State Surveillance

Under observation, we act less free,
which means effectively we are less free."

— Edward Snowden

IANAL

Possibility
vs.
Probability

Bottom Line

Most security failures are rooted in poor opsec rather than in technical vulnerabilities

US LE Techniques

1

Informants

2

Target	Type	Direction	Associate	Start Date	Start Time	Stop Date	Stop Time	Time Zone	Duration	SMS TeleserviceID
4155556666	V	Outgoing-answered	15103303300	5/30/2018	21:57:23	5/30/2018	22:02:27	GMT -7	00:05:04	
4155556666	T	Incoming	5109994345	5/30/2018	21:58:40	5/30/2018	21:58:41	GMT -7	00:00:00	4100 (MMS)
4155556666	T	Incoming	5109994345	5/30/2018	21:58:40	5/30/2018	21:58:41	GMT -7	00:00:00	4100 (MMS)
4155556666	T	Incoming	4158882222	5/30/2018	21:58:42	5/30/2018	21:58:43	GMT -7	00:00:00	4100 (MMS)
4155556666	V	Outgoing-answered	5102024040	5/30/2018	22:02:17	5/30/2018	22:02:27	GMT -7	00:00:10	
4155556666	V	Outgoing	14152118888	5/30/2018	22:02:32	5/30/2018	22:02:33	GMT -7	00:00:01	
4155556666	V	Incoming-answered	4156668001	5/30/2018	22:02:35	5/30/2018	22:04:03	GMT -7	00:01:20	
4155556666	T	Incoming	9254447777	5/30/2018	22:03:04	5/30/2018	22:03:04	GMT -7	00:00:00	4098 (SMS)

Call Detail Records

3

Social Media Warrant

4

Pole Cams

5

Vehicle Tracking Device

6

CALEA

10

Legal Hacking

7

ISP Packet Capture

8

Inside Surveillance

9

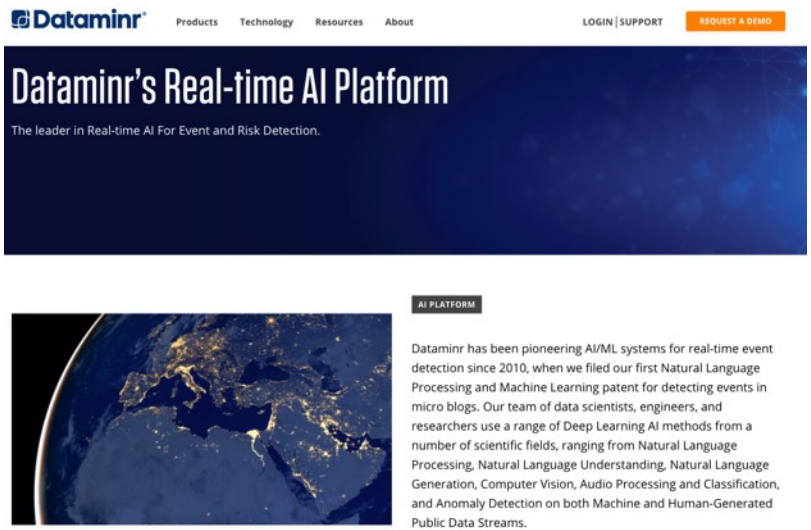
Mobile Surveillance

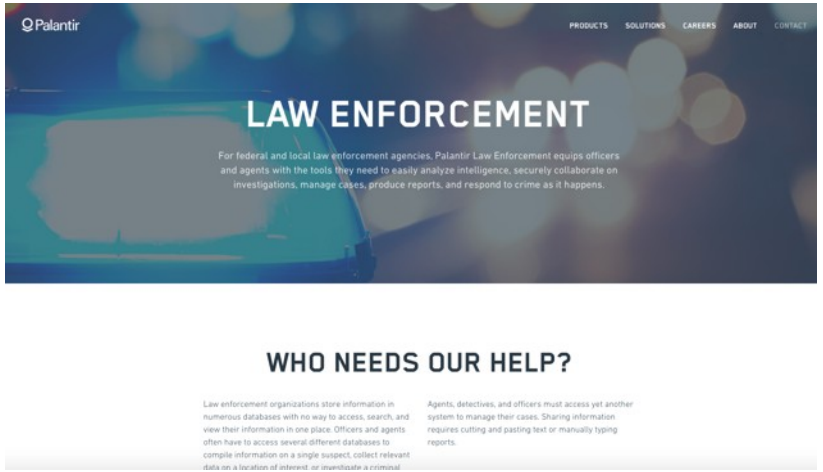
US LE Surveillance

Lessons Learned

1. Long-term LE surveillance involving groups of individuals often involves an informant
2. LE prefers video over audio for technical surveillance
3. The legal bar to conduct surveillance outside a physical location is lower than the bar to conduct surveillance inside a location (IANAL)
4. LE will always prefer the simplest and most straightforward surveillance that will gather the evidence they need

Dataminr


Dataminr
Products
Technology
Resources
About
LOGIN | SUPPORT
REQUEST A DEMO
Dataminr's Real-time AI Platform
The leader in Real-time AI For Event and Risk Detection.
AI PLATFORM
Dataminr has been pioneering AI/ML systems for real-time event detection since 2010, when we filed our first Natural Language Processing and Machine Learning patent for detecting events in micro blogs. Our team of data scientists, engineers, and researchers use a range of Deep Learning AI methods from a number of scientific fields, ranging from Natural Language Processing, Natural Language Understanding, Natural Language Generation, Computer Vision, Audio Processing and Classification, and Anomaly Detection on both Machine and Human-Generated Public Data Streams.


Palantir
PRODUCTS
SOLUTIONS
CAREERS
ABOUT
CONTACT
LAW ENFORCEMENT
For federal and local law enforcement agencies, Palantir Law Enforcement equips officers and agents with the tools they need to easily analyze intelligence, securely collaborate on investigations, manage cases, produce reports, and respond to crime as it happens.
WHO NEEDS OUR HELP?
Law enforcement organizations store information in numerous databases with no way to access, search, and view their information in one place. Officers and agents often have to access several different databases to compile information on a single suspect, collect relevant
Agents, detectives, and officers must access yet another system to manage their cases. Sharing information requires cutting and pasting text or manually typing reports.

Penlink PLX

WHO WE ARE

SERVING LAW ENFORCEMENT FOR MORE THAN 30 YEARS

It's more than big data and analytics.
It's about getting you the tools you need to fully enable your investigations.

FBI Philadelphia Arrest

FPS & Upcoming Protests

Portland Livestream Arrest

Connecting The Dots

Observation

Ex-FBI Director James Comey mentions his Twitter / IG accounts in public appearance

Twitter

Locates account for a “Brien Comey” and confirms via congratulatory tweet

Instagram

Requests to follow on IG recommends Comey family – and reinholdniebuhr

Google

Comey wrote thesis on Reinhold Niebuhr

Twitter

Seven Twitter accounts

ProjectExile7

Social Media Strategies

1. **Don't use social media and delete unused accounts**
2. Protect your accounts
3. Rethink whether you need **every** one of those accounts…
4. Compartmentalize your social media use (personal vs. political)

Be aware of the impact of your social media use on other people

Protect Your Accounts

Your password is a weak link

- Use a unique password for each account
  - *Credential stuffing* is rampant
  - https://haveibeenpwned.com
- Enable *Multi-Factor Authentication* such as app codes or hardware key
- Treat security questions as passwords
- Use a password manager

Remember not all attackers are LE with subpoena power

Protect Your Accounts II

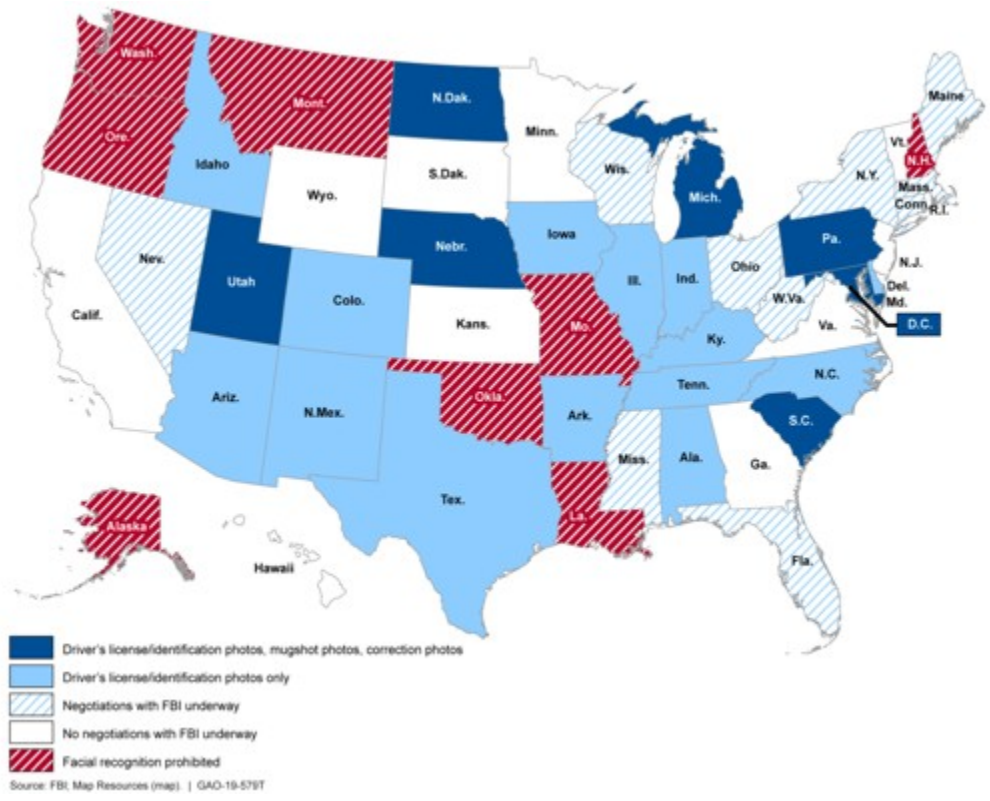
Protect yourself and your connections!

- Use privacy settings to restrict who can see what
- Be mindful of what you share and raise awareness with others
- Scrub metadata from images and documents you share

Protect Your Accounts III

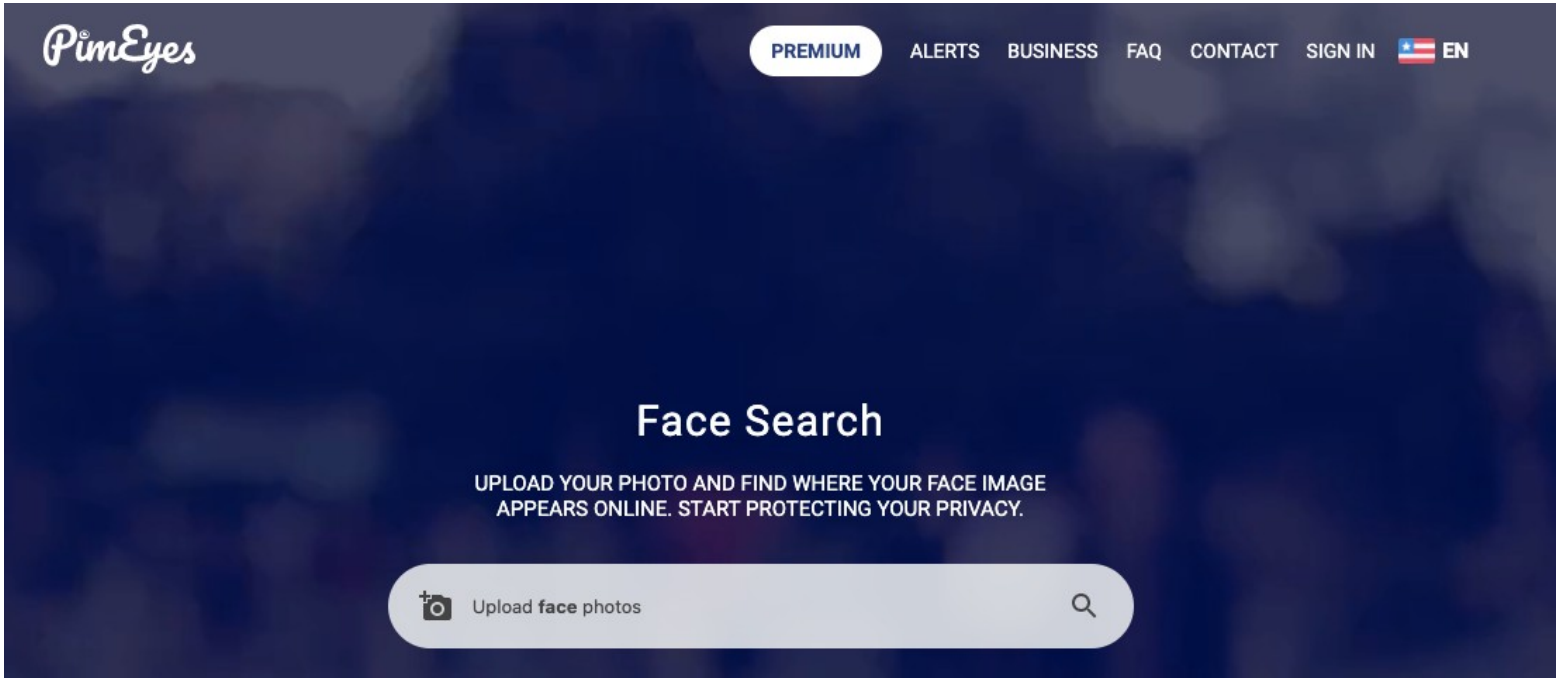
Everything is recorded

- Be cognizant that every access to your social media accounts is logged, including the time and IP address you accessed the platform from
- Your actions within applications can be closely monitored (completely recorded even)



FBI has 640M photographs for in its facial recognition database (FACES)

Facial Recognition

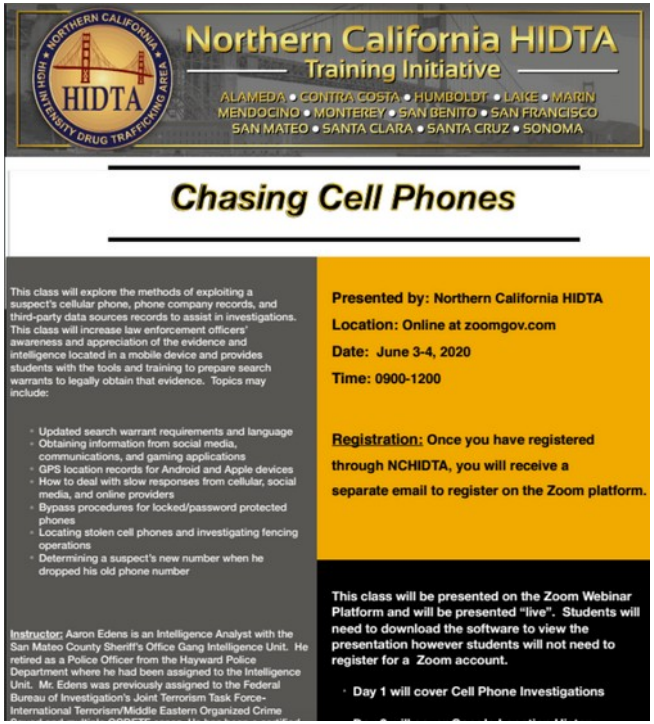


Cellular Surveillance

The greatest material risk to the profession, despite all its advantages, is undoubtedly the telephone. Even if you do not use it carelessly yourself, the other person very often will."

— Allen Dulles, Posthumous Notes

Recent NorCal Example



Northern California HIDTA
Training Initiative

ALAMEDA • CONTRA COSTA • HUMBOLDT • LAKE • MARIN
MENDOCINO • MONTEREY • SAN BENITO • SAN FRANCISCO
SAN MATEO • SANTA CLARA • SANTA CRUZ • SONOMA

Chasing Cell Phones

This class will explore the methods of exploiting a suspect's cellular phone, phone company records, and third-party data sources records to assist in investigations. This class will increase law enforcement officers' awareness and appreciation of the evidence and intelligence located in a mobile device and provides students with the tools and training to prepare search warrants to legally obtain that evidence. Topics may include:

- Updated search warrant requirements and language
- Obtaining information from social media, communications, and gaming applications
- GPS location records for Android and Apple devices
- How to deal with slow responses from cellular, social media, and online providers
- Bypass procedures for locked/password protected phones
- Locating stolen cell phones and investigating fencing operations
- Determining a suspect's new number when he dropped his old phone number

Instructor: Aaron Edens is an Intelligence Analyst with the San Mateo County Sheriff's Office Gang Intelligence Unit. He retired as a Police Officer from the Hayward Police Department where he had been assigned to the Intelligence Unit. Mr. Edens was previously assigned to the Federal Bureau of Investigation's Joint Terrorism Task Force-International Terrorism/Middle Eastern Organized Crime

Presented by: Northern California HIDTA

Location: Online at zoomgov.com

Date: June 3-4, 2020

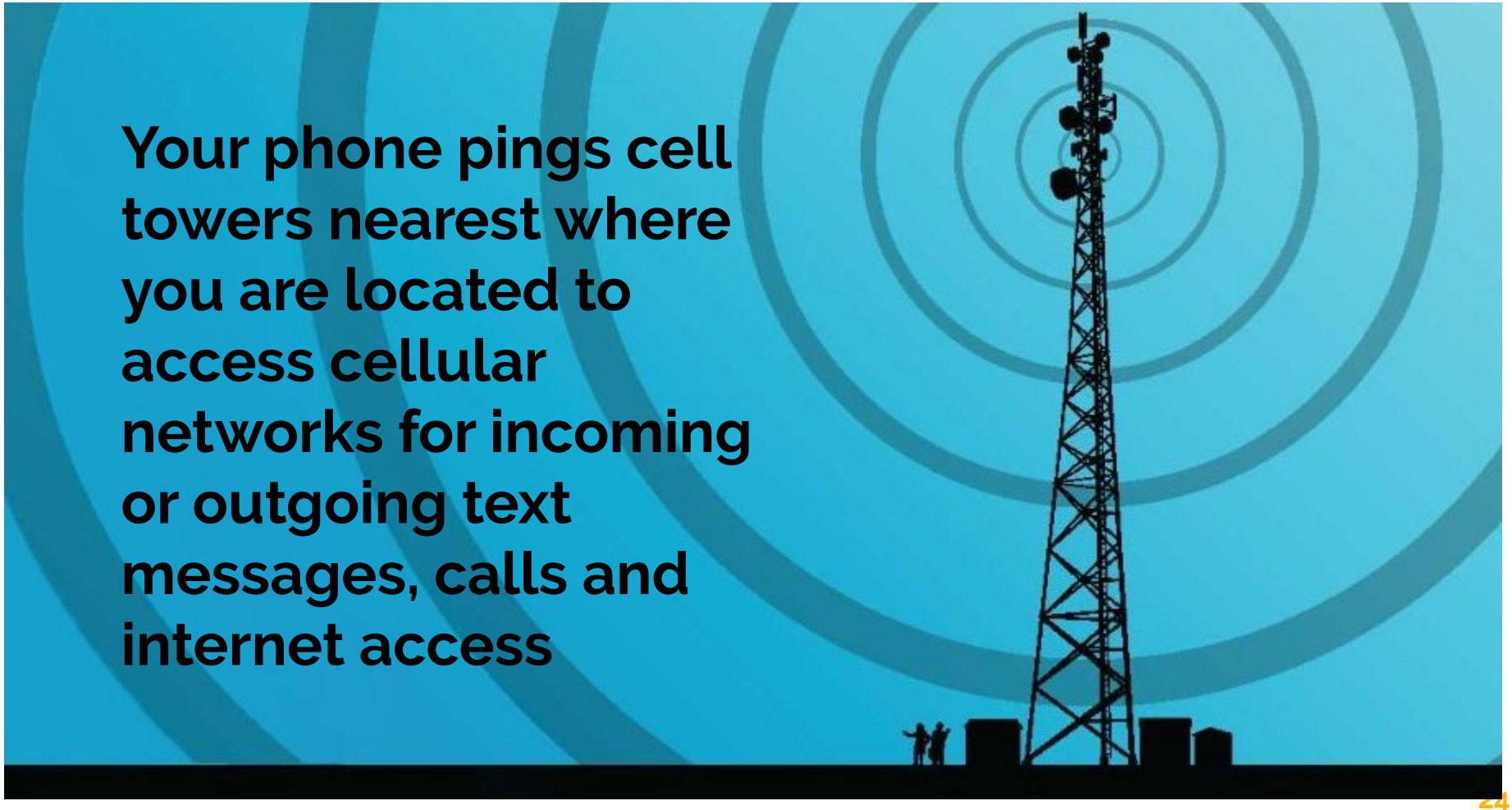
Time: 0900-1200

Registration: Once you have registered through NCHIDTA, you will receive a separate email to register on the Zoom platform.

This class will be presented on the Zoom Webinar Platform and will be presented "live". Students will need to download the software to view the presentation however students will not need to register for a Zoom account.

- **Day 1 will cover Cell Phone Investigations**

Your phone pings cell towers nearest where you are located to access cellular networks for incoming or outgoing text messages, calls and internet access



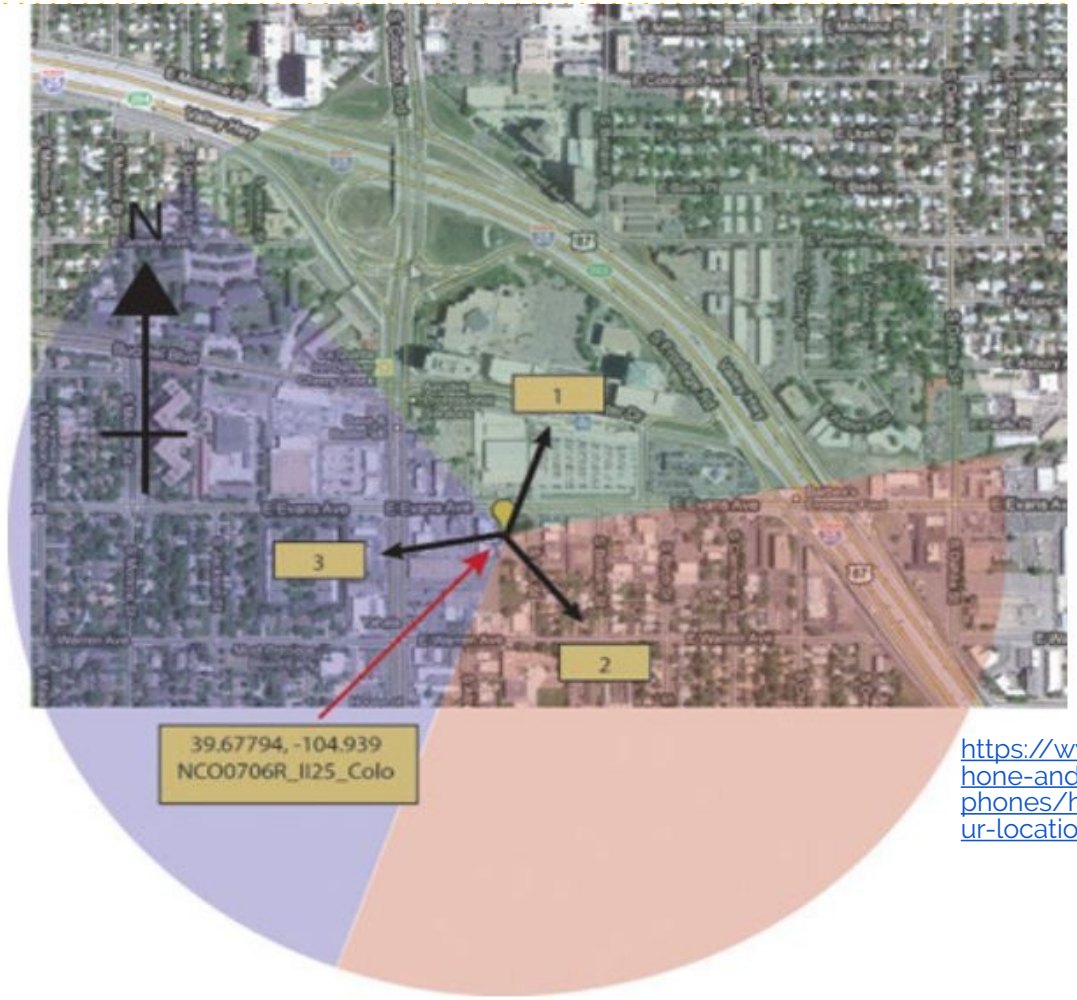
Sample Call Detail Record excerpt after a target's phone data was subpoenaed

Target	Type	Direction	Associate	Start Date	Start Time	Stop Date	Stop Time	Time Zone	Duration	SMS TeleserviceID
4155556666	V	Outgoing-answered	15103303300	5/30/2018	21:57:23	5/30/2018	22:02:27	GMT -7	00:05:04	
4155556666	T	Incoming	5109994545	5/30/2018	21:58:40	5/30/2018	21:58:41	GMT -7	00:00:00	4100 (MMS)
4155556666	T	Incoming	5109994545	5/30/2018	21:58:40	5/30/2018	21:58:41	GMT -7	00:00:00	4100 (MMS)
4155556666	T	Incoming	4158882222	5/30/2018	21:58:42	5/30/2018	21:58:43	GMT -7	00:00:00	4100 (MMS)
4155556666	V	Outgoing-answered	5102024040	5/30/2018	22:02:17	5/30/2018	22:02:27	GMT -7	00:00:10	
4155556666	V	Outgoing	14151118888	5/30/2018	22:02:32	5/30/2018	22:02:33	GMT -7	00:00:01	
4155556666	V	Incoming-answered	4156660001	5/30/2018	22:02:35	5/30/2018	22:04:03	GMT -7	00:01:20	
4155556666	T	Incoming	9254447777	5/30/2018	22:03:04	5/30/2018	22:03:04	GMT -7	00:00:00	4098 (SMS)

Part 1

Begin Cell	Begin IAP SysID	End Cell	End IAP SysID	Begin Map	Begin Latitude	Begin Longitude	Sector Direction [degrees]	End Map	End Latitude	End Longitude	Sector Direction [degrees]
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7687	-122.434	3
26-1	4183-3-1	211-3	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:211	37.7783	-122.423	2
26-1	4183-3-1	26-1	4183-3-1	L:4183-3 C:26	37.7632	-122.434	3	L:4183-3 C:26	37.7632	-122.434	3

Part 2



https://www.techradar.com/news/phone-and-communications/mobile-phones/how-your-phone-betrays-your-location-993674

Or Just Ask Google

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is maintained on computer servers controlled by Google, Inc. ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant, which consists of Google location data associated with a particular specified location at a particular time, as specified in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. ' 2703(c)(1)(A) to require Google

- Contains detailed records of the exact location of hundreds of millions of devices (Android and IOS with Google apps) dating back nearly a decade
- Geofence or "reverse location" warrant
- FBI and police in CA, NC, FL, MN, ME, WA are *known* users

Non-Profits Track You

TECH

Political Groups Track Protesters' Cellphone Data

Voting and advocacy groups track cellphones of participants and send messages; the tactics are 'deeply spooky yet extremely helpful,' says one user

In the last decade, the smartphone has become a tool for witnessing police violence toward African Americans. From the 2009 killing of Oscar Grant to the 2020 killing of George Floyd, we reviewed the footage and talked to the people who captured it, to see how the accounts of racial injustice became clearer as the phones evolved. Photo illustration: Preston Jessee for The Wall Street Journal

By Emily Glazer and Patience Haggin
Updated June 14, 2020 8:44 pm ET

Q: Can LE get into my mobile phone if they have it in their possession?

A: It depends on a number of factors, including the hardware, OS version, whether it is powered on/off, whether you have unlocked it if powered on (AFU), password/passcode complexity, and the agency trying to get into your phone

Cellebrite UFED

Smartphone Acquisition

Key Benefits of iOS Data Extraction

Determine passcodes & perform unlocks for all Apple devices

Sophisticated algorithms to minimize unlock attempts

Perform a forensically sound full file-system extraction

Key Benefits of Android Data Extraction

Bypass or determine locks on all flagship Samsung devices

Extract unallocated data to maximize recovery of deleted items

Perform a forensically sound physical or full file-system extraction

Advanced Unlocking

Determine or disable the Pin/Pattern /Password screen locks or passcodes on the latest Apple iOS and Google Android devices.

Advanced Extraction

Cellebrite makes the world's only decrypted physical extraction capability possible. Retrieve the full file system from all Apple and Android devices.

Advisory Services

We provide evidentiary preparation including independent case review or testimony, to help you ensure the best possible case results.

Cellebrite UFED

Cellebrite Advanced Services (As of 04 July 2020)

Q: Why Signal?

A: Because you probably already use it!

Four steps to increase your Signal security

1. Use a burner number (i.e. Google Voice, Hushed, Sudo)
2. Always verify Safety Numbers (fingerprints)
3. Set Disappearing Messages (one week is a good compromise between security and usability)
4. Do **not** use Signal as your default SMS app (Android)

Increase Mobile Security

1. Use a phone and SIM not tied to your real name (i.e. burner phone)
2. Use a de-Googled mobile OS (Graphene / Librem)
3. Eliminate unnecessary / unused apps (e.g. Facebook, Gmail etc.)
4. Restrict https://myaccount.google.com/intro/activitycontrols
5. Turn your phone off when seizure risk exists (BFU)
6. Segment your communication between different phones

Accept that using a cellular phone is fundamentally insecure

Mask up!

Cover your eye area

Leave your phone

Don't film people

Beware social media

Thanks!

Any questions?

You can still find us by talking to us after ;-)