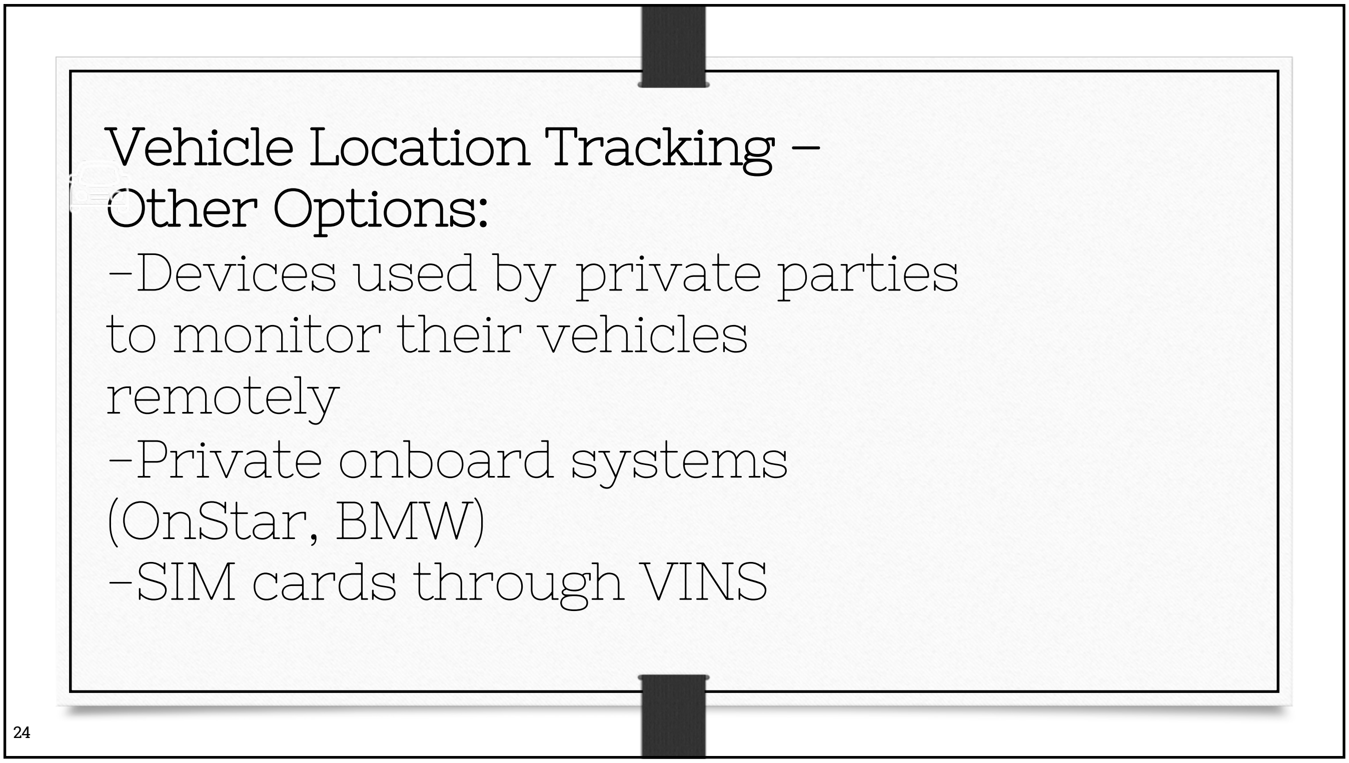
22



TRACKING MOTOR VEHICLES

GPS trackers – need warrant

- Get authorization to install, monitor, and maintain, even on private property
- Get permission to "spot monitor" vehicle on an hourly or daily basis if the vehicle leaves CO



Vehicle Location Tracking – Other Options:

-Devices used by private parties to monitor their vehicles remotely

-Private onboard systems (OnStar, BMW)

-SIM cards through VINS

24