Cell Phone Evidence

February 8, 2020

Saturday Seminar Goals

1. **Comprehensive Overview**
2. **Collaborative**
3. **CalECPA / Social Media: Antonella Nistorescu**
4. **Mapping Expert: Sean Hansen**

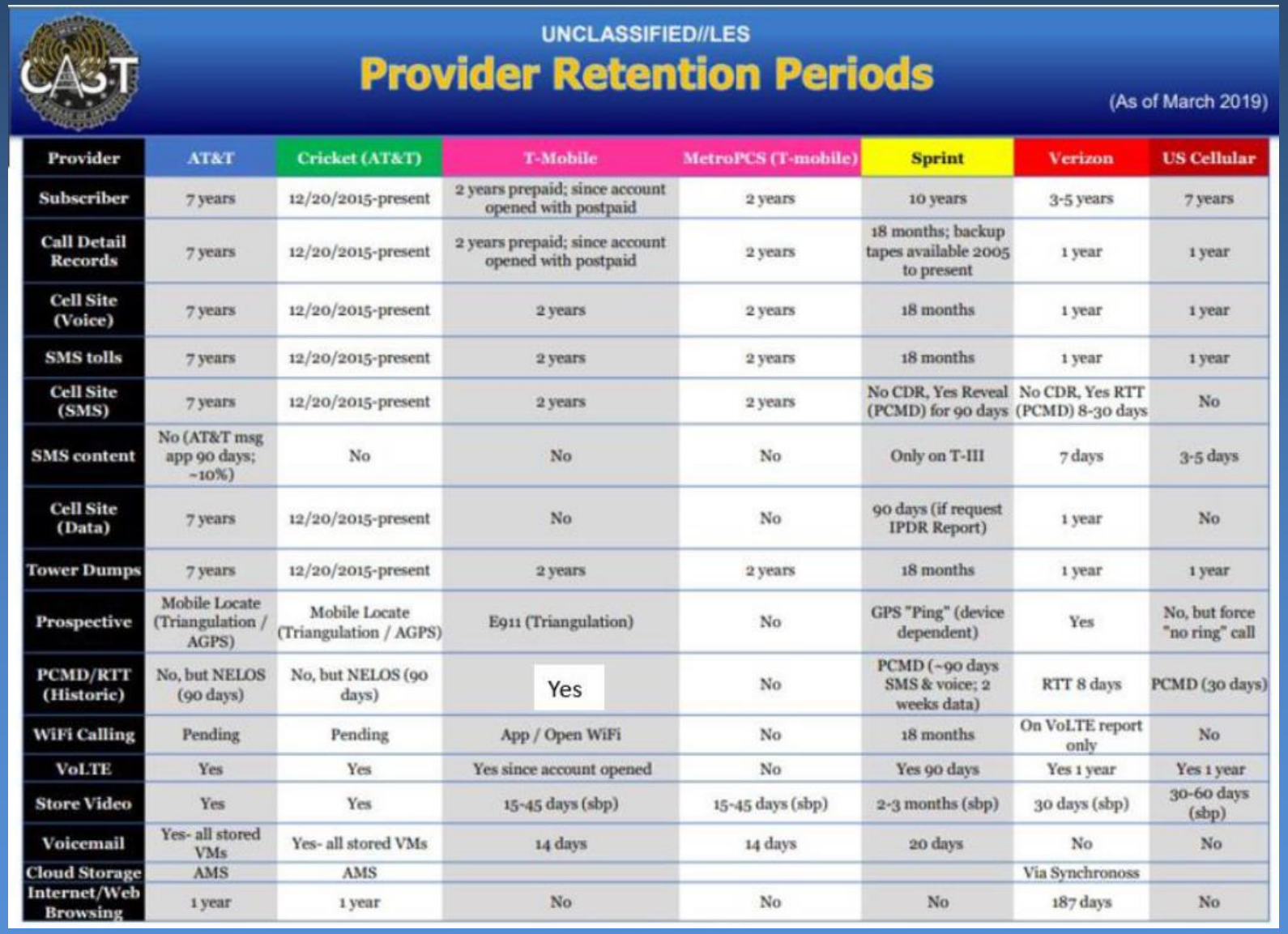
Cell Phone – To Do

1. **Tower Dump**
   - Cell Phone Usage
   - Google Geo-Fencing

2. **CDRs – Call Data Records**
   - NELOS / PCMD / True Call

3. **Cell Phone / Device Dump**

Cell Phone – Preservation Letters



UNCLASSIFIED//LES

Provider Retention Periods

(As of March 2019)

Provider	AT&T	Cricket (AT&T)	T-Mobile	MetroPCS (T-mobile)	Sprint	Verizon	US Cellular
Subscriber	7 years	12/20/2015-present	2 years prepaid; since account opened with postpaid	2 years	10 years	3-5 years	7 years
Call Detail Records	7 years	12/20/2015-present	2 years prepaid; since account opened with postpaid	2 years	18 months; backup tapes available 2005 to present	1 year	1 year
Cell Site (Voice)	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
SMS tolls	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
Cell Site (SMS)	7 years	12/20/2015-present	2 years	2 years	No CDR, Yes Reveal (PCMD) for 90 days	No CDR, Yes RTT (PCMD) 8-30 days	No
SMS content	No (AT&T msg app 90 days; ~10%)	No	No	No	Only on T-III	7 days	3-5 days
Cell Site (Data)	7 years	12/20/2015-present	No	No	90 days (if request IPDR Report)	1 year	No
Tower Dumps	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
Prospective	Mobile Locate (Triangulation / AGPS)	Mobile Locate (Triangulation / AGPS)	E911 (Triangulation)	No	GPS "Ping" (device dependent)	Yes	No, but force "no ring" call
PCMD/RTT (Historic)	No, but NELOS (90 days)	No, but NELOS (90 days)	Yes	No	PCMD (~90 days SMS & voice; 2 weeks data)	RTT 8 days	PCMD (30 days)
WiFi Calling	Pending	Pending	App / Open WiFi	No	18 months	On VoLTE report only	No
VoLTE	Yes	Yes	Yes since account opened	No	Yes 90 days	Yes 1 year	Yes 1 year
Store Video	Yes	Yes	15-45 days (sbp)	15-45 days (sbp)	2-3 months (sbp)	30 days (sbp)	30-60 days (sbp)
Voicemail	Yes- all stored VMs	Yes- all stored VMs	14 days	14 days	20 days	No	No
Cloud Storage	AMS	AMS				Via Synchronoss	
Internet/Web Browsing	1 year	1 year	No	No	No	187 days	No

Cell Phone Downloads

To Do Phone Dumps

** Get ALL phones

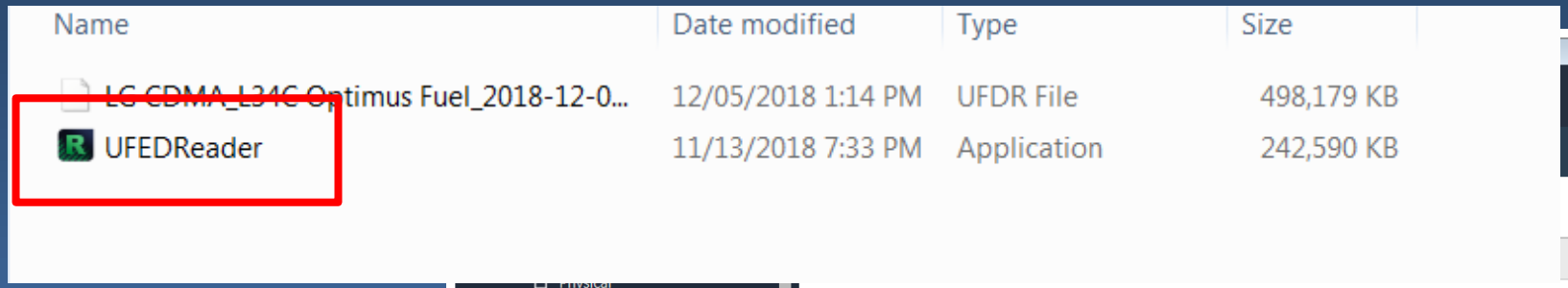
- Password
- Airplane Mode
- Power On
- GRAYKEY
- ***DDA Donn Hoffman*** – Cellebrite Software
- ***Ben Forer / Ethan Milius*** – Compel to Unlock Phone

Cell Phone Downloads

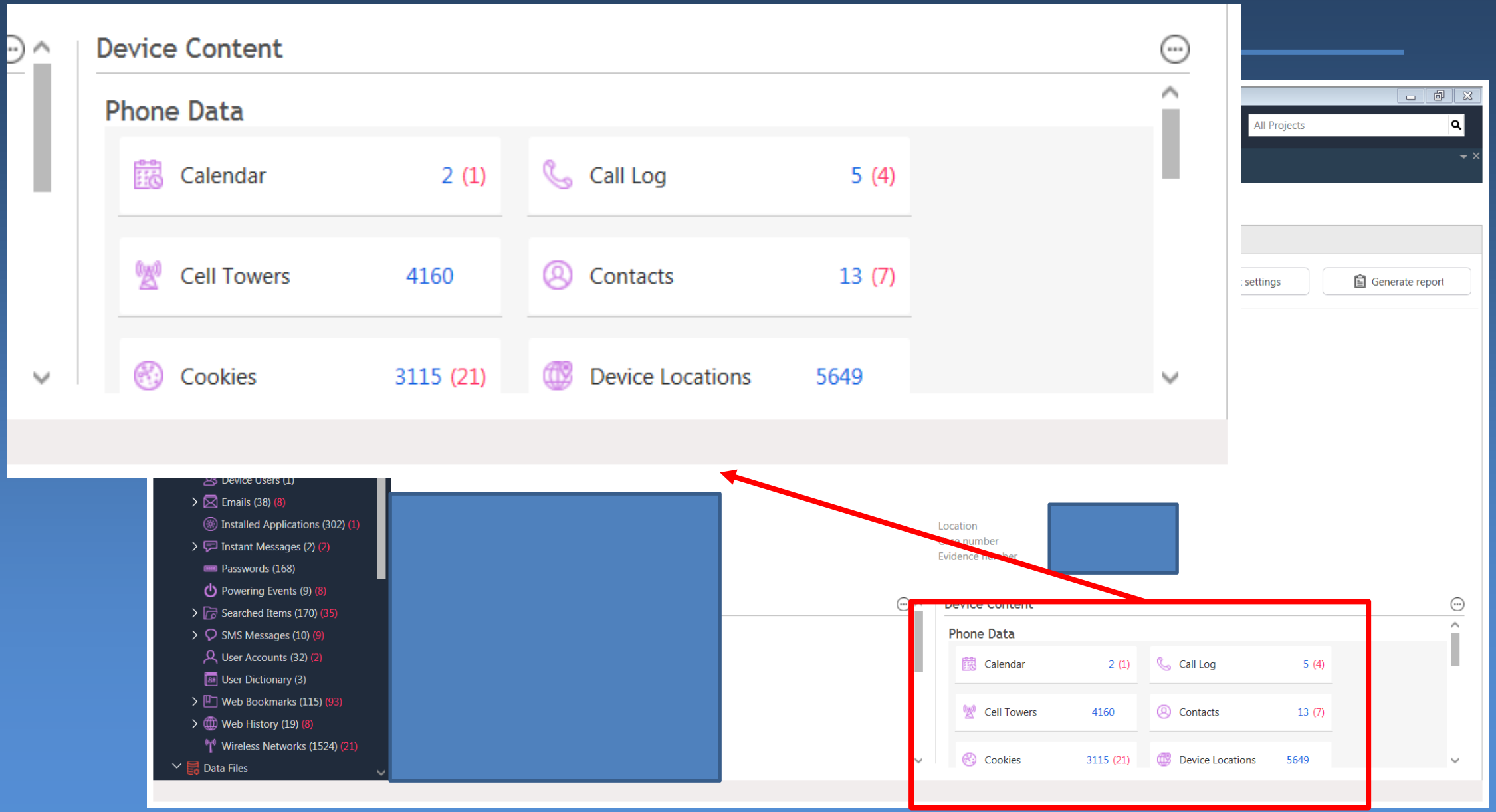
Download Possibilities

1. Recreate the Day
2. Location Data
   - ❖ Wifi Routers / GPS
   - ❖ Waze / Maps
3. Account Usernames / Passwords
4. Movement Records / Heartrate
5. What’s App

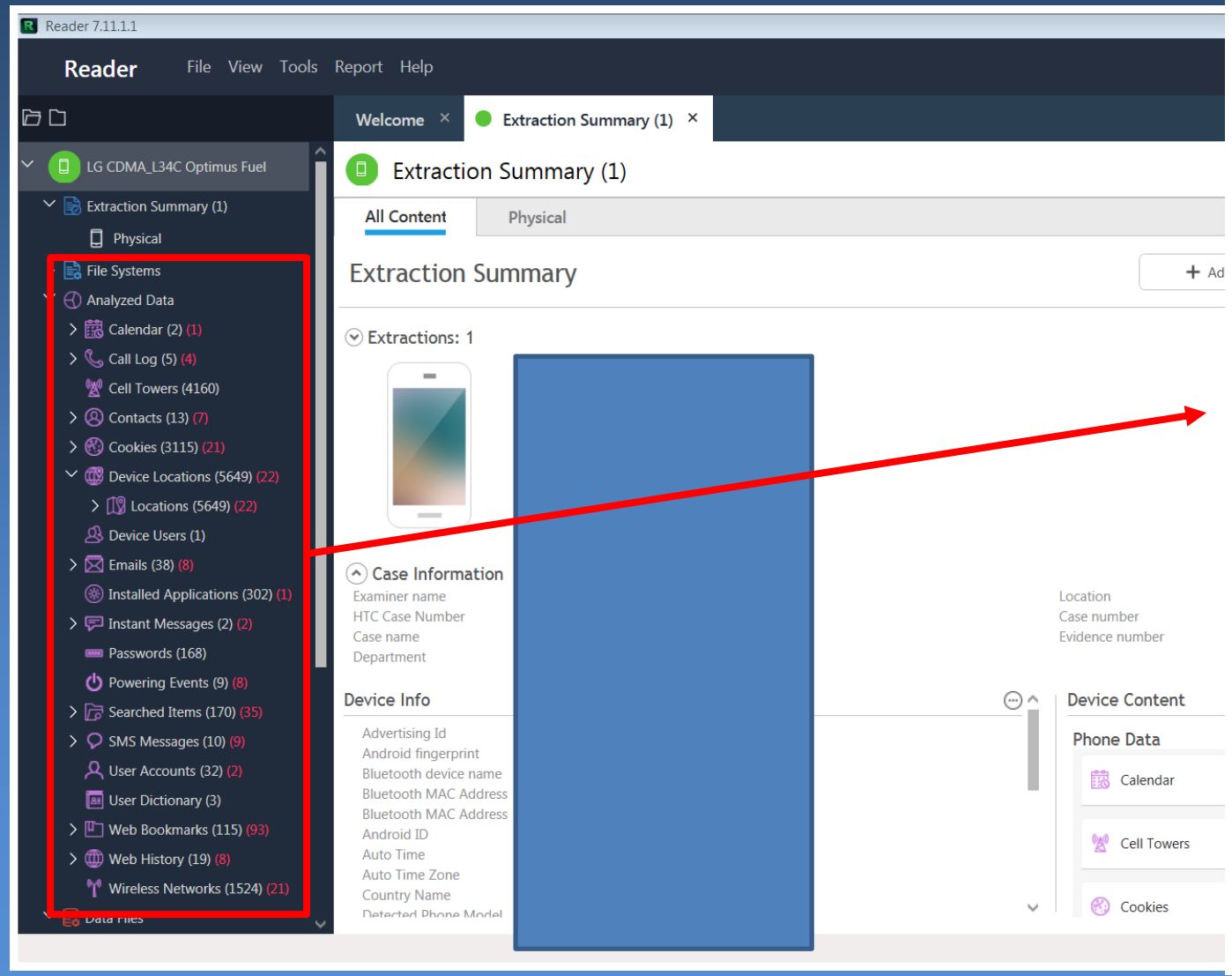
Device Download - Cellbrite

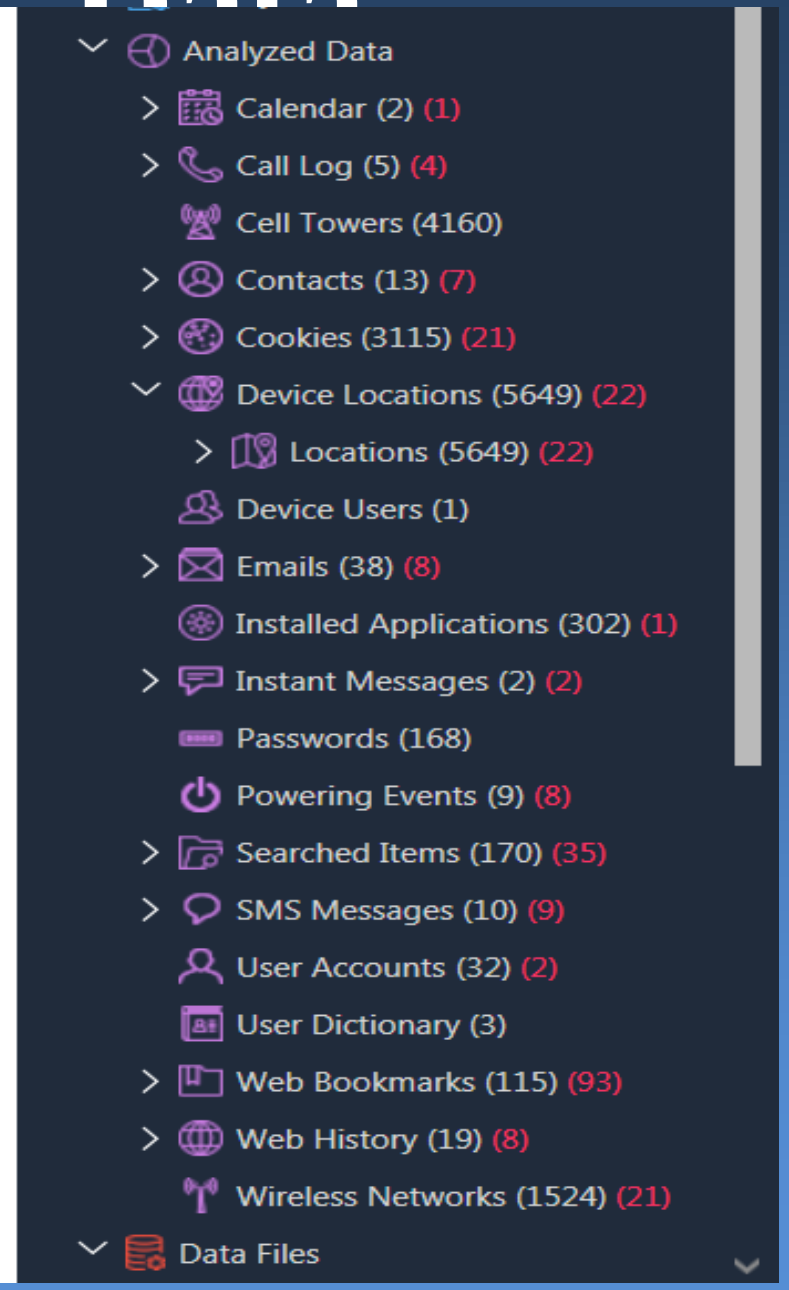


Device Download - Contents



Device Download - Data





CALIF. ELECTRONIC COMMUNICATIONS PRIVACY ACT

(PC §1546 *et seq*)

- ***electronic communication information*** and ***electronic device information***
  - cell phone physical dumps
  - cell tower records, cell call records
  - social media content
  - GPS trackers
  - NOT subscriber information
- No access without warrant
- Limits access to electronic device information

§1546.1(d): The warrant shall describe with particularity the information to be seized by ***specifying the time periods covered and … the target individuals or accounts, the applications or services covered and the types of information sought***.

.

SPECIFIC LINK TO YOUR SUSPECT & CASE:

The above noted account was identified as belonging to and being utilized by [DEF] based on the content found in the public profiles as well as images identifying [DEF].

Your Affiant personally visited the "Facebook" website and located an account your Affiant believes belongs to [DEF]. The username for his "Facebook" account is, "***Many Real***." The user has posted numerous public pictures, **one in which he Is holding a firearm *similar to the one used* in the aforementioned murders and attempted murder. DEF also posted *photographs depicting his gang membership* of the "Winter Gardens" criminal street gang.**

AFFIDAVIT SPECIFICITY:

Your Affiant is seeking a Search Warrant for the aforementioned requested information from Facebook Inc. that ***shall include Expanded Subscriber Content (Neoprint), User Photos (User Photoprint), I.P. (Internet Protocol) logs, private messages, user's inbox, sent mail, received mail, trash/deleted mail, deleted accounts, and all telephone numbers provided by the user and all telephone numbers linked to the users account***.

To include all of the following: Newly created I.P. (Internet Protocol) log, recorded login time, date profile created, date profile was recorded, dates and times of web site login, name, home address, zip code, physical description, date of birth, all e-mail addresses provided by the user, self-photographs of persons, group photographs of persons, private messages, private blogs, wall postings, any messages through the instant messenger application and any other information that is added or posted by the user.

OLD:
Routine Non-Disclosure

Records Request

Please complete all fields below and be sure to attach all relevant documentation. A U.S. search warrant, Mutual Legal Assistance Treaty (MLAT) or letter rogatory is generally required to compel disclosure of user content.

The Law Enforcement Response Team reviews each request separately and discloses account records solely in accordance with our terms of service and applicable law. Additional information can be found in the Facebook or Instagram Law Enforcement Guidelines.

Internal Case Reference Number [?]

Cybertip Number [?]

Legal Process [?] Select One

Nature of Case [?] Select One

Legal Process Signed Date [?] mm/dd/yyyy

Request Due Date [?] mm/dd/yyyy

Accounts Facebook Add

Requesting Records Between [?] Select

Documentation [?] Please attach all relevant legal documents
Must be PDF, JPG, PNG or other common image formats
Attach File

Non-Disclosure Order Yes No

A "non-disclosure order" is an order, signed by a judge that specifically prohibits Facebook from notifying the account holder at issue of the fact that Facebook has been served with legal process seeking information about their account.

I am a law enforcement agent authorized to request account records and all the information I have provided is accurate.

Submit

NEW: Mandatory Disclosure

PC §1524.3(d)(1)

- Mandatory notification to target of the warrant **contemporaneous with service** of the warrant
- **90-day delay with showing of *adverse result***:
  - Danger to life or safety,
  - Flight from prosecution,
  - Destruction of or tampering with evidence,
  - Intimidation of potential wits,
  - Serious jeopardy to investigation

REQUEST FOR NONDISCLOSURE

It is further requested that pursuant to the preclusion of notice provisions of Penal Code § 1546.2 and 18 U.S.C. § 2703(b), **[FACEBOOK] be ordered not to notify any person (including the subscriber, customer or owner of the electronic communication or device information to which the materials relate) of the existence of this warrant for ninety days**.

Your affiant is aware that Penal Code § 1546.2 mandates that the law enforcement agency serving this warrant notify the target of the warrant contemporaneously with the service of the warrant unless an order delaying notification is granted.

Furthermore, I request **authorization for further delay(s) of notification** (with each delay not to exceed **90 days**) upon a showing that such notification(s) would lead to an adverse result.

Such an order is **justified because providing prior notice to the target / party in this matter would lead to an *adverse result* which may result in the destruction of or tampering with evidence; or otherwise seriously jeopardize an investigation or unduly delay of trial.**

§ 1524.3(c): any information obtained through the execution of this warrant that is unrelated to the objective of the warrant shall be *sealed* and shall not be subject further review, use, or disclosure ***absent an order from the Court***.

- Reviewed by investigator and prosecutor, no requirement for third party evaluation

Klugman v. Superior Court

*decided Aug 2019, ordered published

- Motion to quash warrant & suppress evidence under both 4th Am & CALECPA for lack of limiting time periods, specific accounts, precise descriptions of type of information sought …. Lack of safeguards such as sealing to preserve privacy of information unrelated to purpose of the warrant.

SUPPRESSION

- Old CALECPA exclusionary language: violations of CALECPA per se inadmissible
- New CALECPA language: defendant can move to suppress based on violation of 4th Am or CALECPA provisions

FOUNDATION

- EC §1271 (writings): custodian or **qualified witness (gang officer)**

- EC § 1560, 1561: **certification (ask for it in warrant)**

- Foundation: sufficient evidence for a jury to find that the writing/photo is genuine … a prima facie case
  - *P v. Gold*smith (2014) 59 Cal.4th 258, 292.
- THE FACT THAT CONFLICTING INFERENCES CAN BE DRAWN REGARDING AUTHENTICITY GOES TO WEIGHT, NOT ADMISSIBILITY
  - *P v. Goldsmith* (2014) 59 Cal.4th 258, 267;
  - *Jazayeri v. Mao* (2009) 174 Cal.App.4th 301.
- Authentication of evidence, including writing or photos, may be supplied by the person who created it, the person witnessing its creation OR by circumstantial evidence, content or any means provided by law
  - EC 1400; *P v. Goldsmith* (2014) 59 Cal.4th 258, 268.

Evidence Code §1400 *et seq*

- § 1421: authenticity established by **contents** (only author would know matters referred to)
- § 1420: by **evidence of reply** or ongoing communication
- § 1411: **no restriction** on means by which a writing may be authenticated

EVIDENCE OF AUTHENTICITY

- Used own name when signed up (same DOB, email, residence)
- Tagged in multiple photos by profile name
- Cell phone used to access account
- Interest (ex: suspect posting gang video in which he's featured)
- Known family posting to account
- Intimate, continuous dialogue
- Greetings to user by name

People v. Valdez

201 Cal.App.4th 1429 (2011)

- Admission of the social media page(s) themselves, as well as particular content/photos on those pages
- Picture of Defendant throwing gang signs
- Content of pic itself unequivocal
- Corroboration from additional content on his MySpace page expressing interest in that gang: "*consistent, mutually-reinforcing content*"

Valdez / *Beckley*

- ***Beckley*** found authentication of website photo insufficient due to lack of independent verification where lone photo at issue was on defendant's girlfriend's MySpace page showing her making a gang sign
- Distinguished by ***evidence of password requirement for posting & deleting content***, and
- ***Pervasive consistency of content*** of the page (filled w/ personal photos, communications) ***showing owner management*** of the page

Valdez

201 Cal.App.4th 1429

- PROSECUTION'S THRESHOLD AUTHENTICATION BURDEN FOR ADMISSIBILITY IS NOT TO ESTABLISH VALIDITY OR NEGATE FALSITY IN A CATEGORICAL FASHION, BUT RATHER TO MAKE SHOWING ON WHICH JURY COULD CONCLUDE THAT PROFERRED CONTENT IS AUTHENTIC … **AUTHENTICATION DOES NOT MEAN PROVING GENUINENESS**

In Re K.B.

238 Cal.App.4th 989 (2015)

- [distinguishing Beckley] equating authentication with proving genuineness would ignore a fundamental principal underlying authentication emphasized in Goldsmith: the court need only conclude that a prima facie showing has been made that the content is accurate … the ultimate determination of authenticity is for the jury…

Cell Phone – To Do

1. **iCloud Warrant**

2. **Google Warrant**
   - Content
   - Location Data

3. **Drive Tests**
   - Towers
   - WiFi Routers

Presentation in Court

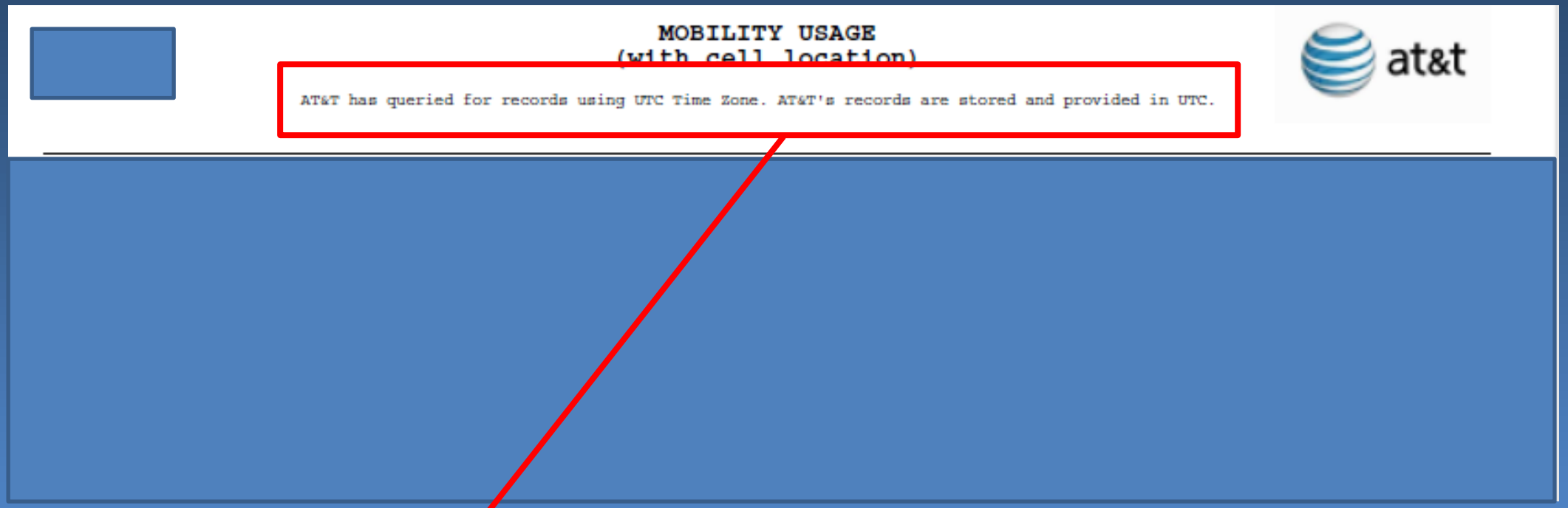
1. **<u>WHAT</u>: Phone Records / CDRs**
   - ❖ All records or modified?
   - ❖ Are the calls otherwise important

2. **<u>HOW</u>: Custodian of Records / Provider Representative**
   - ❖ Stipulation?

<u>BEST PRACTICE</u>:

1. ***Mark and Submit All Records – Just In Case***
2. ***Make 'User Friendly' Exhibit***
3. ***Provide to Defense in Advance***
   - ❖ ***Evidentiary Hearing***

Presentation in Court – Records



UTC = Convert to PST

Resources

Cyndi Barnes	213-257-2330 / 213-422-9458
	cbarnes@da.lacounty.gov
Antonella Nistorescu	213-257-2223 (CalECPA / Social Media)
	anistorescu@da.lacounty.gov
Sean Hansen	310-420-7127 (cell)
	Sean.Hansen@ic.fbi.gov
CAST Intake Form	https://forms.fbi.gov/cast-intake-form

Resources

Donn Hoffman	213-257-2429 (Cell Phone / Email)
LASD Analysts	rihaas@lasd.org or dnhefte@lasd.org
IMEI Number Resource	www.imei.info
Time Zone Fix	timeanddate.com

**** Please reach out to cbarnes@da.lacounty.gov with any questions or suggestions. My goal is to keep this training updated as we evolve into new technology and new challenges, so any input is very much appreciated. Thanks!**

Cell Phone Evidence

February 8, 2020