



Password cracking machine built with 4 Nvidia 2080 graphic cards each



The evidence server now has 1 Petabyte of storage + a 1 Petabyte backup server.



Siri is a chocolate Labrador Retriever trained to indicate on all electronic storage devices such as SD Cards, Micro SD Cards, thumb drives, cell phones, external hard drives, hard drives, ipads, and all other electronic devices





# PURPOSE OF DIGITAL FORENSICS



THE DIGITAL  
FORENSIC  
EXAMINER

1. Evidence Handling
2. Acquisitions
3. Analysis
4. Expert Witness
5. Ethics



## (1) EVIDENCE HANDLING

Chain-of-Custody forms have to be filled out showing how data was seized, gathered, transported, stored, copied, analyzed, preserved and secured for production.

Chain-of-Custody documentation must be maintained for all evidence

## (2) ACQUISITIONS



All new and re-used media wiped & verified before use.



Commercial Off the Shelf (COTS) computer forensic tools will be used.



The use of open source, freeware, shareware or in-house developed software is limited to support small specialized tasks and to fill gaps the COTS products lack.



### (3) ANALYSIS OF 1:1 FORENSIC COPIES



Forensic copy is used  
(not original media).



Document process (all  
HW, SW & Media).



All deleted files are  
recovered.



Unallocated space  
examined.



Slack space examined  
for lost/hidden data.



Password protected  
and encrypted files are  
unlocked, decrypted  
and examined.

## (4) EXPERT WITNESS



A skilled, qualified, and experienced practitioner that has been qualified by the court.



Ability to simplify technical concepts using facts.



May express an opinion deduced from evidence.



Knowledge of standardized and specific procedures.



Adhere to an established code of ethics.

## (5) ETHICS



How a specialized skill set is used to address moral and professional issues that are encountered daily.



Follow a code that includes characteristics such as honesty, integrity, objectivity, transparency, accuracy, accountability and confidentiality.



Practice due diligence, i.e., thoroughly analyze evidence based upon established and validated principles and only present facts.







# SMARTPHONE/WEARABLES & USER CHOICE



GREEN: WORN  
AND FULL DATA



YELLOW: PARTIAL  
DATA BY CHANCE



ORANGE: PARTIAL  
DATA BY CHOICE



RED: NO DATA BY  
CHOICE



DARK: NO  
ACTIVITY



BATTERY DEAD



HON. SAMUEL ALITO,  
UNITED STATES  
SUPREME COURT

RILEY V. CALIFORNIA,  
US. NO. 13–132

“Modern cell phones are of great value for both lawful and unlawful purposes. They can be used in committing many serious crimes, and they present new and difficult law enforcement problems.”





LAW = COMPLICATED

- Electronic Communications Privacy Act, 18 USC §2510
- Stored Communications Act, 18 USC §2701
- Protect America Act, Public Law 110-55
- Third-Party Doctrine

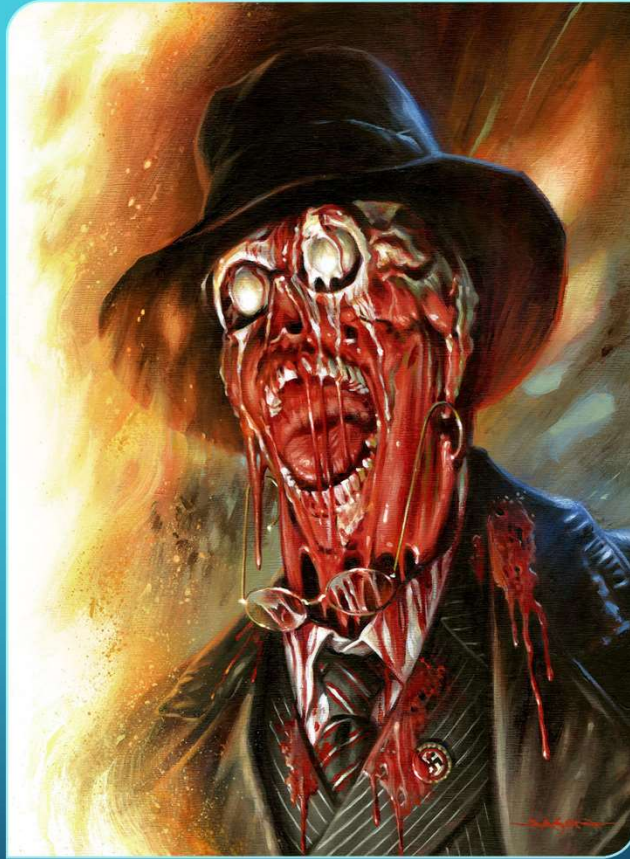
## TRADITIONAL METHODS











# RILEY V. CALIFORNIA

US. NO. 13-132. ARGUED APRIL 29, 2014—DECIDED JUNE 25, 2014

**Held:** The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

CRIMINAL COURT OF THE CITY OF NEW YORK  
COUNTY OF QUEENS

Warrant# \_\_\_\_\_

IN THE MATTER OF THE APPLICATION OF  
DETECTIVE \_\_\_\_\_ SHIELD NO. \_\_\_\_\_  
OF THE NYPD FOR A SEARCH WARRANT

SEARCH  
WARRANT

TO ANY MEMBER OF THE NEW YORK CITY POLICE DEPARTMENT AND TO ANY  
POLICE OFFICER OF THE STATE OF NEW YORK:

Proof by affidavit and/or oral deposition, having been made this day before me by  
Detective \_\_\_\_\_ Shield No. \_\_\_\_\_ of the New York City Police Department,  
there is reasonable cause to believe the following will be found at  
Street, \_\_\_\_\_ Queens County, New York:

- Computers (as that term is defined in Section 156.00 (1) of the Penal Law of New York), also known as electronic devices, including but not limited to desktop CPUs, laptops, cell phones, tablets and gaming devices;
- computer-related equipment such as video gaming devices, smart TVs, BluRay players, printers, scanners, keyboards, video display monitors, video game systems, optical readers, related communications devices such as modems and other devices that allow a user to connect to the internet;
- external storage media including hard drives, video gaming systems, optical storage devices, Smart TVs, memory storage devices including cameras, web cameras, and devices capable of storing and/or transmitting digital images;
- portable storage media such as flash drives, thumb drives, USB devices, memory cards, compact discs, DVDs, BluRay discs, magnetic media such as tape, cassette, disk, diskette or memory storage devices such as optical disks, programmable instruments such as telephones including cellular telephones, electronic calendar/address books, calculators, wristwatches, personal communication service (PCS) devices or any other storage media;
- documents in both hard copy format (printed, written, typed, photocopied, faxed, photographs, etc.), and electronically stored as computer data (as that term is defined in Section 156.00 (2) of the Penal Law of New York) (also known as electronic data) which may be contained on internal storage media or on any external storage media and which is likely to contain emails, chat transcripts or instant message transcripts, text messages, histories of access to internet websites, any contact information for correspondents including names, addresses, telephone

numbers, email addresses, screen names, profiles, etc. which may be contained in compilations such as buddy lists, or address books or in any other files;

- any documents or data, including but not limited to concerning email accounts, instant message accounts, and internet access accounts, regarding the possession, acquisition, storage, or transmission of images of adults or children engaged in sexually explicit conduct;
- any evidence including but not limited to any software that may be used for communicating over the internet or for storing said data or documents on an electronic device or on the internet including any online storage accounts also known as "cloud storage", e-mail accounts, or other remote electronic storage account including unique software for such account, subscriber information, user logs, or archived data that shows connection to such service, and user login and password for such service;
- any records containing or concerning addresses, telephone numbers, e-mail addresses, e-mails, instant messages, text messages or other electronic correspondence between or regarding correspondence between persons any person(s) appearing to be a minor child or person(s) interested in sex with young children including but not limited to correspondence and other records concerning attempts to contact young children, obtaining sharing or storing of photos or image files including video and still, any depictions of young children and/or adults engaged in sexual contact or lewd exhibition of the genitals;
- any software that may be used for sharing files over the internet or a local network including but not limited to any peer to peer software;
- records regarding the ownership of any electronic devices not limited to those recovered from the premises as well as manuals or notebooks regarding the operation of said electronic devices and any programs or external electronic device connected or contained on them;
- any notes regarding the protection of files by passwords, as well as any handwritten notes containing the name or any portion of any screen name, email address, profile name or password for any account;
- records regarding the ownership or use of said premises and equipment including but not limited to utility bills, telephone bills, cell phone bills, internet service provider bills, and bank account records which may be found at the premises described as follows:

Street, \_\_\_\_\_ Queens County, New York – an attached, private house with beige siding with suckers affixed to the exterior of the front, first-floor storm door which state Two entrances are in the front of the building – one beige door on the left side, garden-level and one red door with a glass window on the right-side, first-



floor – both with exterior glass and metal storm doors. In the center of first-floor storm door is a mail slot.

MOREOVER, there is reasonable cause to believe that the property set forth above will be at the premises set forth above and that said property is stolen or unlawfully possessed or has been used or is possessed for the purpose of being used to commit or conceal the commission of an offense or constitutes evidence or tends to demonstrate that an offense was committed in this state, or that a particular person participated in the commission of an offense in this state, to wit: Promoting a Sexual Performance by a Child, New York Penal Law Section 263.15; Possessing a Sexual Performance by a Child, Penal Law Section 263.16 and Conspiracy to commit those crimes as defined in Article 105 of the Penal Law.

YOU ARE THEREFORE COMMANDED to make a search of the above-described premises, to wit: Queens County, New York, within ten (10) days of the signing of this warrant and commencing between the hours of 6 am and 9 pm, without first announcing your presence or authority,

**NO KNOCK**

AND, if you find such property and/or evidence, or any part thereof, to bring it and this warrant before this or another Court without unnecessary delay, and it is further;

ORDERED that Special Agents from Homeland Security Investigations, Child Exploitation Group may assist in the search of the above-described premises;

ORDERED that you may forensically examine such computer(s), computer related equipment, internal or external storage media, portable storage media, or personal communication devices and computer data as you may find, and copy any computer data, and examine and photograph or videotape or digitally copy any of the above described property and that the premises may be photographed, to assist in the documentation of the search;

ORDERED that the affidavit of Detective \_\_\_\_\_ of the New York City Police Department, in support of the application for this warrant is hereby sealed pending the further order of this Court or another court of appropriate jurisdiction.

ORDERED that you may utilize fingerprint unlocking or facial recognition require any occupant of \_\_\_\_\_ Queens County, New York to press their finger(s) against the fingerprint sensor of the

locked device(s) found at the premises in an attempt to identify the device user(s) and unlock the device(s).

ORDERED that should the device require facial recognition, you may have each occupant look at the phone screen in an attempt to unlock the device.

IT IS FURTHER ORDERED, that in performing the forensic examination you are hereby authorized to utilize the assistance of others with expertise in decoding and/or obtaining password protections and/or encryptions, and in transferring, downloading, converting, dumping or draining of data from the memories of such electronic devices, in order to minimize the possible loss or alteration of such data in the course of making such data legible and storable in legible form. Such experts may be members of law enforcement organizations not empowered to execute search warrants by New York law, industry trade associations, or from companies which manufacture or service such electronic devices or telecommunications industries.

Queens, New York

Judge of the Criminal Court

Date: 11/18/19

Time: 2:46 PM

NO MINUTES TAKEN

# RILEY V. CALIFORNIA

US. NO. 13-132. ARGUED APRIL 29, 2014—DECIDED JUNE 25, 2014

Officers may examine the phone's physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one.

# IDEAL CONCEAL CELLPHONE GUN



Chimel v. California (395 U.S. 752): Requires that a search incident to arrest be limited to the area within the arrestee's immediate control. Where it is justified for officer safety and/or evidence preservation.

United States v. Robinson (414 U. S. 218): Expanded Chimel to almost all arrest situations.

**The Court in Riley declines to extend Robinson's categorical rule to searches of data stored on cell phones...But a search of digital information on a cell phone does not further the government interests identified in Chimel, and implicates substantially greater individual privacy interests than a brief physical search.**



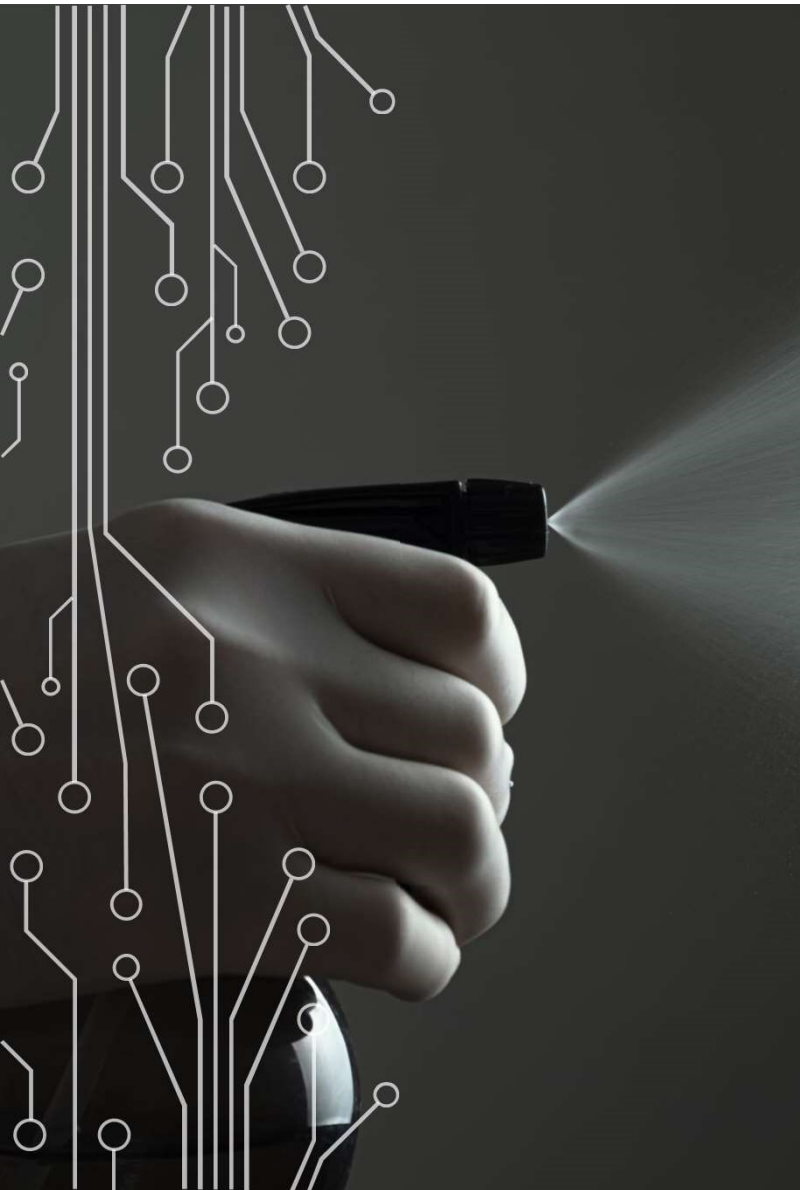
# RILEY V. CALIFORNIA EXCEPTIONS

- Exigent Circumstances



## RILEY V. CALIFORNIA

The United States and California raise concerns about the destruction of evidence, arguing that, even if the cell phone is physically secure, information on the cell phone remains vulnerable to remote wiping and data encryption.



The briefing also gives little indication that either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution. And, at least as to remote wiping, law enforcement currently has some technologies of its own for combatting the loss of evidence.

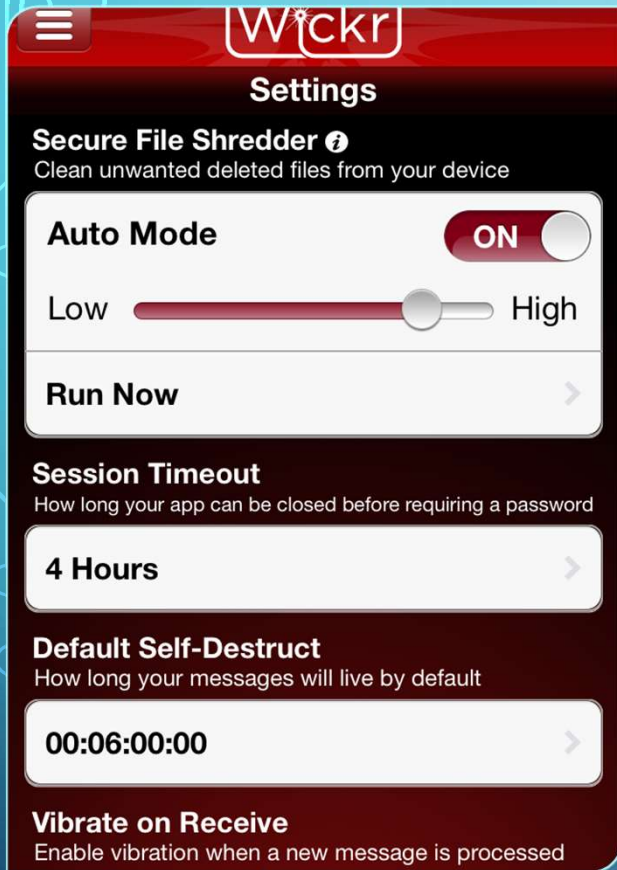
## **St. Augustine Man Pleads Guilty To Remotely Deleting Contents Of His iPhone After Federal Agents Seized It During The Execution Of A Search Warrant**

Jacksonville, Florida – United States Attorney Roger B. Handberg announces that Gabriel Basart (33, St. Augustine) today pleaded guilty to destroying evidence with the purpose of preventing and impairing the United States' lawful authority to take and search that evidence pursuant to a lawful search warrant. Basart faces a maximum penalty of five years in federal prison. A sentencing date has not yet been scheduled.





## REMOTE WIPE



# REMOTE FORENSIC WIPE

POST  
RILEY V.  
CALIFORNIA

Arrest → Search/Arrest  
Warrant → 1:1 Image

Search/Arrest Warrant →  
Arrest → 1:1 Image



# 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



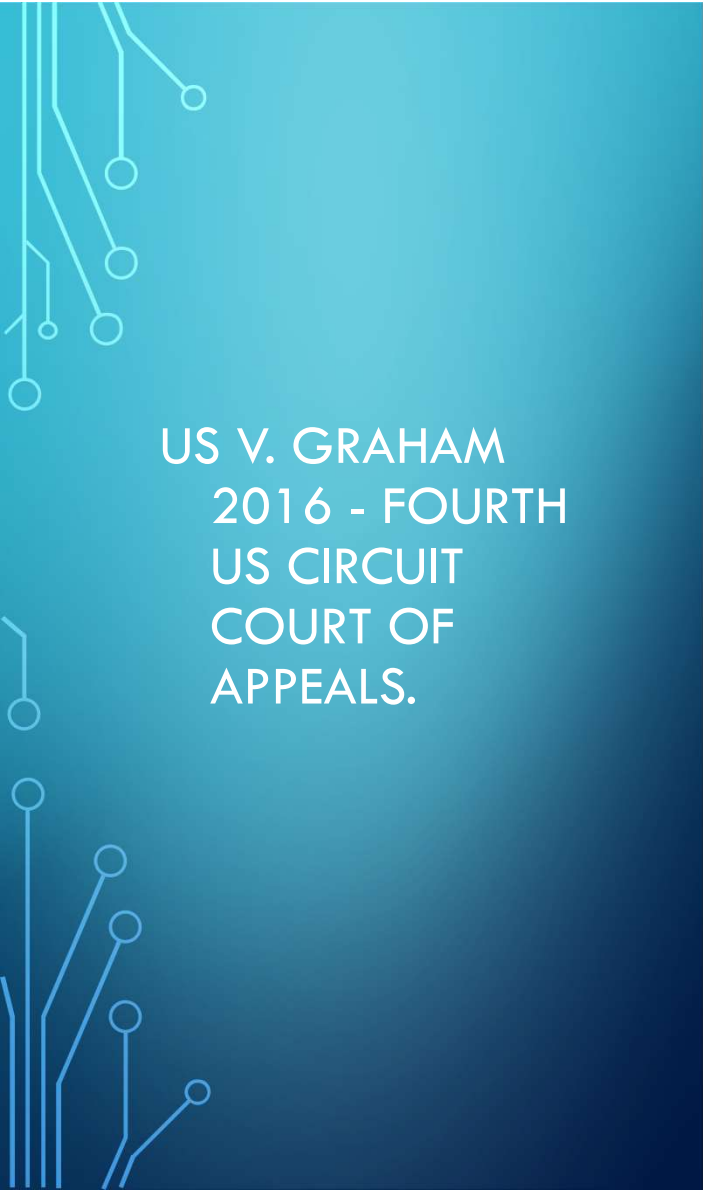
## THIRD PARTY DOCTRINE

---

“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" of the information.

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

"Without a showing of a legitimate expectation of privacy in the information, the Fourth Amendment does not apply."

Therefore, the court did not conclude that the Government violated the Fourth Amendment.

Content

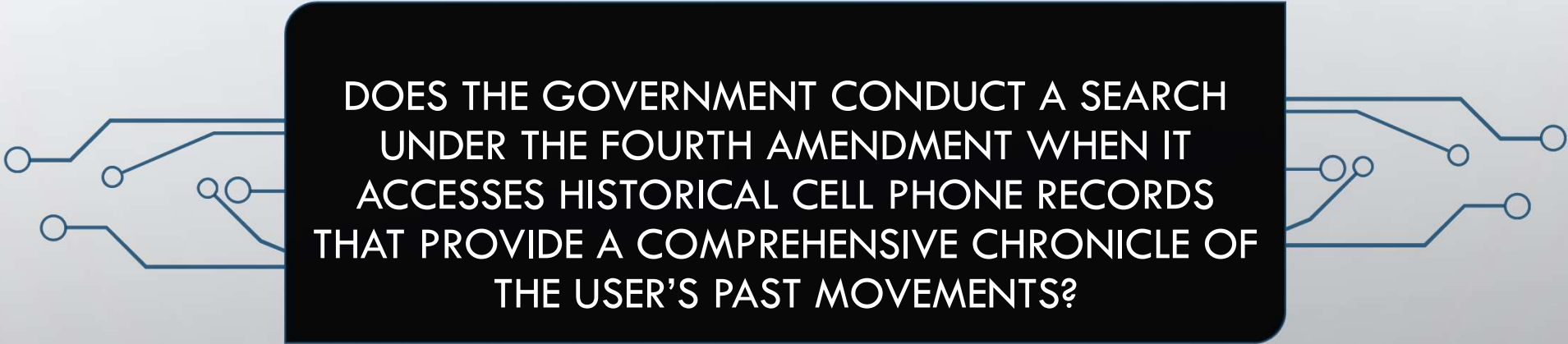
OVERTURNED



# CARPENTER V. UNITED STATES

585 U.S. \_\_\_, 138 S.Ct. 2206 (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("../" . $Delete);  
        if ($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\" folder=\"$folders[$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++)  
        fsetrcmp(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.



**verizon**wireless

**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>