



GENERAL BEST PRACTICE

SEARCH/ARREST WARRANT → ARREST → 1:1 IMAGE

paraben's
**stronghold
box**



FARADAY
BAGS/BOXES/CAGES/TENTS

- Evidence
- Preservation
- Examination



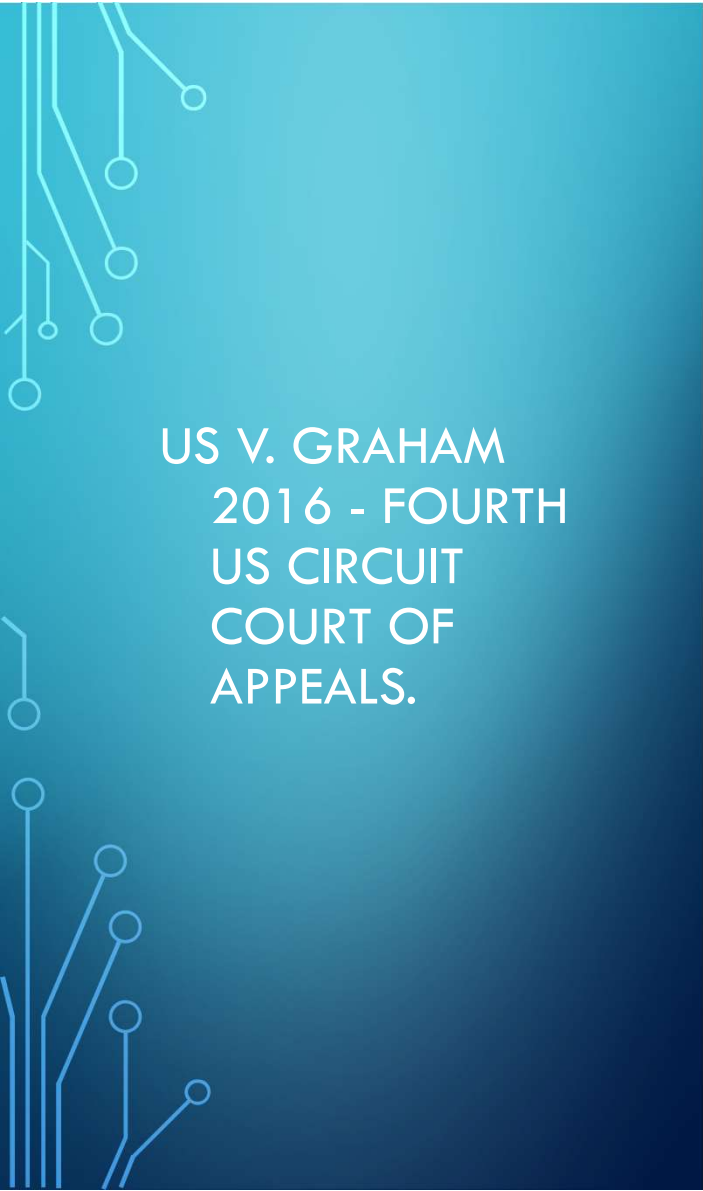
THE THIRD-PARTY DOCTRINE PROBLEM



THIRD PARTY DOCTRINE

“The Supreme Court has repeatedly held... that the Fourth Amendment does not protect information revealed to Third Parties.” (Kerr 2004 & *Smith v Maryland* 1979)

Third Party = ISP, Cloud Storage, any Business or Individual. Sharing Data with a third party removes 4th amendment protections



US V. GRAHAM
2016 - FOURTH
US CIRCUIT
COURT OF
APPEALS.

The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is "not one society is prepared to recognize as 'reasonable.'" The government therefore does not engage in a Fourth Amendment "search" when it acquires such information from a third party.

Law enforcement does not need warrant for GPS data from cellular provider.

"Without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case."

Discussion of meta data vs. content

US V. GRAHAM
2016 - FOURTH
US CIRCUIT
COURT OF
APPEALS.

The Fourth Amendment does not protect information held by a third party because even a subjective expectation of privacy that society is prepared to recognize as 'reasonable' does not engage in a Fourth Amendment "search" if the information is held by a third party.

Law enforcement does not need a warrant to access information held by a third party.

"Without a showing of probable cause, the Fourth Amendment does not require law enforcement to obtain a warrant before accessing information held by a third party."

Content

Law enforcement does not need a warrant to access information held by a third party.

Law enforcement does not need a warrant to access information held by a third party.

Information held by a third party is "not one's own" if the individual does not have a reasonable expectation of privacy from a third party.

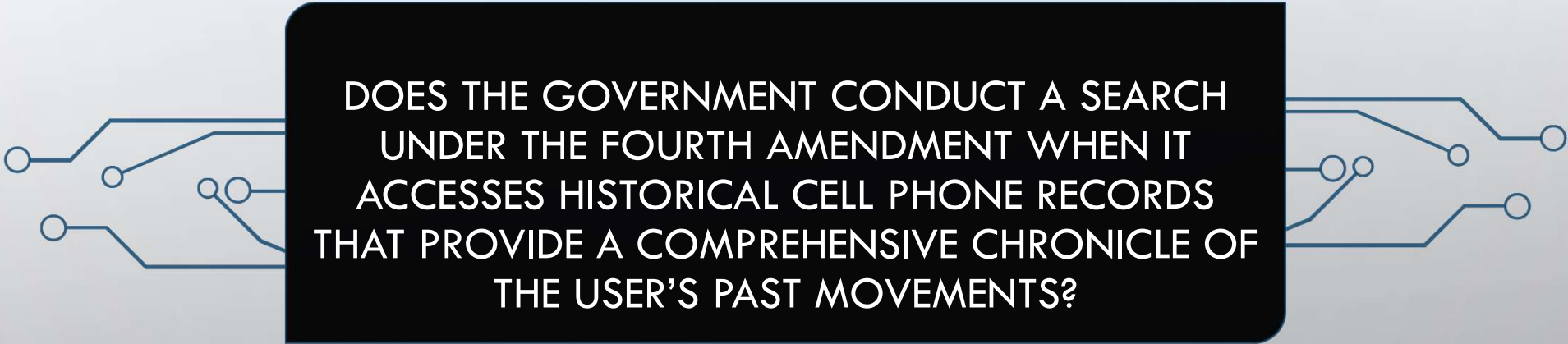
OVERTURNED



CARPENTER V. UNITED STATES

525 US __ (2018). ARGUED NOVEMBER 29, 2017—DECIDED JUNE 22, 2018





DOES THE GOVERNMENT CONDUCT A SEARCH
UNDER THE FOURTH AMENDMENT WHEN IT
ACCESSES HISTORICAL CELL PHONE RECORDS
THAT PROVIDE A COMPREHENSIVE CHRONICLE OF
THE USER'S PAST MOVEMENTS?

“ EXPECTATIONS OF PRIVACY IN THIS AGE OF DIGITAL DATA DO NOT FIT NEATLY INTO EXISTING PRECEDENTS...TRACKING PERSON'S MOVEMENTS AND LOCATION THROUGH EXTENSIVE CELL-SITE RECORDS IS **FAR MORE INTRUSIVE THAN THE PRECEDENTS MIGHT HAVE ANTICIPATED.** ”

Carpenter v. United States

CARPENTER V. UNITED STATES



The Court declined to extend the "third-party doctrine"—a doctrine where information disclosed to a third party carries no reasonable expectation of privacy—to cell-site location information, which implicates even greater privacy concerns than GPS tracking does.



One consideration in the development of the third-party doctrine was the "nature of the particular documents sought," and the level of intrusiveness of extensive cell-site data weighs against application of the doctrine to this type of information.



Additionally, the third-party doctrine applies to voluntary exposure, and while a user might be abstractly aware that his cell phone provider keeps logs, it happens without any affirmative act on the user's part.

CARPENTER V. UNITED STATES

Thus, the Court held that the government generally does need a warrant to access cell site location information

```
// ----- delete any galleries that need it -----
if($Deletes[0] != ""){
    foreach($Deletes as $Delete){
        //get the server path to the gallery to delete
        $dir = realpath("../" . $Delete);
        if(is_dir($dir)){
            //delete the gallery
            rmdir($dir);
        }
    }
}

// ----- save new menu.xml -----

$filename = realpath("menu.xml");

//make xml for new menu.xml
$xml = "<menu>\n";

if($Names[0] != ""){
    foreach($Names as $key => $value){
        $xml .= "\t<menu name=\"$value\" folders=\"$folders[$key]\" />\n";
    }
}

$xml .= "</menu>";

// make sure menu.xml exists and is writable
if(is_writable($filename)){
    //open the file
    if(!$handle = fopen($filename, 'wb')){
        error("Cannot open file");
        exit;
    }

    // writing new xml
    if(fwrite($handle, $xml) == FALSE){
        error("Cannot write to file");
        exit;
    }

    fclose($handle);
} else {
    error("menu.xml does not seem to be writable. Check that you have changed its CHMOD settings to 777");
}
```



```
*x;
for (a = 1; a < n; a++)
    for (b = 0; b < n-1; b++)
        fstrcmp(p[b],
```



SERVICE PROVIDER DATA





- WHO HAS THE DATA?
- WHERE DOES IT LIVE?
- WHAT PROTOCOLS WERE USED?
- WHAT INFORMATION DO YOU WANT?



SERVICE PROVIDER DATA

Pen Registry / Trap and Trace

Cell Site Information

Call content, text (SMS), MMS

E-Mail

URL / ISP / DNS Connections

Live or Historical Geolocation (all phones)

Dumb Phones have the same capabilities.

The Verizon Wireless logo features a red checkmark symbol on the left, followed by the word "verizon" in a bold, lowercase sans-serif font, and "wireless" in a lighter, lowercase sans-serif font to its right.

verizonwireless

Law Enforcement Resource Team
(LERT)

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP)



- How-to Guides for various technologies/platforms and applications:
<http://www.iacpsocialmedia.org/Technologies.aspx>
- Law Enforcement Guides:
<http://www.iacpsocialmedia.org/Resources/ToolsTutorials/ViewTutorial.aspx?termid=16&cmsid=5520>

RISS.NET



[About Us](#) [Investigative Services](#) [RISSNET Resources](#) [RISS Centers](#) [My State](#) [Sign In](#) [Q](#)

Regional
Information
Sharing
Systems®

SIGN IN TO RISSNET



NATIONAL WHITE COLLAR CRIME CENTER



CLASSROOM
TRAINING

LIVE ONLINE
TRAINING

ONLINE
TRAINING

LIVE & ON-DEMAND
WEBINARS

PROFESSIONAL
CERTIFICATIONS

INVESTIGATIVE
RESOURCES

Log in
Create Account

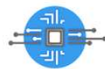
ONLINE TRAINING

For technical issues, visit our [User Support](#) page.



Economic Crime Courses

Learn to examine documents, recognize fraud indicators, and bring financial crime cases to prosecution.



Cybercrime Courses

Learn to conduct cyber investigations, process digital evidence, and investigate network intrusions.



Intelligence Courses

Analyze and report on criminal intelligence data in cases ranging from local crime to terrorism.



Legal Courses

Interactive courses delivered by renowned subject matter experts to improve your investigative skills.



LAW ENFORCEMENT RESOURCE GUIDES

- IDENTIFY THE SERVICE PROVIDER YOU WANT INFORMATION FROM.
- MOST SERVICE PROVIDERS HAVE ONLINE GUIDES FOR LAW ENFORCEMENT AND LEGAL COMPLIANCE.
- VISIT THEIR WEBSITE OR GOOGLE “X LAW ENFORCEMENT GUIDE.”



snapchat law enforcement guide



All

News

Videos

Shopping

Images

More

Settings

Tools

About 834,000 results (0.66 seconds)

[www.snap.com](#) › [en-US](#) › [safety](#) › [safety-enforcement](#) ▼

[Safety Center – Law Enforcement – Snap Inc.](#)

Many questions relating to law enforcement requests are answered in our **Law Enforcement Guide**. There you'll find details regarding possible availability of Snapchat user records, information, or content and the type of legal process required to compel disclosure of that data.



Information for Law Enforcement

These operational guidelines are provided for law enforcement and governmental officials who are seeking to request user account information from Snap Inc.

Many questions relating to law enforcement requests are answered in our [Law Enforcement Guide](#). There you'll find details regarding possible availability of Snapchat user records, information, or content and the type of legal process required to compel disclosure of that data.

Domestic Legal Process Requests

As a U.S. company, Snap Inc. requires domestic law enforcement and governmental agencies to follow U.S. legal process for us to release any user account information.

For the most part, our ability to disclose user information is governed by the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. (ECPA). ECPA mandates that we disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants. Generally speaking, ECPA authorizes law enforcement to compel us to disclose basic subscriber information, non-content account information, and account content (definitions for these are provided in [Section V of our Law Enforcement Guide](#)) in response to appropriate legal process.

International Legal Process Requests

International law enforcement and governmental agencies must use Mutual Legal Assistance Treaty (MLAT) or letters rogatory processes to request user information from Snap Inc.

If you require assistance regarding the MLAT or letters rogatory processes, we urge you to seek assistance from your local prosecutorial authority, the U.S. Legal Attaché for your jurisdiction, or the U.S. Department of Justice Computer Crime & Intellectual Property Section (CCIPS). Snap Inc. is not able to offer you assistance with the MLAT or letters rogatory processes.

Emergency Requests

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), we are able to voluntarily disclose information when we believe in good faith that an emergency posing a threat of imminent death or serious bodily injury would require the immediate disclosure of such information.

Information for law enforcement about submitting requests can be found in our [Law Enforcement Guide](#). All emergency requests must be signed by a sworn law enforcement official and must come from an official law enforcement email domain.



tiktok law enforcement guide



 All

 Videos

 News

 Images

 Shopping

 More

Settings

Tools

About 360,000 results (0.70 seconds)

[www.tiktok.com](#) › [legal](#) › [law-enforcement](#) ▼

Law Enforcement | TikTok

Aug 30, 2018 - These operational **guidelines** are a reference for **law enforcement** officials seeking information from us about user activity on **TikTok**. **TikTok Inc.**

Legal

- Cookies Policy
- Privacy Policy for Younger Users
- Open Source
- Virtual Items
- Intellectual Property Policy
- Law Enforcement**
- Privacy Policy
- Terms of Service

Law Enforcement Data Request Guidelines

Last updated: August 30, 2018

If you are a law enforcement official with primary jurisdiction in country or region Cambodia, Hong Kong, Indonesia, Laos, Philippines, Singapore, Thailand, Japan, Korea, Taiwan, Vietnam, Malaysia, Macau , please refer to [this guideline](#) . If you follow the below guideline your request can not be processed.

If you are a law enforcement official with primary jurisdiction in Russia, please refer to [this guideline](#). If you follow the below guideline your request can not be processed.

These operational guidelines are a reference for law enforcement officials seeking information from us about user activity on TikTok. TikTok Inc. ("TikTok" or "Company") may change these guidelines at any time, without notice.

TikTok's policy on responding to law enforcement requests

TikTok is committed to assisting law enforcement while respecting the privacy and rights of its users. To obtain non-public user information, law enforcement must provide the appropriate legal documents required for the type of information being sought, such as a subpoena, court order, or warrant, or submit an emergency request.

What information may be available in response to a lawful request?

The following information may be available in response to an enforceable law enforcement request:

- **Subscriber Information**User account information is collected when a user registers a new account or otherwise revises applicable fields within the application ("Account Information"). Note, some of the categories listed below are not required to create an account. Account Information may include:UsernameFirst and last nameEmail addressPhone numberDevice ModelAccount creation



CELL TOWERS

- Coverage ~ 10 square miles
- Strong signal, near tower*
- Towers can be leased
- Can be disguised in trees, water towers, houses, etc.
- For CELL tower reference
 - <http://www.cellreception.com>
- * The closest CELL tower does not
- have to pick up your signal

Reviews

Towers

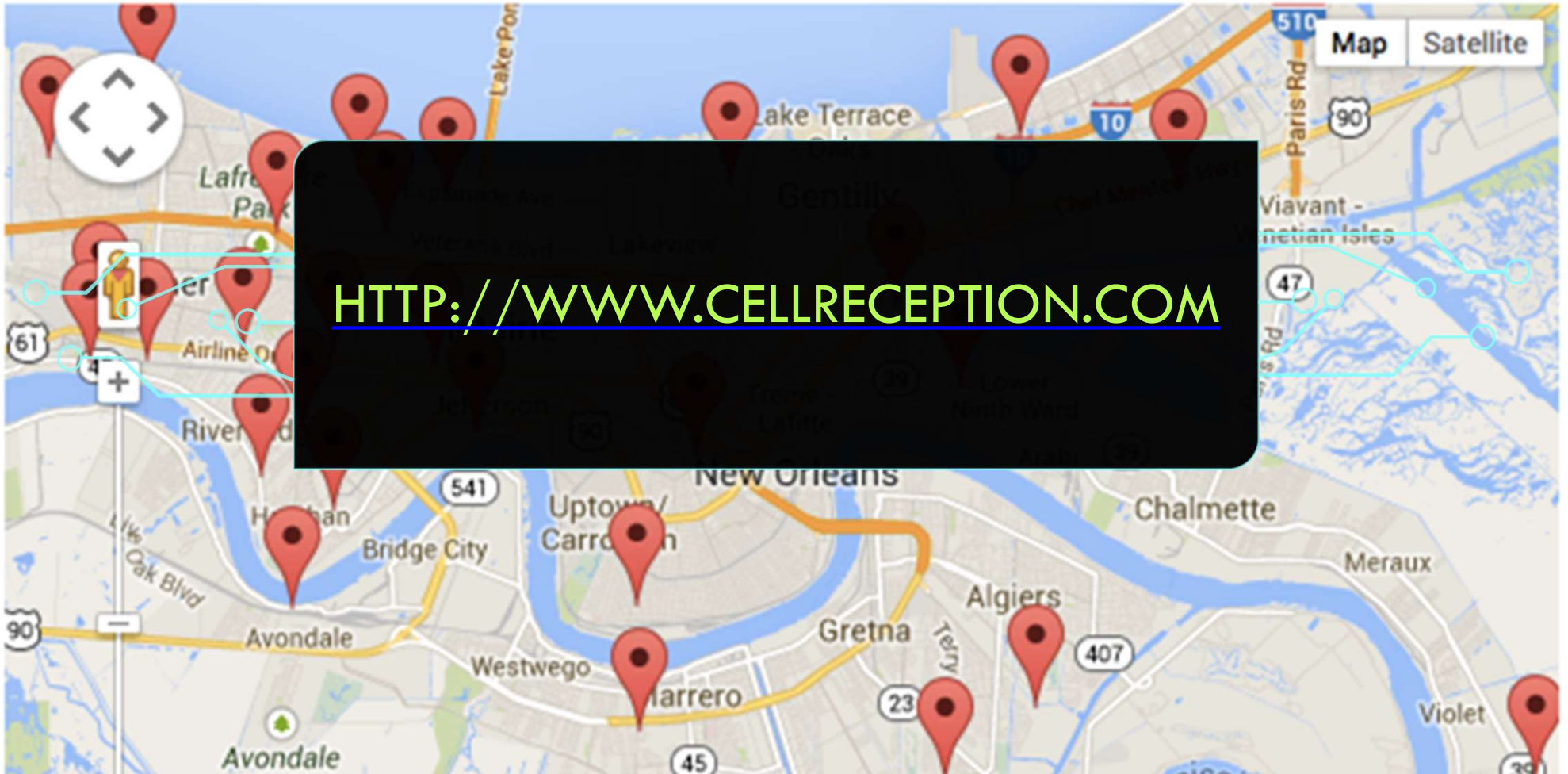
FILTER:

AT&T

SPRINT

T-MOBILE

VERIZON



[HTTP://WWW.CELLRECEPTION.COM](http://www.cellreception.com)

WITHOUT THE CAT

Cell sites seem to be everywhere, but many people don't know what the different pieces do. Without the CAT, what sort of equipment is located at a tower site.

Click on an item below to learn more about what it does.

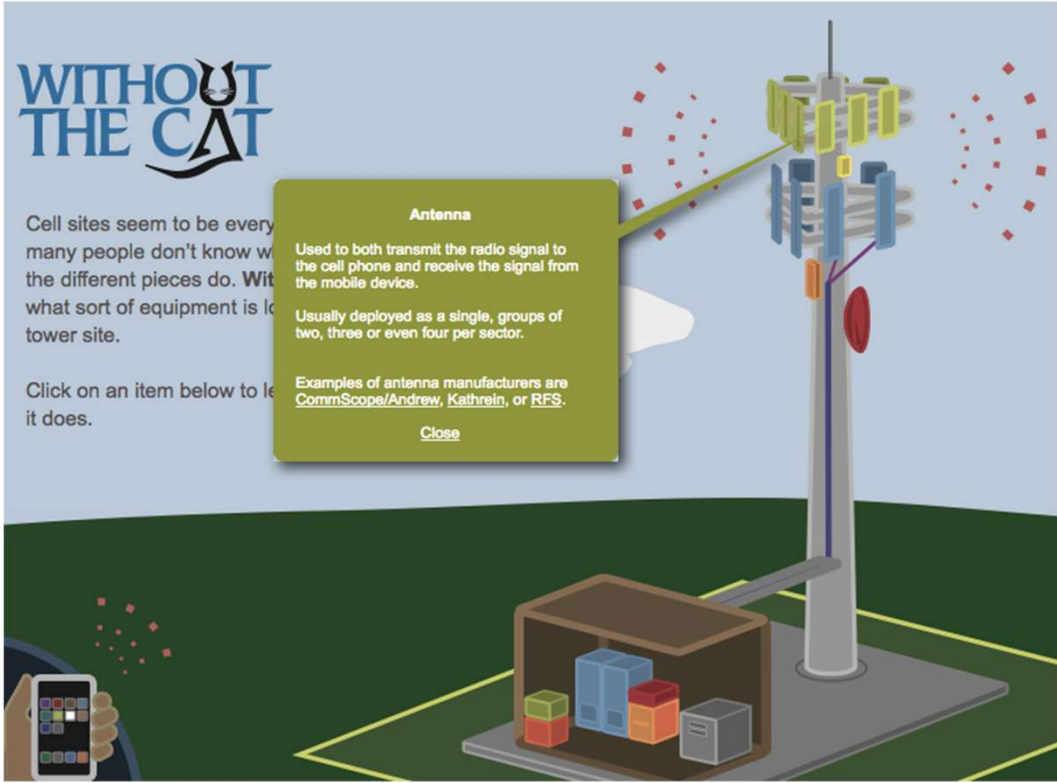
Antenna

Used to both transmit the radio signal to the cell phone and receive the signal from the mobile device.

Usually deployed as a single, groups of two, three or even four per sector.

Examples of antenna manufacturers are [CommScope](#), [Andrew](#), [Kathrein](#), or [RFS](#).

[Close](#)



WITHOUTTHECAT.COM

establish
information
degrees
foundation
prove
admissible
demonstrate
confirmation
defense
law
jury
material
judge
burden
legal
law
facts

EVIDENCE

document
proof
case
truth
likely
subject
important
degree
testimony
gather
proven
deciding
attestation
argument
court
verification
motive
raise
doubt
affirm
subject
document
likely
important
gather
deciding
attestation
argument
court
verification
motive
raise
doubt
affirm

EVIDENCE ADMISSIBILITY

Evidence Collection

- Follow established legal processes.
- Use accepted and proven techniques and tools.
- Employ certified digital experts.



CHAIN-OF-CUSTODY

- Chronological Documentation
 - Accounts for location and access of evidence from the time it is collected/seized until the time it is used in a legal or administrative proceeding.

The image features a central black rounded rectangle containing white text. On either side of the rectangle, there are decorative blue circuit-like lines with small circles at their ends, resembling a printed circuit board layout. The background is a light blue gradient.

IN GENERAL CHAIN-OF-CUSTODY FOR
ELECTRONIC EVIDENCE IS NOT MUCH DIFFERENT
THAN OTHER PHYSICAL EVIDENCE – BUT REQUIRES
A LOT MORE INFORMATION

CHAIN-OF-CUSTODY (COC)

The "sequencing" of the CoC follows this order: identification and collection; analysis; storage; preservation; transportation; presentation in court; return to owner.

The CoC shows: who obtained the evidence; where and when the evidence was obtained; who secured the evidence; who had control or possession of the evidence.

EVIDENCE

- Evidence should be handled according to agency policy while maintaining a chain of custody.
- Network isolation should be maintained.
- Additional forensic analysis may need to be performed:
 - To conduct traditional forensic processes on a mobile phone (DNA, latent prints, etc.).
 - Contact appropriate crime lab personnel for guidance on processing order to avoid the destruction of forensic evidence.

EVIDENCE: FARADAY

- Faraday Bag/Box: Used for digital evidence collection, preservation and examination.
 - Shields digital evidence from cellular, WiFi, Bluetooth and radio frequency (RF) signals.
 - <https://edecdf.com/collections/mobile>
- Faraday Cage/Tent

FARADAY BAGS/BOXES/CAGES/TENTS



- Evidence
- Preservation
- Examination



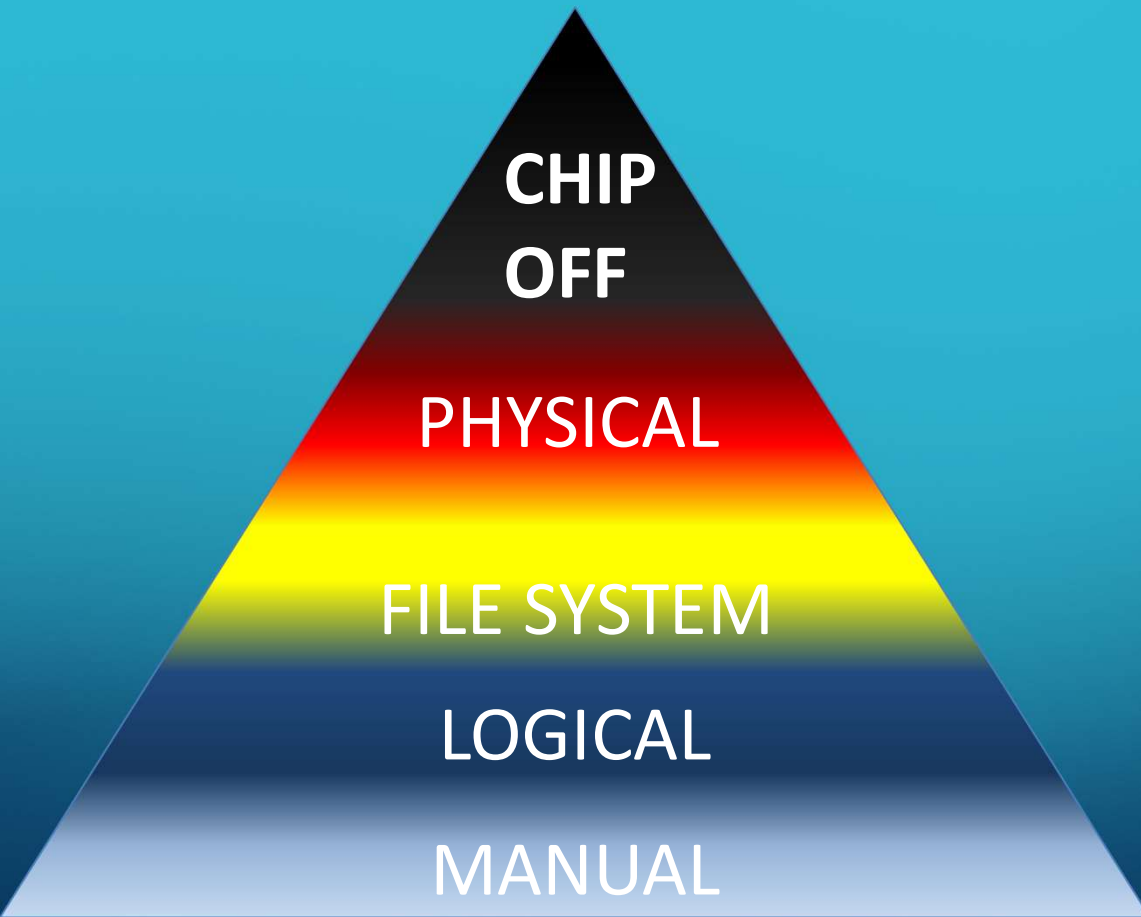
Seizing Evidence

- Review search warrant.
- **“Ask” mobile user for pass codes or PINs.**
- Process Immediately OR Turn off Phone and remove battery?
 - Turning OFF:
 - Preserves call logs and last cell tower location information (LOCI).
 - Prevents overwriting deleted data.
 - Prevents improper mobile phone handling.
 - CON - Removes information from active memory.
 - CON - May make it harder for forensic analysis.

Seizing Evidence

- Locking the phone by password or PIN.
- Many mobile phones can be placed in “Airplane” mode.
 - Not really a great solution - Does not do what people expects
- Collect associated chargers, cables, peripherals, and manuals.

PYRAMID LEVELS OF EXAMINATION



- The higher the level, the more complex
- Tools more \$
- Longer analysis times
- More training
- More Invasive



mobileforensics