Cell Phone Technology Searches

CRIMINAL LAW POWER UPDATE

October 30, 2014

Presented by:

Donald H. Flanary, III

Goldstein Goldstein and Hilley


The “US Government” Would Like To Use Your Current Location
OK
OK


WATCHING YOU

Edward Snowden: the whistleblower behind the NSA surveillance revelations

Guardian.co.uk – By: Glenn Greenwald, Ewan MacAskill, Laura Poltras – June 8, 2013

The individual responsible for one of the most significant leaks in US political history is Edward Snowden, a 29-year-old former technical assistant for the CIA and current employee of the defence contractor Booz Allen Hamilton. Snowden has been working at the National Security Agency for the last four years as an employee of various outside contractors, including Booz Allen and Dell.

He left the CIA in 2009 in order to take his first job working for a private contractor that assigned him to a functioning NSA facility, stationed on a military base in Japan. It was then, he said, that he **"watched as Obama advanced the very policies that I thought would be reined in", and as a result, "I got hardened."**

Over the next three years, he learned just how all-consuming the NSA's surveillance activities were, claiming **"they are intent on making every conversation and every form of behaviour in the world known to them".**


NATIONAL SECURITY
at&t
AGENCY

Revelations about NSA in December

- **“Snowden documents show NSA gathering 5 billion cell phone records daily”**
- **“By cracking cell phone code, NSA has capacity for decoding private conversations”**
- **“How the NSA is tracking people right now”**

Revelations about NSA in December

- **“NSA infers relationships based on mobile location”**
- **“NSA tracking cell phone locations worldwide, Snowden documents show”**
- **“Cell phone data spying: It's not just the NSA”**

JUST CELL PHONE ISSUES

- Warrantless Search of Cell Phones Incident to Arrest
- Basics of Cell Phones and Evidence Collection
- The Electronic Tracking Post-*Jones*
- Cell Phone Data and Records
- Technologies Used by the Gov to Collect Information

Cell Phone Stats

- 83% of Americans have a cell phone
- 45% of cell phones are “Smartphones”

- **<u>Only way to keep your cell phone safe:</u>**

Warrantless Search of Cell Phones Incident to Arrest

- **Constitutional Debate:**
  - Cell phone is a “Container”

    vs
  - Cell phone is a “mini-computer”
  - 18th Century concepts for 21st Century Technology

Back to the Basics of Search Incident to Arrest

- *Weeks v. U.S.* (1914)
  - Police can search accused when arrested to discover evidence of a crime
- *Katz v. U.S.* (1967)
  - Search must be reasonable, meaning: pursuant to a warrant or an established exception
    - Search incident to arrest
    - Exigent circumstances
    - Written policy on inventory
    - Vehicle exception

Search Incident to Arrest

- *Chimel v. California* (1969)
- Police searched Chimel's entire home incident to his arrest
- Warrantless search incident to arrest is limited to:
  - (1) the arrestees person
  - (2) *area* under immediate control of arrestee.
    - Meaning "the area from within which he might gain possession of a weapon or destructible device"

Search Incident to Arrest

- *U.S. v. Robinson* (1973)
- Police searched pack of cigarettes found in breast pocket of arrestee's jacket
  - Two permitted searches of "areas":
    - Search "of the person"
    - Search of "the area within control of arrestee"

Search Incident to Arrest

- *U.S. v. Edwards* (1974)
- Police examined clothing to see if paint from crime scene was present. Because it was late and he had no other clothes to wear they searched the next morning.
  - Search of "both person and property in his immediate possession may be searched at the station house after arrest has occurred at another place"

Search Incident to Arrest

- *U.S. v. Chadwick* (1977)
- Agents searched a footlocker found in a trunk 90 minutes after arrest and at the station
  - A closed container in immediate control of arrestee is different than the clothing of the arrestee
  - If search of container is remote in time or place of arrest or exigency then there is no exception to the warrant requirement
  - “Repository of personal effects”

Search Incident to Arrest

- *U.S. v. Chadwick* (1977)
- Since the locker was not part of Chadwick's "person" when arrested,
- Then a warrantless search is not reasonable if no danger arrestee could access property to get a weapon or destroy evidence.

Search Incident to Arrest

- Clothing in *Robinson* and *Edwards* are considered to be part of "arrestee's person"
- Distinguishably different from the closed container in the "area within immediate control of arrestee" as in *Chadwick*

Search Incident to Arrest

- *New York v. Belton* (1981)
  - "Area within immediate control of arrestee"can be searched incident to arrest, including passenger compartments
  - This includes "containers" in the passenger compartments within reach regardless of whether it could actually hold a weapon or evidence of crime under investigation
  - "Container" is any object capable of holding another object

Search Incident to Arrest

- *Arizona v. Gant* (2009)
- Limited *Belton*
  - Search of a car incident to arrest unauthorized "after the arrestee has been secured and cannot access the interior of the vehicle"

Cell Phone Search Incident to Arrest

- The debate hinges on whether a cell phone is:
  - a container immediately associated with the person
    - Like a cigarette pack in *Robinson* or clothing in *Edwards*

  Or

  - an item not associated with the person, but an item within a person's immediate control
    - Like a footlocker in *Chadwick*

United States v. Wurie
Riley v. California
134 S. Ct. 2473 (2014)

- Supreme Court unanimously ruled that the search incident to arrest *exception* does **not** extend to a cell phone and that police need to get a search warrant in order to search an arrestee's phone after arrest

Riley and Wurie

- In *Wurie,* the United States appealed the judgment of the First Circuit which suppressed evidence from the cell phone of the defendant
- In *Riley*, the defendant appealed the judgment of the California Court of Appeals which affirmed his conviction.

Riley and Wurie

- In both cases, the contents of the defendants' cell phones were searched after they were arrested and evidence obtained from the cell phones was **used to charge the defendants with additional offenses.**
- While the officers could examine the phones' physical aspects to ensure that the phones would not be used as weapons, digital data stored on the phones could **not** itself be used as a weapon to harm the arresting officers or to effectuate the defendants' escape.

Riley and Wurie

- Further, the potential for destruction of evidence by remote wiping or data encryption was **not shown to be prevalent** and could be **countered by disabling the phones**.
- Moreover, the immense storage capacity of modern cell phones **implicated privacy concerns** with regard to the extent of information which could be accessed on the phones.

Cell Phone searches in Texas

State v. Granville,
423 S.W.3d 399 (Tex Crim App 2014)

- Defendant arrested at a school for disorderly conduct.
- Defendant's cell phone was searched and then charged with "improper photography"
- Cell phone was in the property room and accessed by police
- Most logical and outspoken rejection of *Finley*

State v. Granville

- "We reject [the State's] argument that a modern-day cell phone is like a pair of pants or a bag of groceries, for which a person loses all privacy protection once it is checked into a jail property room."

≠

State v. Granville

- "A cell phone is unlike other containers as it can receive, store, and transmit an almost unlimited amount of private information."
- "The potential for invasion of privacy, identify theft, or at a minimum, public embarrassment is enormous."

State v. Granville

- "Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once. There is no doubt that the Fourth Amendment protects the subjective and reasonable privacy interest of citizens in their homes and in their personal 'papers and effects.'"

State v. Granville

- Citizens do not lose their "expectation of privacy in the contents of [their] cell phone merely because [they have] been arrested and [their] cell phone is in the custody of police for safekeeping."
- The officer "could have seized appellant's phone and held it while he sought a search warrant, but, *even with probable cause*, he could not 'activate and search the contents of an inventoried cellular phone' without one."

Other Electronic Devices

- Cell phones
- Laptops
- Tablets
- USB drives
- Digital Cameras

Basics of Cell Phones and Evidence Collection

- The first handheld mobile phone was first invented in 1973

Nuts and Bolts of Cell Phones

- 30 minute battery life, charge time 10 hours
- By 2014 there will be 7.4 billion cell phones world wide
- 326 million cell phones in the U.S.
- 300,000 Cell sites in the U.S.
- In 2012 the average person sent/received 164.5 calls, 10 hours of voice, and 764 texts per month.

Nuts and Bolts of Cell Phones

- "A modern cell phone *is* a computer" Judge Posner. *U.S. v. Lopez*, 670 F.3d 803 (7th Cir. 2012)
- Modern Cell phones:
  - send and receive text messages
  - emails,
  - photos and video
  - access the Internet
  - play games,
  - Play and store music,
  - Act as GPS device
  - Run any of the 375,000 apps

Basic Cell Phone Location Technology

- Sophisticated radios
- That connect to a cellular network
- That accesses a public telephone network.

WHAT IS A CELL?

- In typical analog cell phone system, each carrier receives 800 frequencies to use across city
- carrier chops the city into the cells
- Each cell is thought of as hexagons on a big hexagonal grids

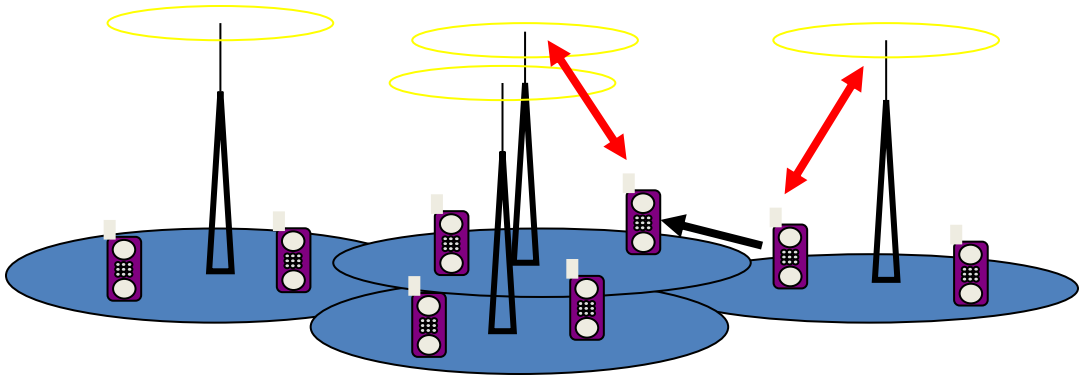
WHAT IS A CELL?

WHAT IS A CELL?

- Typically sized at about 10 square miles(26 kilometers)
- Each cell has base station consisting of tower and radio equipment
- Different cells (non-adjacent)can use the same set of frequencies

The Core Idea: Cellular Concept

- **The cellular concept**: multiple lower-power base stations that service mobile users within their coverage area and
- **handoff** users to neighboring base stations as users move.
- Together base stations **tessellate** the system coverage area.

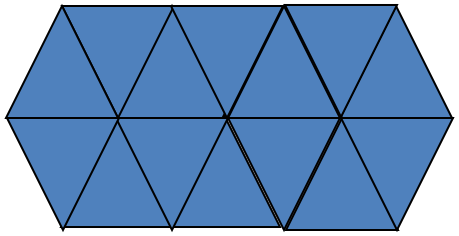


3 Core Principles

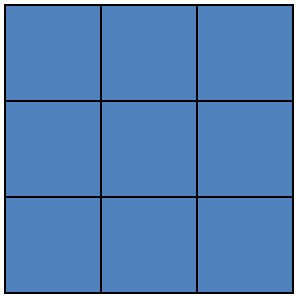
- Small cells tessellate overall coverage area.
- Users handoff as they move from one cell to another.
- Frequency reuse.

Tessellation (Cont'd)

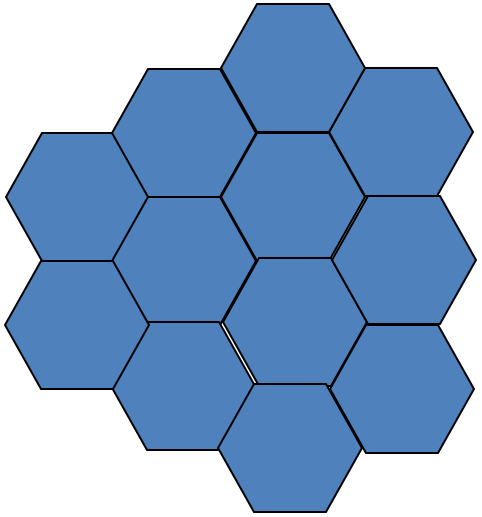
- Three regular polygons that always tessellate:
  - Equilateral triangle
  - Square
  - Regular Hexagon



Triangles



Squares



Hexagons

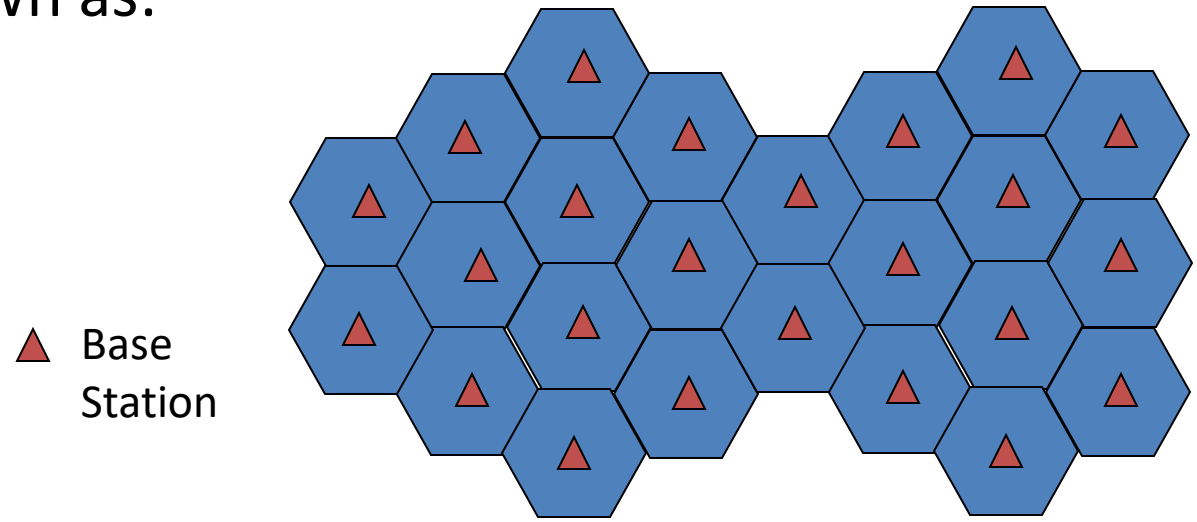
Circles Don’t Tessellate

- Thus, ideally base stations have identical, circular coverage areas.
- Problem: Circles do not tessellate.

- The most circular of the regular polygons that tessellate is the hexagon.
- Thus, early researchers started using hexagons to represent the coverage area of a base station, i.e., a cell.

Thus the Name Cellular

- With hexagonal coverage area, a cellular network is drawn as:



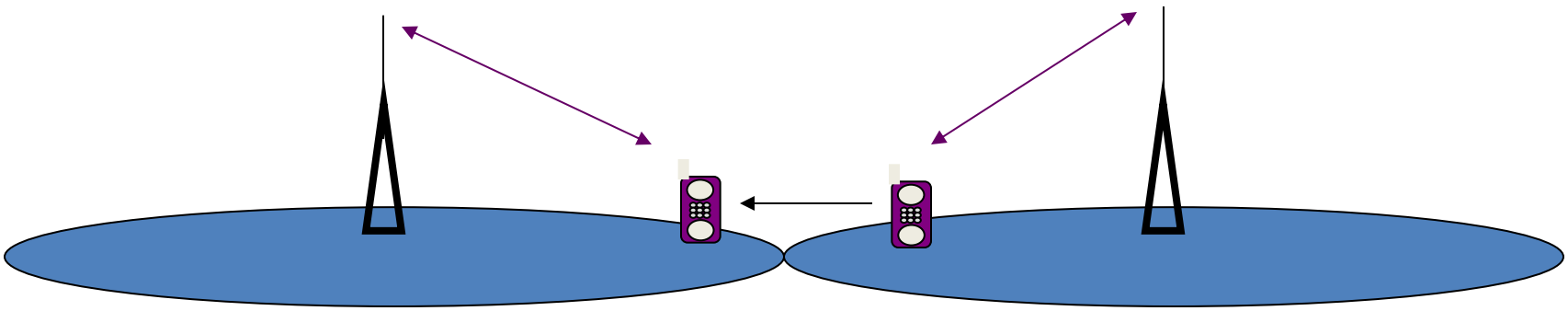
- Since the network resembles cells from a honeycomb, the name cellular was used to describe the resulting mobile telephone network.

Handoffs

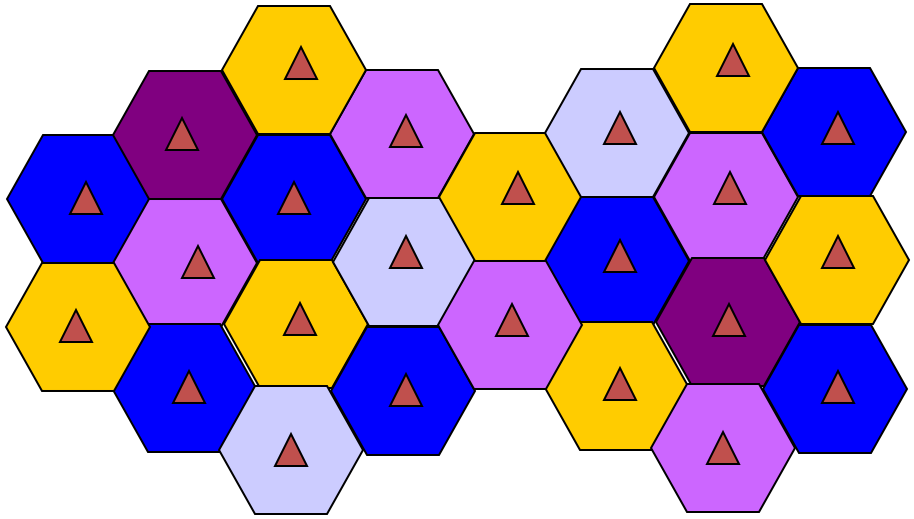
- A crucial component of the cellular concept is the notion of handoffs.
- Mobile phone users are by definition mobile, i.e., they move around while using the phone.
- Thus, the network should be able to give them continuous access as they move.
- This is not a problem when users move within the same cell.
- When they move from one cell to another, a **handoff** is needed.

A Handoff (Cont'd)

- At some point, the user's signal is weak enough at B_1 and strong enough at B_2 for a handoff to occur.
- Specifically, messages are exchanged between the user, B_1, and B_2 so that communication to/from the user is transferred from B_1 to B_2.



Example of Frequency Reuse



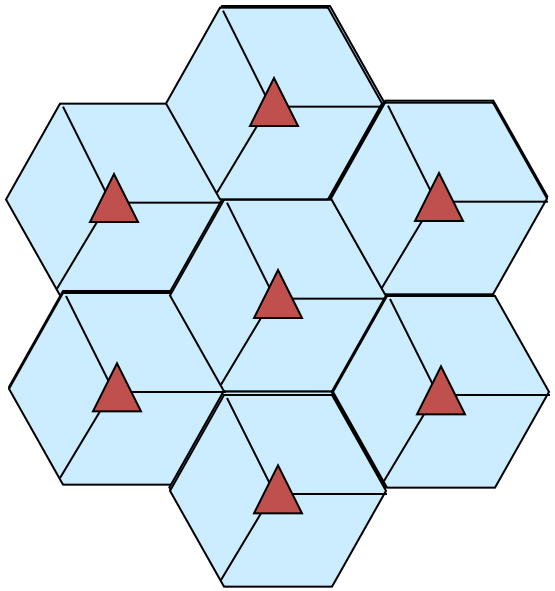
Cells using the same frequencies

Directional Antenna

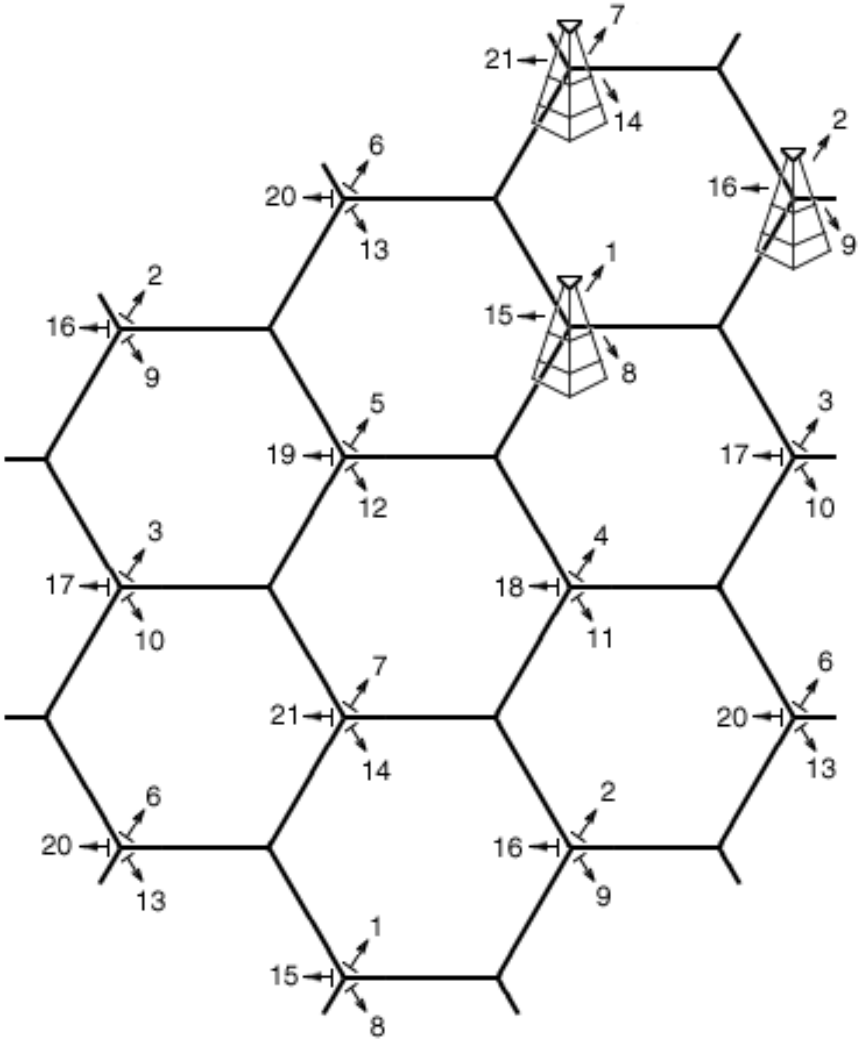
- One way to get more capacity (number of users) while maintaining cell size is to use directional antenna.
- Assume antenna which radiates not in alldirections (360 degrees) but rather in 120 degrees only.

Directional Antenna at Base Station

With 120 degree antenna, we draw the cells as:



Cellular Network with Directional Antennas



120 Degree Antenna Towers

CELL PHONE CODES

- All cell phones have special codes associated with them
- Service identification code (SID): 5 digit code assigned to each carrier
- Electronic serial number (ESN): 32 bit code programmed into phone by manufacturer
- Mobile identification number (MIN): 10 digit derived from phone's number

PURPOSE OF CODES

- Let we switch on the phone, then what happens?
- It listen for SID on control channel (special frequencies)
- “no service” message displayed
- Comparison of SID on control channel with the one programmed in phone.
- MTSO keeps track of phone’s location in database

Cell Phones as Tracking Devices

- Cell phones can used to track location:
  - "historically"
    - Or
  - in "Real Time"
- Cell phones can give
  - general location (by locating transmitting tower)
  - specific location (by intercepting GPS function)

Areas of Concern

- Line of sight
- Geography
- Weather
- Traffic and usage
- Scheduled/unscheduled maintenance
- An other things recommend by expert

The Electronic Tracking Post-*Jones*

Cell phones are similar to GPS devices but,

Only GPS addressed in *Jones*

U.S. v. Jones, 132 S.Ct. 645 (2012)

- Placing a GPS device on a vehicle and using it to track a vehicle's movement constitutes a search for 4th Amendment purposes.
- Agents obtained a warrant to placed a GPS device on Jones' Jeep during a drug investigation. However, Agents placed the GPS on the vehicle beyond the timing that the warrant allowed.

U.S. v. Jones, 132 S.Ct. 645 (2012)

- Decision based on 18th century law of Trespass
- Although a unanimous decision, 5-4 split on whether it is a violation as a trespass on property or a violation of expectation of privacy
- Access to factory installed or cell phone GPS was not addressed in *Jones (*Sotomayor concurring)
- Alito addresses Reasonable Expectation of Privacy and GPS

Cell Phone Data and Records

- **Cell Phones as Tracking Devices**
- **The Stored Communications Act**
- **Cellular Site Location Information (CSLI)**
- **Millions of Subpoena Requests by Law Enforcement**

Cell Phones as Tracking Devices

- Triangulation
- New phones are GPS devices

Triangulation

- Since phones connect to multiple towers, signal strength is analyzed and the distance from each tower is estimated.
- The more towers the phone is connected to, the better the estimation.
- This method cannot exactly pinpoint where a phone is, but is accurate enough to narrow it down to an area the size of an average neighborhood.
- REAL time or Historic

GPS

- Wireless service providers are required by law to have the capability to estimate position within 328 feet.
- These devices offer much higher levels of accuracy. In principle, they work on the premise of triangulation.
- Devices receives signals from 12 or more satellites in low-Earth orbit. These phones have software that runs in the background, unknown to the user, that gives the provider accurate readings on the customer's whereabouts.
- Only REAL time, not Historic (that we know of)

Four Categories of Electronic Surveillance

- (1) **wiretaps**, which are authorized pursuant to 18 U.S.C. §§ 2510-2522, upon what could be called a "probable cause plus" showing;
- (2) **tracking devices**, which are authorized pursuant to 18 U.S.C. § 3117, upon a Rule 41 probable cause showing;
- (3) **stored communications and subscriber records**, which are authorized pursuant to the Stored Communication Act (SCA) upon a showing of specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation; and
- (4) **pen registers and trap and trace devices** authorized pursuant to the pen register statute (PRS), upon the government's certification that the information sought is relevant and material to an ongoing criminal investigation


Don't Worry!
ABOUT THE CLICKING ON YOUR PHONE!
YOU'VE GOT NOTHING TO BE WORRIED ABOUT... IF YOU'RE NOT A TERRORIST!
A Message From The Ministry Of Homeland Security

Different Standards for Different Data

- **Intercepted real time electronic communications** (Title III **Wiretap**, "super-warrants"):
- 18 U.S.C. § 2510-2522 requiring probable cause to believe that a crime has been, is being, or is about to be committed; that communication is relevant to the crime; that normal investigation procedures have been tried, but failed; and the location of communication is connected to the crime.

Different Standards for Different Data

- **Tracking Device** installed GPS devices and Beepers
- Magistrate must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device. Rule 41, Fed Rules Crim. Pro.

Different Standards for Different Data

- **Stored communications and subscriber or customer account records** (Billing records and ID information as well as Historic Cell Location information):
- Subpoena requiring an application to a Federal Court including specific and articulable facts showing reasonable grounds for relevancy and materiality to ongoing investigation. 18 USC 2703(d) “Stored Communications Act”

Stored Communication Act
18 USC 2703

- Subscriber information 2703(c) court order, administrative or grand jury subpoena
  - Name, address,
  - Historic Cell phone information

- Content information- 2703(a) “a warrant”
  - Email, text messages, voicemail, photos, videos

Administrative Subpoenas

- Courts have held: no expectation of privacy in subscriber information and, therefore, a lesser showing is required of law enforcement to obtain the information *United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010), United States v. Perrine, 518 F.3d 1196, 1204,* (10th Cir. 2008); Guest v. Leis, 255 F.3d 325, 335-336 (6th Cir. 2001), United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

Administrative Subpoenas

- With an administrative subpoena, therefore, only the recipient of the subpoena, meaning the third party company, has cause to challenge the subpoena.
- Recently, Twitter challenged a government subpoena served to obtain the record information of people suspected to be members of WikiLeaks. *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), No. GJ3793,* 2011 WL 5508991 (E.D.Va. Nov. 10, 2011).

Different Standards for Different Data

- **Pen register and trap and trace device** (incoming and outgoing numbers, data sent and received): Court order requiring an application to a Federal Court showing that the information to be obtained is likely to be "relevant to an ongoing criminal investigation" 18 USC 3122(b)(2)

Third Party Records

Third Party Records

- BIG QUESTIONS!
- Content of stored communication rather than subscriber or billing records
- i.e. – Your Emails and Texts
- Not just the date and time of transmission.
- *U.S. v. Miller,* 425 U.S. 436 (1976) says no expectation of privacy in Third Party Records
  - i.e.: Bank Records, etc.

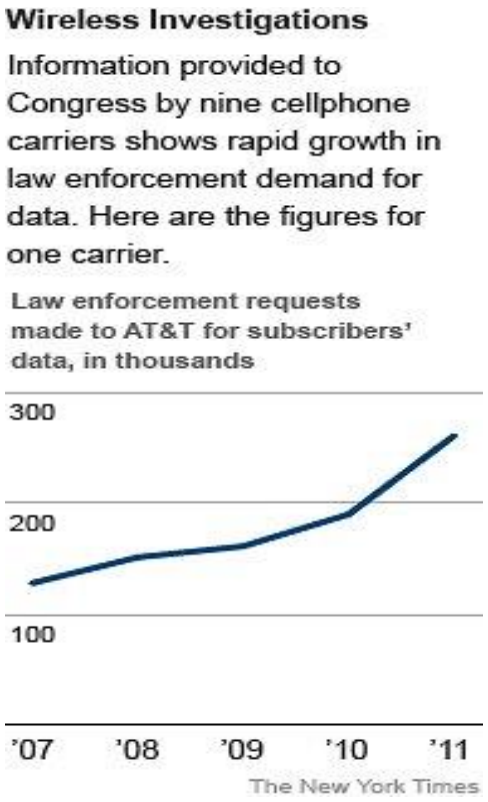
U.S. v. Pineda-Moreno

- In a companion case to *Jones*
  - 9th Circuit Chief Judge *Kozinski* dissented to the denial of rehearain en banc: "1984 may have come a bit later than predicted, but it's here at last."
- "If you have a cell phone in your pocket, then the government can watch you. At the government's request, the phone company will send out a signal to any cell phone connected to its network, and give the police its location. Last year, law enforcement agents pinged users of just one service provider-Sprint-over eight million times. The volume requests grew so large that the 110-member electronic surveillance team couldn't keep up, so Sprint automated the process by developing a web interface that gives agents direct access to users' location data."

More Demands on Cell Carriers in Surveillance

NYTimes.com – Eric Lictblau – July 8, 2012

In the first public accounting of its kind, cellphone carriers reported that they responded to a startling **1.3 million demands for subscriber information** last year from law enforcement agencies seeking **text messages, caller locations and other information in the course of investigations.**



CONGRESS GETS INVOLVED

The cellphone carriers' reports, which come in response to a Congressional inquiry, document an explosion in cellphone surveillance in the last five years, with the companies turning over records thousands of times a day in response to **police emergencies, court orders, law enforcement subpoenas and other requests.**

ALL LEVELS OF LAW ENFORCEMENT

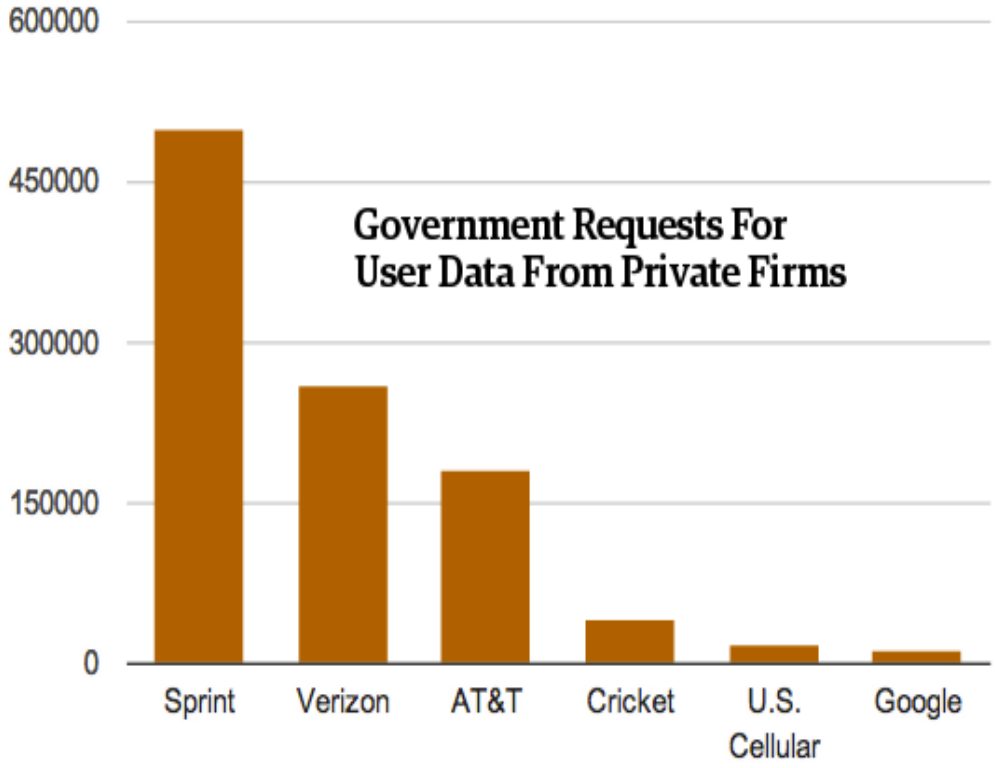
While the cell companies did not break down the types of law enforcement agencies collecting the data, they made clear that the **widened cell surveillance cut across all levels of government — from run-of-the-mill street crimes handled by local police departments to financial crimes and intelligence investigations at the state and federal levels**.

Here's How Often AT&T, Sprint, And Verizon Each Hand Over Users' Data To The Government

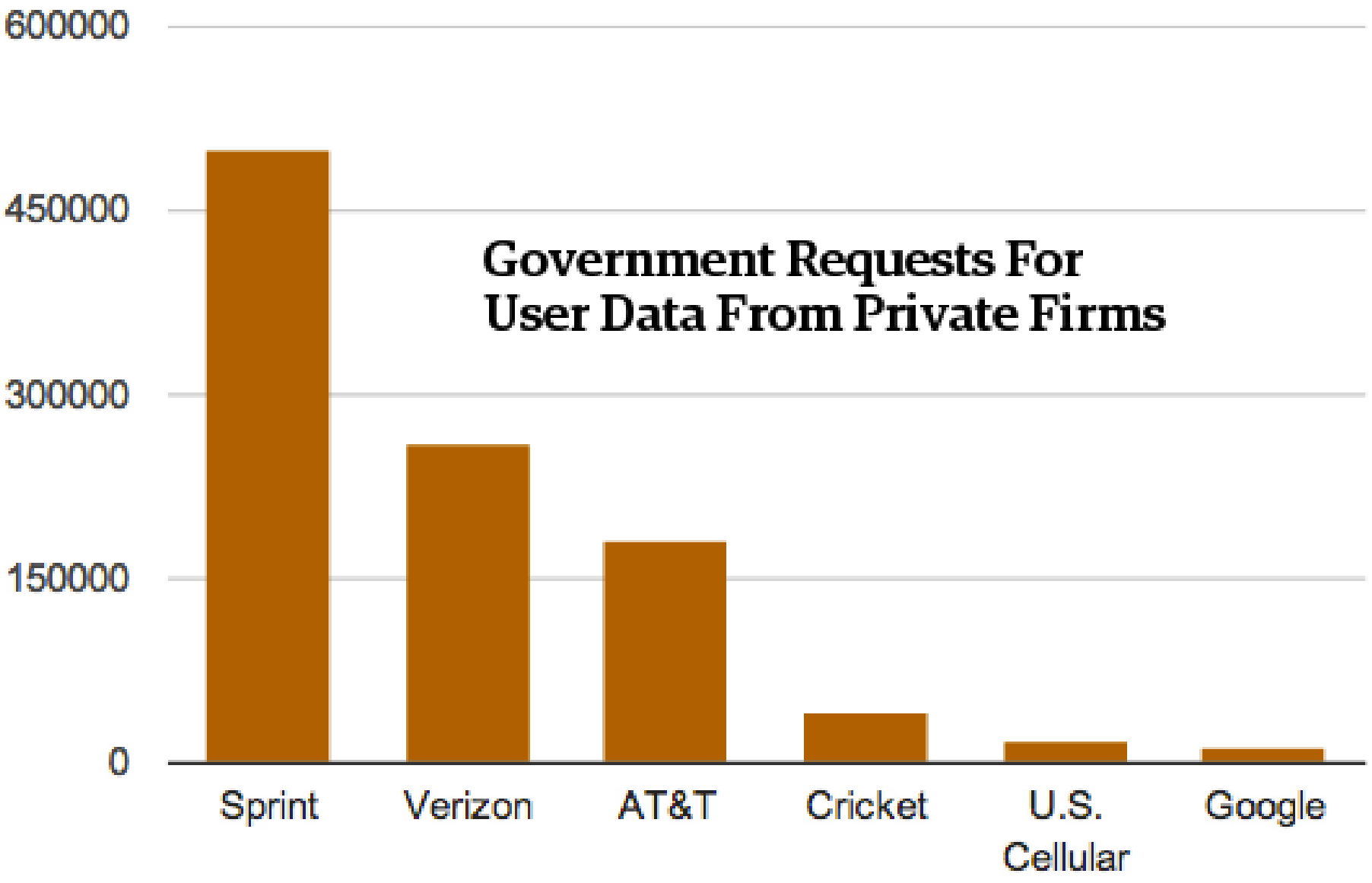
Forbes.com – By: Andy Greenburg – July 7, 2012

The vast majority of law enforcement's demands that phone carriers and Internet services hand over users' private data **don't require a warrant, and occur with little or no accountability**. It's not just that we don't know how much surveillance takes place.

To paraphrase Donald Rumsfeld, we don't even know *what we don't know* about how much the government knows about us.



It's important to remember that the information revealed Monday includes **"tower dumps,"** too, says Chris Calebrese, an attorney with the ACLU. "Just the sheer volume of orders is amazing, but a significant chunk are dumps from entire cell towers," he says. **"That means tons of people's information is being grabbed with a single one of these orders."**


600000
450000
300000
150000
0
Government Requests For
User Data From Private Firms
Sprint
Verizon
AT&T
Cricket
U.S. Cellular
Google

Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps

Forbes.com – By: Andy Greenburg – April 3, 2012

Wiretaps

T-Mobile charges law enforcement a flat fee of $**500** per target.

Sprint's wireless carrier Sprint Nextel requires police pay $**400** per "market area" and per "technology" as well as a $10 per day fee, capped at $2,000.

AT&T charges a $**325** activation fee, plus $5 per day for data and $10 for audio.

Verizon charges a $50 administrative fee plus $700 per month, per target.

Voicemail & Text Messages

AT&T demands $150 for access to a target's voicemail

Verizon charges $50 for access to text messages.

Sprint asks $120 for pictures or video, $60 for email, $60 for voice mail and $30 for text messages.

Cell Tower Dumps

AT&T charges $75 per tower per hour, with a minimum of two hours.

Verizon charges between $30 and $60 per hour for each cell tower.

T-Mobile demands $150 per cell tower per hour.

Sprint charges $50 per tower, seemingly without an hourly rate.

Real Time Location Data

Sprint charges $30 per month per target to use its L-Site program for location tracking.

AT&T's E911 tool costs $100 to activate and then $25 a day.

T-Mobile charges a much pricier $100 per day.

Technologies Used by the Gov to Collect Information

- **Cell Phone Software Extractors**
- **Stingray and Kingfish Cell Phone Tracking Devices**
- **Government Software/Internet Surveillance Programs**

Cell Phone Software Extractors

- **“Extraction Devices”** download personal information from cell phones,
  - including contacts
  - videos
  - GPS data
  - pictures
- “The handheld machines have various interfaces to work with different models and can even **bypass security passwords and access some information,”**

Mich. Cops Can Now Steal Your Cell Phone Data — 'Without the Owner Knowing'

TheBlaze.com – Jonathon M. Seidl – April 20, 2011

It's a scary scenario. You're driving down the road and get pulled over by a state patrolman. After checking your license and registration, the officer asks for your cell phone, and then uses a futuristic machine to download all your data. In Michigan, it's happening.

Michigan State Police are using **"Extraction Devices"** to download personal information from motorists' cell phones, including contacts, videos, GPS data, and pictures, **"even if they're not suspected of any crime."**

"The handheld machines have various interfaces to work with different models and can even **bypass security passwords and access some information,"**

What is Extracted???

"Complete extraction of **existing, hidden, and deleted phone data, including call history, text messages, contacts, images, and geo-tags,"** a brochure from device manufacturer Cellebrite says about the tool's capabilities.

"**The Physical Analyzer** allows visualization of both **existing and deleted locations** on Google Earth. In addition, location information from GPS devices and image geo-tags can be mapped on Google Maps."

cellebrite
delivering mobile expertise

UFED TOUCH ULTIMATE

All-inclusive Mobile Forensic Solution

UFED series

UFED TOUCH ULTIMATE

All-inclusive Mobile Forensic Solution

Cellebrite's UFED Touch Ultimate is a high performance mobile forensic solution. With its intuitive GUI and easy-to-use touch screen, the UFED Touch Ultimate enables the physical, logical and file system extraction of all data and passwords (even if they've been deleted) from the widest range of popular mobile phones, portable GPS devices and tablets.

The UFED Touch Ultimate includes:

- **UFED Physical Analyzer**: A powerful mobile forensic application enabling advanced decoding, analysis and reporting
- **UFED Phone Detective**: For instant mobile phone identification
- **UFED Reader**: Enables sharing of information with any authorized personnel

The UFED Touch Ultimate is a mission-ready solution for investigations in the field or lab and available in both standard and ruggedized versions.

The UFED Touch Ultimate Advantage

Setting the industry standard for mobile data forensic solutions, the UFED Touch Ultimate provides investigators with maximum capabilities:

- Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth, etc.
- Widest support for Apple devices running iOS3+
- Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including HTC, Motorola, Samsung Galaxy SIII family and more
- Physical extraction from Nokia BB5 devices – password extraction from selected devices
- File system extraction from any device running Windows phone 7.5 and 8 including Nokia, HTC, Samsung, Huawei and ZTE
- The most powerful solution for phones with Chinese chipsets
- TomTom® trip-log decryption, and data extraction from other portable GPS devices
- Obtain existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes etc.
- Proprietary technology and boot loaders ensure forensically sound extractions
- Frequent updates to ensure compatibility with new phones as they enter the market

Mission-Ready

The all-inclusive standard and ruggedized mobile forensic kits contain a full range of peripherals and accessories for successful investigations in the field or lab. Complete with lightweight phone connector tips, an embedded work shelf in the ruggedized case, integrated long-life battery and external hard drive makes mobile investigations quicker, easier and more efficient.

RUGGEDIZED KIT

STANDARD KIT

UFED Physical Analyzer

The UFED Physical Analyzer is the most powerful and technologically advanced mobile forensic application available. It exposes every segment of a device's memory data and provides in-depth decoding, analysis and reporting methods. Features include:

- **Malware Detection** – On-demand searches for viruses, spyware, Trojans and other malicious payloads in files
- **Project Analytics** – View statistics on communications and identifying relationship strengths
- **Rich Set of Data** – Includes calendar, call logs, contacts, SMS, MMS, chats, applications
- **Advanced Search** – Based either on open text or specific parameters
- **Timeline** – Monitor events in a single chronological view
- **Watch List** – Ability to highlight information based on predefined list of values
- **Image Carving** – Powerful feature used to recover deleted image files and fragments when only remnants are available
- **Conversation View** – View communications between sources in date and time order
- **Report Generator** – Generate and customize reports in different formats e. g. PDF, HTML, XML and Excel
- **SQLite Databases Viewer** – Viewing, searching and exporting tables and content (including deleted data) from SQLite database files
- **Hex Viewer** – Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more
- **Highlighted Parsed Content in the Hex** – Highlights the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex
- **Python Scripting** – Using the Python shell, enhances the capabilities for content decoding
- **Plugin and Chain Management** – Run Python scripts via plugins; edit and create new decoding chains

The UFED Phone Detective

The UFED Phone Detective appliaction comes with the UFED Touch kit, helping investigators identify a mobile phone at the start of an investigation. This eliminates the need to open the phone, risking phone lock. To identify a phone, users answer questions about the phone's attributes. UFED Phone Detective provides details on extraction capabilities, connectivity, device characteristics and more.

UFED Reader

UFED Reader allows authorized personnel to share examination results with others, regardless of whether they own UFED software. Simply forward the application and the extraction report to users for viewing and searching within the extracted data.

UFED CHINEX

Available as an add-on to the UFED Touch Ultimate is UFED CHINEX; the premium, field-ready solution for the extraction of evidentiary data from phones manufactured with Chinese chipsets. The kit contains:

- Enhanced phone adapter
- Adapter cables
- A large selection of individual connectors
- USB cable
- Quick user guide

Applications: UFED Physical Analyzer – UFED Reader – UFED Phone Detective

Hardware: UFED Touch Device – UFED Solid Protective Case – Tips & Cables Set – Tips & Cables Organizer – UFED Power Supply – Standard Carrying Case – Ruggedized Carrying Case* – Case Embedded Work Surface* – UFED Touch Screen Cover* – UFED External Hard Drive* – SIM ID Cloning Cards X3 – SIM ID Cloning Cards X5* – Micro SIM ID Cloning Cards X3 – Micro SIM ID Cloning Cards X5* – Micro SIM Adapter – Car Power Adaptor – UFED To PC Cable – Phone Power Up Cable – USB Flash Drive (8 GB) – DC 5v To 6v Adapter – Cleaning Brush For Phone Connectors – UFED Phone Charger* – UFED Forensic Memory Card Reader* – Faraday Bag* – User Manual

* Available in ruggedized version only

About Cellebrite

Founded in 1999, Cellebrite is a global company known for its technological breakthroughs in the cellular industry. A world leader and authority in mobile data technology, Cellebrite established its mobile forensics division in 2007, with the Universal Forensic Extraction Device (UFED). Cellebrite's range of mobile forensic products, UFED Series, enable the bit-for-bit extraction and in-depth analysis of data from thousands of mobile devices, including feature phones, smartphones, portable GPS devices, tablets and phones manufactured with Chinese chipsets.
Cellebrite's UFED Series is the prime choice of forensic specialists in law enforcement, military, intelligence, corporate security and eDiscovery agencies in more than 60 countries.

Cellebrite is a wholly-owned subsidiary of the Sun Corporation, a listed Japanese company (6736/JQ)

www.ufedseries.com
sales@cellebrite.com

HEADQUARTERS
Cellebrite Ltd.
94 Em Hamoshavot St.
Petah Tikva 49130
Israel
Tel: +972 3 926 0900
Fax: +972 3 924 7104

USA
Cellebrite USA Inc.
266 Harristown Rd., Suite 105
Glen Rock, NJ 07452
USA
Tel: +1 201 848 8552
Fax: +1 201 848 9982

GERMANY
Cellebrite GmbH
Am Hoppenhof 32a
33104 Paderborn
Germany
Tel: +49 52 51 54 64 90
Fax: +49 52 51 54 64 9 49

cellebrite
delivering mobile expertise

TOUCH ULTIMATE

inclusive Mobile
rensic Solution

UFED Touch Ultimate is a high
e mobile forensic solution. With its
I and easy-to-use touch screen, the
h Ultimate enables the physical,
file system extraction of all data and

The UFED Touch Ultimate Advantage

Setting the industry standard for mobile data forensic solutions, the UFED Touch Ultimate provides investigators with maximum capabilities:

- Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth, etc.
- Widest support for Apple devices running iOS3+
- Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including HTC, Motorola, Samsung Galaxy SIII family and more
- Physical extraction from Nokia BB5 devices – password extraction from selected devices
- File system extraction from any device running Windows phone 7.5 and 8 including Nokia, HTC, Samsung, Huawei and ZTE
- The most powerful solution for phones with Chinese chipsets
- TomTom® trip-log decryption, and data extraction from other portable GPS devices
- Obtain existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes etc.
- Proprietary technology and boot loaders ensure forensically sound extractions
- Frequent updates to ensure compatibility with new phones as they enter the market

Stingray and Kingfish Cell Phone Tracking Devices

KingFish-ing for Info

Fwweekly.com – By: Zach Shlachter – May 30, 2012

Police Use Cell Tracking to Establish Probable Cause!

In a memo to the council, police officials promised to use the new system, called **KingFish**, **“to establish probable cause” in criminal cases.** Thing is, probable cause — that is, enough evidence to establish that there is probable cause to believe a crime has occurred — is what a law enforcement agency usually needs ***first***, **to convince a judge to approve invasive measures such as home searches, arrests, wiretaps or, in some contexts, use of tracking technology against an individual.**

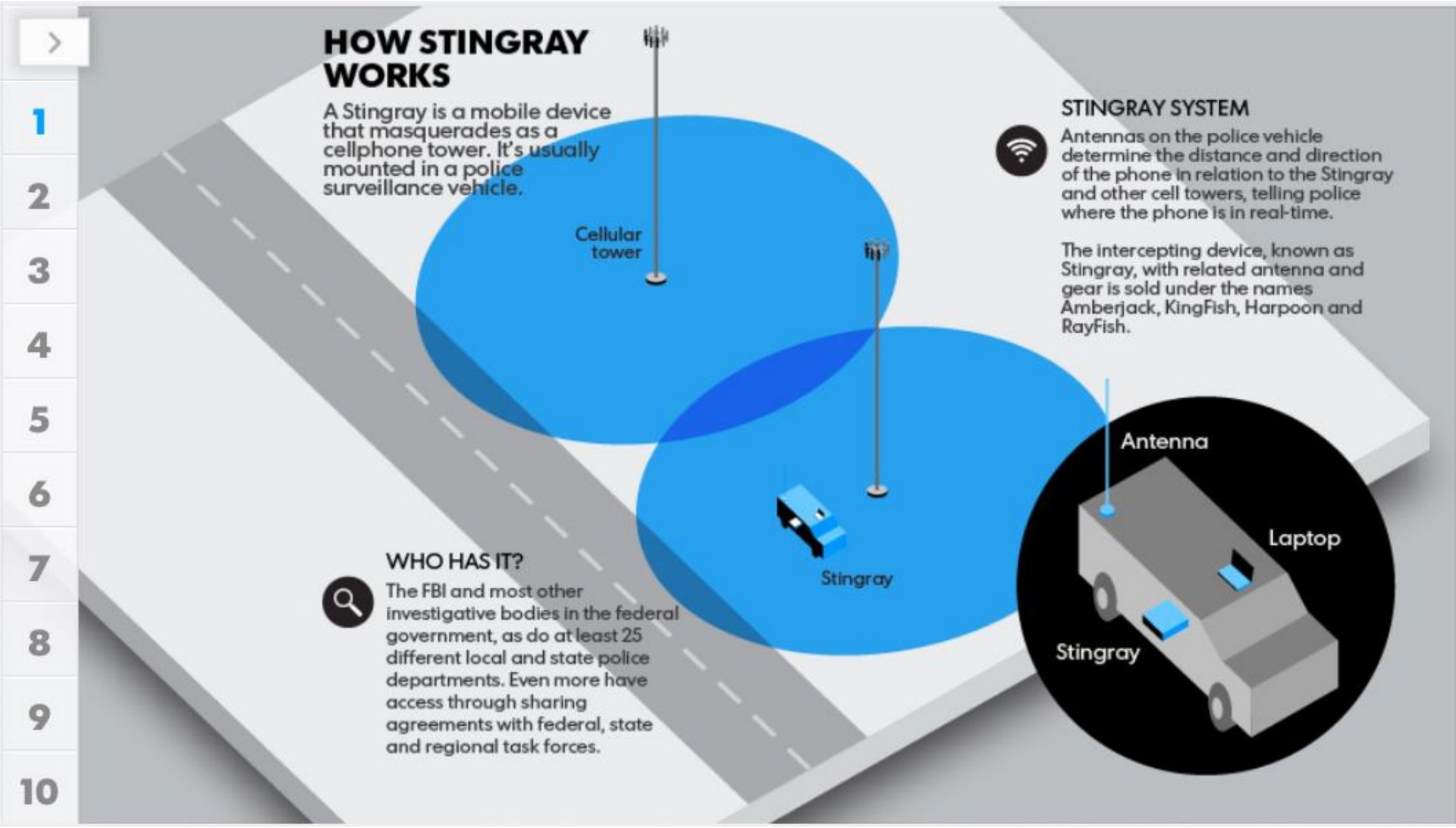
Police did not return *Fort Worth Weekly*’s calls seeking information for this story.

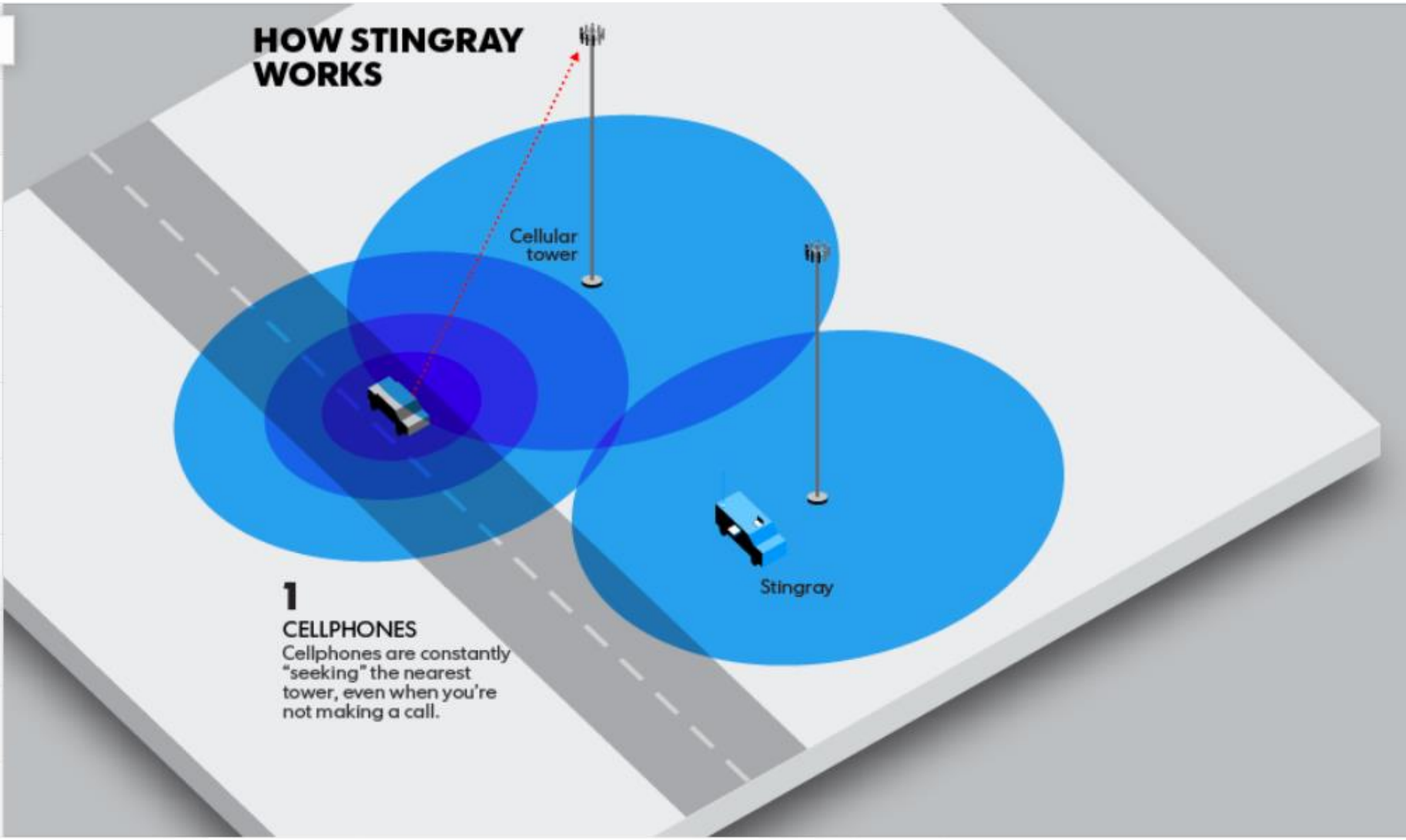
How Police avoid the 4th Amendment

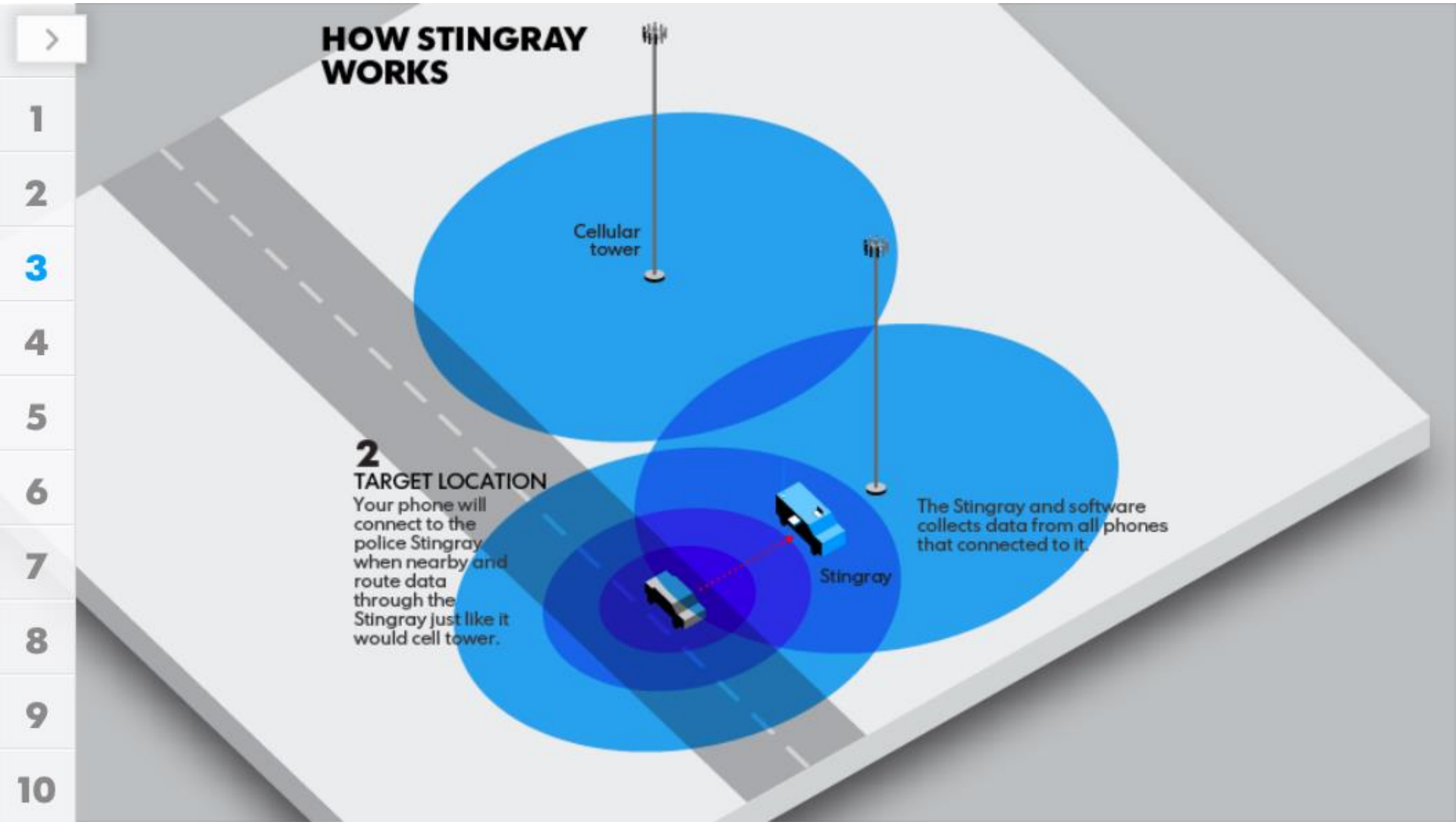
The KingFish devices — of a type generally known as **“stingrays”** — work differently than usual GPS monitors. Made by the Harris Corporation of Florida, **the devices act like dummy cell phone towers, so that a cell phone signal will ping off the device and make it unnecessary for police to get a court order to have the cell phone company release the information.**

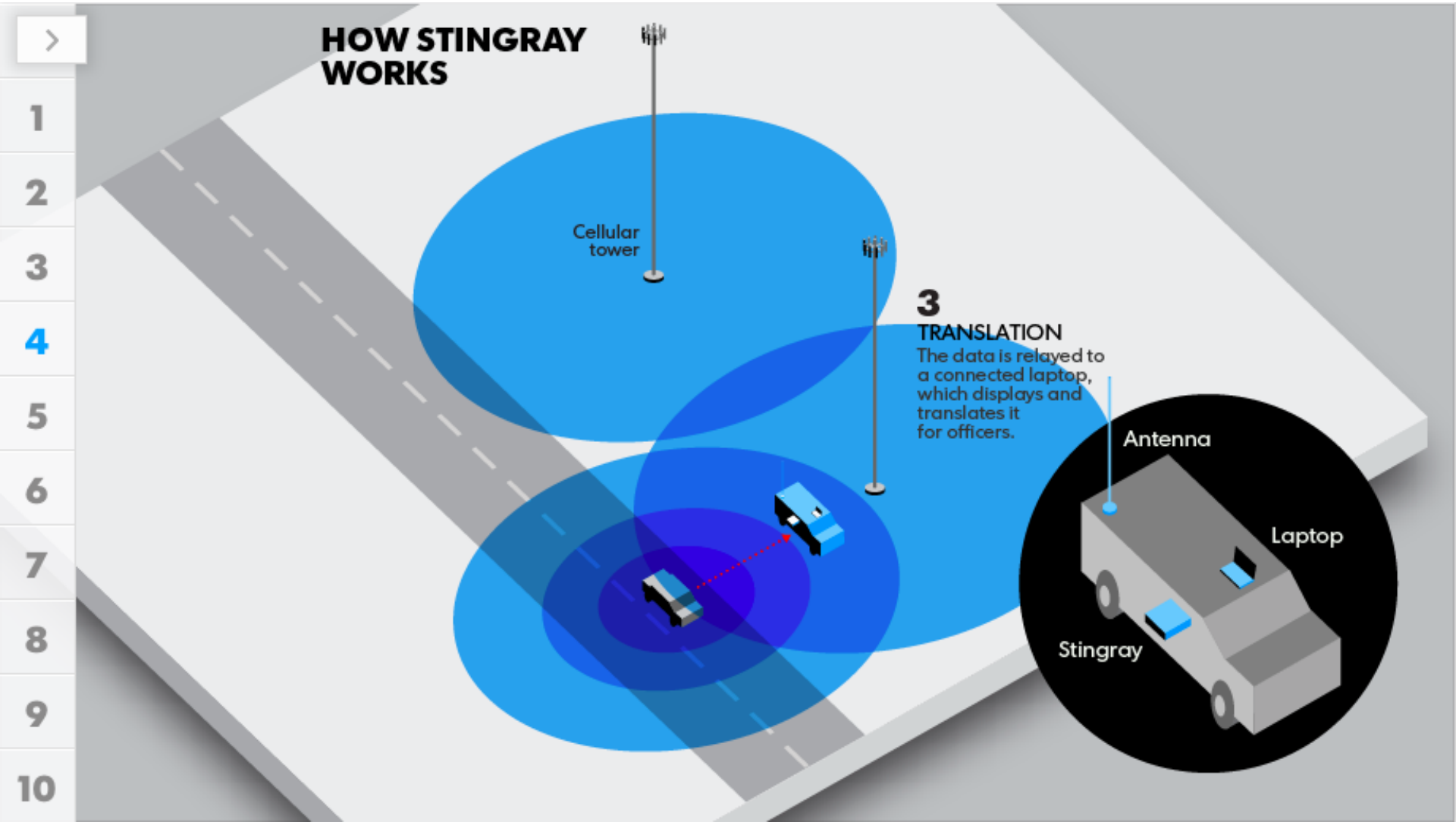
Under a 1986 federal law that controls some government information-gathering practices, **“non-content”** information like **location requires less of a legal showing than, say, a wiretap.**

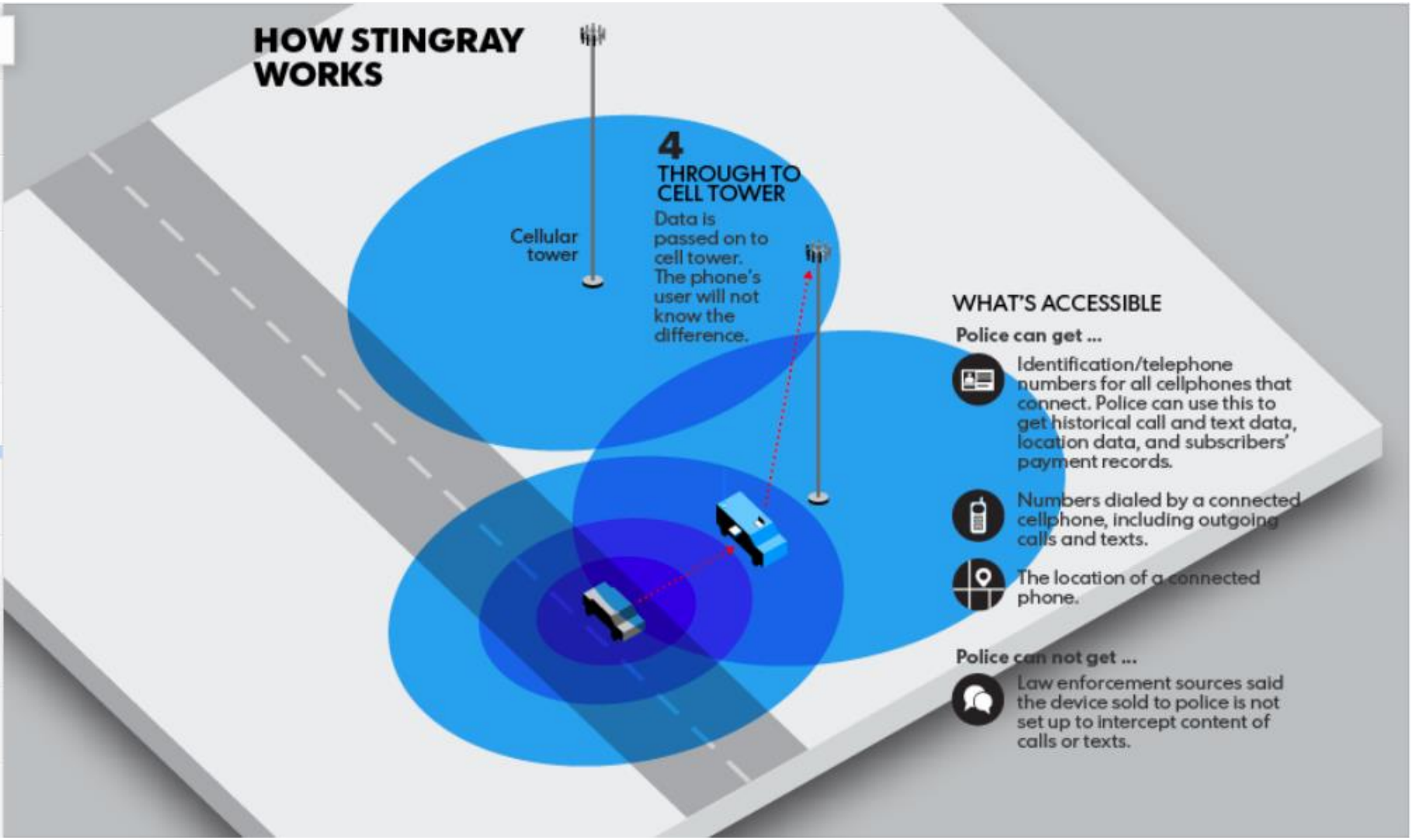
So it’s possible that Fort Worth police could legally use the their new stingray devices **without getting warrants**.


HOW STINGRAY WORKS
A Stingray is a mobile device that masquerades as a cellphone tower. It's usually mounted in a police surveillance vehicle.
Cellular tower
Stingray
STINGRAY SYSTEM
Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time.
The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.
Antenna
Laptop
Stingray
WHO HAS IT?
The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.


HOW STINGRAY WORKS
Cellular tower
Stingray
1
CELLPHONES
Cellphones are constantly "seeking" the nearest tower, even when you're not making a call.


HOW STINGRAY WORKS
Cellular tower
2
TARGET LOCATION
Your phone will connect to the police Stingray when nearby and route data through the Stingray just like it would cell tower.
Stingray
The Stingray and software collects data from all phones that connected to it.


HOW STINGRAY WORKS
Cellular tower
3
TRANSLATION
The data is relayed to a connected laptop, which displays and translates it for officers.
Antenna
Laptop
Stingray


HOW STINGRAY WORKS
Cellular tower
4
THROUGH TO CELL TOWER
Data is passed on to cell tower. The phone's user will not know the difference.
WHAT'S ACCESSIBLE
Police can get ...
Identification/telephone numbers for all cellphones that connect. Police can use this to get historical call and text data, location data, and subscribers' payment records.
Numbers dialed by a connected cellphone, including outgoing calls and texts.
The location of a connected phone.
Police can not get ...
Law enforcement sources said the device sold to police is not set up to intercept content of calls or texts.

The "StingRay" Cell Phone Spying Device

Global Research – By: Clarence Walker – April 13, 2013

Originally intended for terrorism investigations, the feds and local law enforcement agencies are now using the James Bond-type surveillance to track cell phones in drug war cases across the nation without a warrant. Federal officials say that is fine — responding to a Freedom of Information Act (FOIA) request filed by the Electronic Freedom Foundation (EFF) and the First Amendment Coalition, the Justice Department argued that **no warrant was needed to use StingRay technology.**

"If a device is not capturing the contents of a particular dialogue call, the device does not require a warrant, but only a **court order under the Pen Register Statute** showing the material obtained is relevant to an ongoing investigation," the department wrote.

Federal Prosecutors try to "Fool" Judges

The StingRay technology is so new and so powerful that it not only raises Fourth Amendment concerns, it also **raises questions about whether police and federal agents are withholding information about it from judges to win approval to monitor suspects without meeting the probable cause standard required by the Fourth.** At least one federal judge thinks they are. Magistrate Judge Brian Owsley of the Southern District of Texas in Corpus Christi told the Yale conference federal prosecutors are using clever techniques to fool judges into allowing use of StingRay. **They will draft surveillance requests to appear as Pen Register applications, which don't need to meet the probable cause standards.**

"After receiving a second StingRay request," Owsley told the panel, "I emailed every magistrate judge in the country telling them about the device. And **hardly anyone understood them."**

Carrier IQ

- Carrier IQ is a program for mobile devices that records every keystroke and every piece of data that comes in or out of your device.
- The data is sent back to Carrier IQ's servers.
- The program cannot be turned off and is very hard to track.
- It is believed to be used on HTC, Android and Blackberry phones. There is some evidence that it exists on Apple products as well.
- AT&T confirms that it uses the software while Verizon and Nokia deny that it exists on there phones.

Carrier IQ

- The rational is that the information collected will help the device manufacturers and software developers create better products and services for the consumer.
- Problem: Can the government access this information?
- We could see class-action litigation over these issues.
- *Source:* http://www.washingtonpost.com/business/technology/what-is-carrier-iq/2011/12/01/gIQApql1GO_story.html

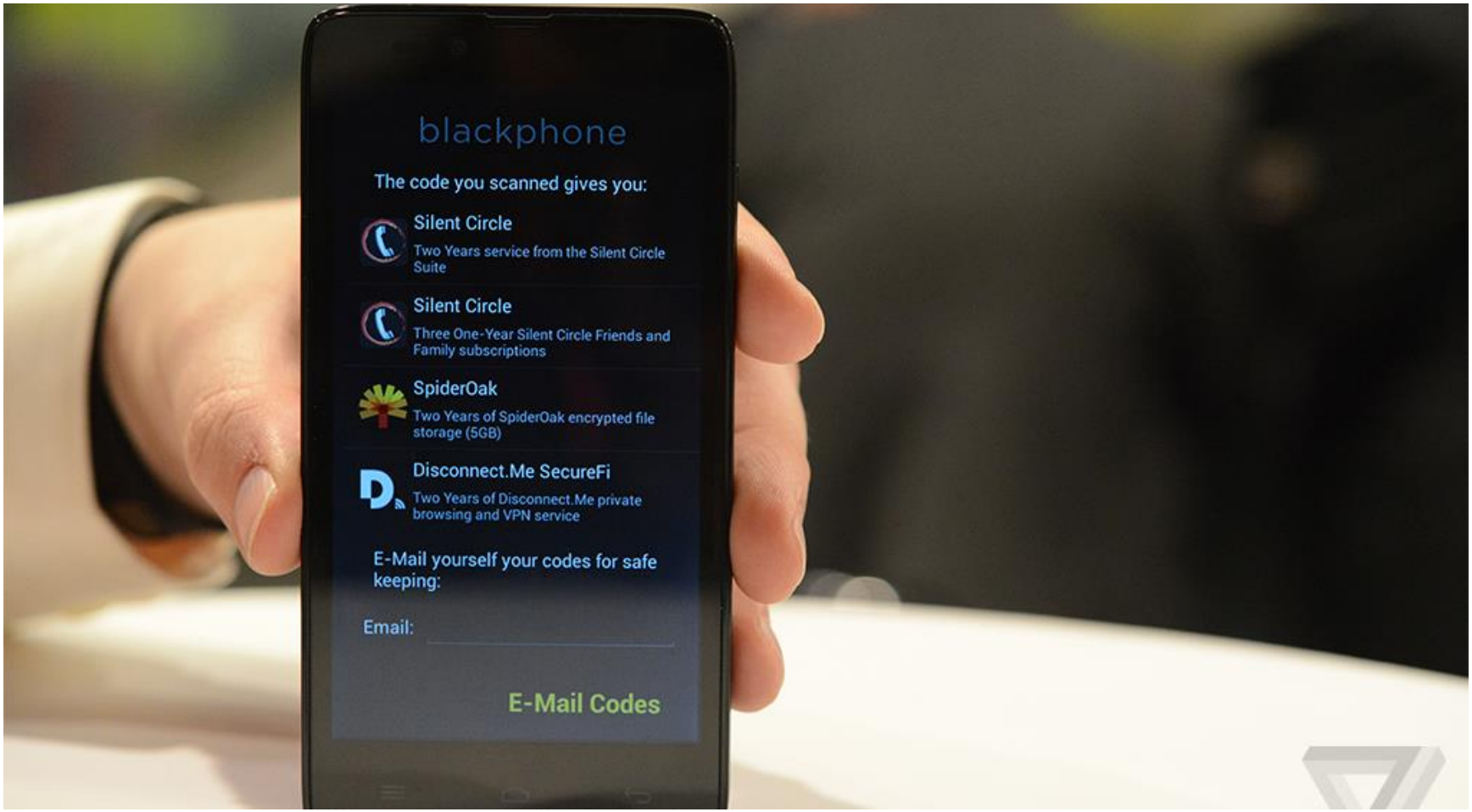
Things to Remember

- **State cases**
  - No searches of cell phones incident to arrest
  - Be aware of exigencies, i.e. destruction of evidence
- **Federal cases**
  - *Finley* controls for now but *Wurie* is on the horizon.
  - Good faith will apply for now, but getting a search warrant is always good practice

Things to Remember

- Cell site location information can be a helpful tool in determining the location of a defendant.
- There are strengths and weaknesses of the technology of which you should be aware.
- Where necessary consult an expert.

Get a Blackphone!



ABA Journal

- *Tools for Lawyers worried that NSA is Eavesdropping on their Confidential Conversations*
- www.abajournal.com
- Posted Mar 30, 2014 12:44 PM CDT By **Victor Li**

Blackphone

- “For lawyers worried about talking on the phone, their prayers could be answered in June when Spanish smartphone company GeeksPhone and software company Silent Circle launch Blackphone, an encrypted smartphone that protects phone calls, text messages, emails and Internet browsing. Using VPN technology, Blackphone promises to be an NSA-resistant phone.”

Get a Faraday Bag
(Radio wave sheild)

The End

- For more information:
- www.ggandh.com/presentations-lectures/

verizon wireless

Law Enforcement Resource Team (LERT)

Law Enforcement Resource Team

The LERT is centralized and handles all requests from local, state, county and federal law enforcement nationwide

LERT Responsibilities

- Ensuring all court orders, search warrants and subpoenas are processed confidentially and in compliance with all applicable laws and company policies
- Providing 24x7x365 technical assistance for electronic surveillances
- Providing 24x7x365 support for exigent situations
- Ensuring CALEA compliance both technically and procedurally
- Coordinating court appearances for a Verizon Wireless Custodian of Records
- Providing informational presentations for law enforcement organizations and associations

General Information

- Company Name: Cellco Partnership d/b/a Verizon Wireless
- Mailing Address:

  Verizon Wireless
  Attn: Custodian of Records
  180 Washington Valley Road
  Bedminster, NJ 07921

- Normal Hours of Operation: 7am-8pm Sun-Sat
- Exigent Situations: 24x7 on-site (prompt "4", should also be used for emergencies that may result in loss of information)

LERT Hotline

(800) 451-5242

- Prompt 1: General Information
- Prompt 2: Subpoenas & Search Warrants
- Prompt 3: Court Ordered Surveillances
- Prompt 4: Exigent (24x7)

LERT Fax Numbers

- Subpoenas & Search Warrants:
  - **(888) 667-0028**
- Court Orders:
  - **(908) 306-7491**
  - **(908) 306-7492**
- Exigent:
  - **(908) 306-7501**

Subpoena Group

- Responsible for all subpoenas, search warrants and the coordination of court appearances
- Goals
  -Subpoenas & Search Warrants – 14 days or within compliance time frame
  -To accommodate same or next day emergency requests (volumes permitting)

Types of Readily Available Information

Type of information	Current Retention
Subscriber - post paid	Typically 3-5 yrs*
Call detail records/cell sites	1 rolling year
Text message detail	1 rolling year
Text message content	3-5 days
IP session information	1 rolling year
IP destination information	30 days
Pictures	Only if on web site**
Bill copies - post paid	Last 12 months
Payment history - post paid	Typically 3-5 yrs*

*may vary by former company

**customer can add or delete pictures at any time

Other Types of Available Information

Type of information	Current Retention
Bill copies older than 12 months	Typically 3-5 yrs*
Check copies	Approximately 6 months
Credit Card Numbers	Approximately 6 months
Store Surveillance Videos	Typically 30 days
Service Applications	Typically 3-5 yrs*

* may vary by former company

Information Stored in the phones

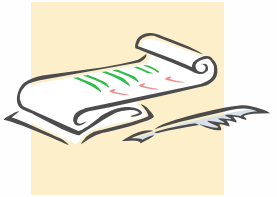
- Dependent in some cases on make and model
- Managed by person in possession of phone
- Types of information:
  - Text messages
  - Contact list/information
  - Calendar/schedule
  - Pictures
  - Downloads from internet (i.e., games, ring tones)
  - Dialed numbers
  - Incoming numbers

Court Order Group

- Staffed on-site 24x7
- Responsible for all surveillances, per court order requests, exigent situations, requests for location information and any content requests (i.e., text messages)
- Goals
  -Exigent Situations - immediately
  -Surveillances - same day
  -Per Court Order Requests - within 24 to 48 hours

Court Ordered Surveillances

- Fax required worksheet along with court order
  - -Names of authorized points of contact
  - -Address (street, city, state and zip code)
  - -Billing contact name and number
- All court orders must have a complete worksheet with set-up and billing information when faxed in order to be processed in a timely manner



Exigent Situations

- Complete, sign and fax exigent form/letter*
- Call (800) 451-5242 prompt "4" – 24x7
- Release of information

*If fax is unavailable because the officer/agent is in the field, we will use a call back verification process. If the call is to 9-1-1 and we can view it we will release the information. If we cannot see the call to 9-1-1 we will perform a callback verification.

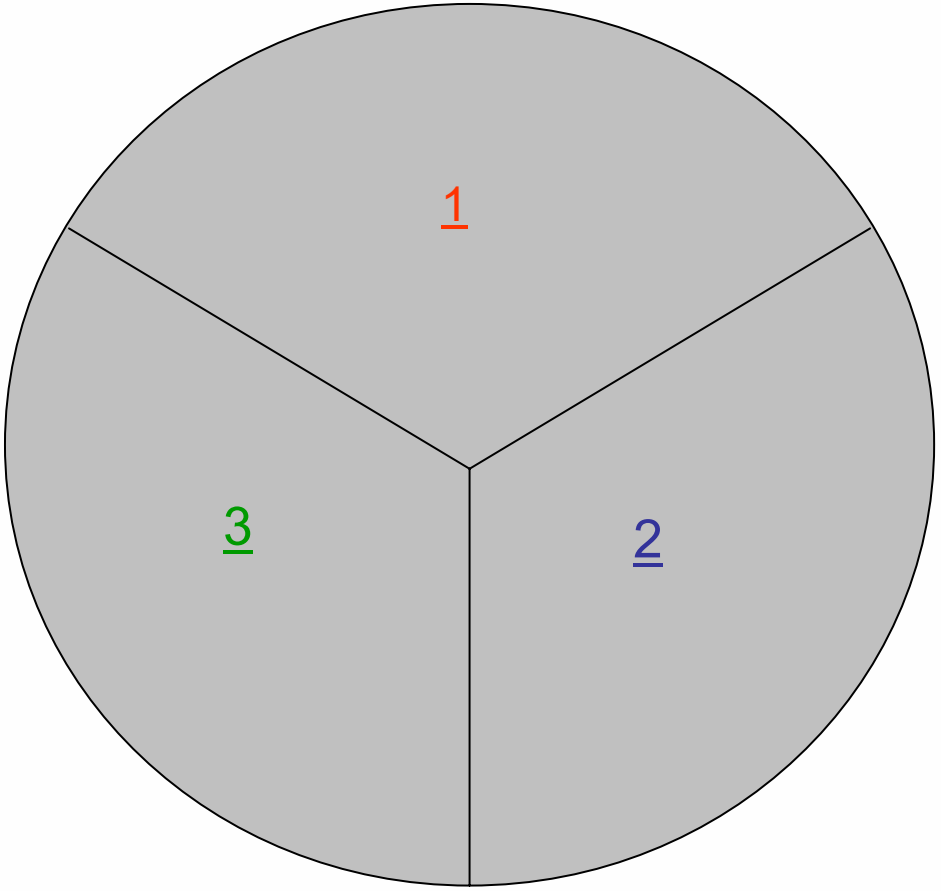
Tracking/Location Information

- Cell site, sector and approximate distance is available for recently completed calls and text messages
- Cell site and sector information is available for completed calls for a rolling 365 days.
- 9-1-1 calls are Phase II compliant but output delivered is dependent on the answering point's equipment
- Cannot obtain information in a timely manner for a call in progress if the mobile number is unknown

Cell Site Sectors

Cell sites can vary in the number of sectors they contain:
-Omni directional (no sectors)
-3 sector
-2 sector
-6 sector

VZW towers are mostly **3 sector**
and **omni directional towers.**
Each sector has a designation associated with it:
1= Alpha =X
2= Beta =Y
3= Gamma =Z



Sample Call Detail w/ Cell Sites

Switch	Date	Time	Orig C/G	Term C/G	Dir	MDN	Called #	ESN	CPN	Szr
Plymouth_Meeting2	7/13/2006	11:10:32	0	640	MF	6103607662	6103607662	2a0ab6c3	6103607662	43
Branchburg1	7/13/2006	11:10:26	292	1900	MO	6103607662	*86	2a0ab6c3	6103607662	44
Branchburg1	7/13/2006	11:00:45	250	292	MT	6103607662	6103607662	2a0ab6c3	6103609438	24
Plymouth_Meeting2	7/13/2006	11:00:45	0	640	MF	6103607662	6103607662	2a0ab6c3	6103609438	71
Branchburg1	7/12/2006	16:07:42	126	1901	MO	6103607662	6103609438	2a0ab6c3	6103607662	4665
Branchburg1	7/11/2006	18:09:39	250	292	MT	6103607662	6103607662	2a0ab6c3	6103609438	3347
Branchburg1	7/11/2006	15:31:31	294	689	MO	6103607662	9083067788	2a0ab6c3	6103607662	98
Branchburg1	7/11/2006	15:31:04	294	603	MO	6103607662	9083097788	2a0ab6c3	6103607662	2
Branchburg1	7/11/2006	15:30:27	294	603	MO	6103607662	9083097788	2a0ab6c3	6103607662	24
Branchburg1	7/11/2006	15:30:11	294	602	MO	6103607662	9085913523	2a0ab6c3	6103607662	5
Branchburg1	7/11/2006	10:03:15	250	292	MT	6103607662	6103607662	2a0ab6c3	9088126899	1538
Branchburg1	7/11/2006	9:27:30	250	292	MT	6103607662	6103607662	2a0ab6c3	9083067496	15

Description of Call Detail

- Switch: The switch the call is hitting
- Date: The date of the call
- Time: The time of the start of the call (based on the switch)
- Orig C/G: Valid cell site for outgoing calls (**Only for MO calls**)
- Term C/G: Valid cell site for incoming calls (**Only for MT calls**)
- Dir:
  - MO=Outgoing
  - MT=Incoming
  - MF=Incoming to voicemail and in rare cases, mobile forwarding
- MDN: Your target number
- Called #: If outgoing, this is the number your target dialed
- ESN: Electronic Serial Number of your target
- CPN: If incoming, this is the number that called your target
- Szr: Duration of the call in seconds

Sample RTT

Date *	Access Time	Call End Time *	Call Length (sec)	ESN	Subscriber #	Entry Type *	Init Cell	Init Sector	Access Dist (mi)	Last Cell	Last Sector
4-Apr	53:50.3	54:55.7	65.4	1438dac0	9084488669	Term	168	3	1.1	106	1
2-Apr	27:54.2	29:11.8	77.6	1438dac0	9084488669	Orig	292	2	0	292	2
1-Apr	25:42.5	26:44.8	62.4	1438dac0	9084488669	Orig	293	1	0.3	293	2
1-Apr	24:52.7	25:18.5	25.9	1438dac0	9084488669	Term	293	1	0.8	293	1
31-Mar	38:13.6	38:39.4	25.8	1438dac0	9084488669	Term	138	1	0.6	138	1
31-Mar	02:06.8	03:05.8	59	1438dac0	9084488669	Orig	14	1	0.8	14	1
31-Mar	20:24.7	20:31.6	7	1438dac0	9084488669	Orig	3	1	1.9	3	1
31-Mar	52:35.5	01:35.4	539.9	1438dac0	9084488669	Orig	138	1	0.6	138	1
30-Mar	34:29.7	51:44.8	1035.1	1438dac0	9084488669	Orig	138	1	0.6	138	1
30-Mar	34:13.1	34:13.1	0	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	32:49.6	33:55.8	66.2	1438dac0	9084488669	Term	0	0	0	0	0
30-Mar	33:55.7	33:55.7	0	1438dac0	9084488669	Term	138	1	0	138	1
30-Mar	32:46.8	33:54.0	67.2	1438dac0	9084488669	Orig	138	1	0.4	138	1
30-Mar	29:45.4	32:34.0	168.6	1438dac0	9084488669	Orig	138	1	0.6	138	1
30-Mar	29:57.0	29:57.0	0	1438dac0	9084488669	Term	138	1	0	138	1
30-Mar	28:40.1	29:06.1	26	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	19:22.2	19:48.1	25.9	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	12:07.4	12:33.4	26	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	58:07.3	59:58.1	110.8	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	55:59.3	57:37.1	97.8	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	45:29.6	55:34.0	604.4	1438dac0	9084488669	Term	138	1	0.6	138	1
30-Mar	00:45.2	14:46.0	840.8	1438dac0	9084488669	Orig	138	1	0.4	138	1
30-Mar	26:05.8	37:39.4	693.6	1438dac0	9084488669	Orig	138	1	0.6	138	1
30-Mar	25:02.6	25:42.9	40.3	1438dac0	9084488669	Orig	138	1	0.6	138	1
30-Mar	43:02.2	55:28.4	746.2	1438dac0	9084488669	Term	138	1	0.4	138	1
30-Mar	41:35.3	42:44.2	69	1438dac0	9084488669	Term	138	1	0.4	138	1
30-Mar	14:52.4	20:28.5	336.2	1438dac0	9084488669	Orig	272	3	3.2	272	3
30-Mar	14:52.4	14:52.4	0	1438dac0	9084488669	Term	0	0	3.2	0	0
30-Mar	14:20.4	14:48.3	27.9	1438dac0	9084488669	Term	0	0	0	0	0

Sample Text Message Detail

MDN	MSG_SND_DT_TM	MSG_DLVR_DT_TM	ORIG_ADDR	DEST_ADDR
6103607662	5/15/2006 7:25	5/15/2006 7:25	1111	6103607662
6103607662	5/16/2006 8:27	5/16/2006 8:27	1111	6103607662
6103607662	5/16/2006 7:15	5/16/2006 7:15	1111	6103607662
6103607662	5/31/2006 16:00	5/31/2006 16:01	1111	6103607662
6103607662	6/4/2006 9:56	6/4/2006 9:56	endofitem@ebay.com	6103607662
6103607662	6/8/2006 6:56	6/8/2006 6:56	1111	6103607662
6103607662	6/12/2006 14:40	6/12/2006 14:42	6103609438	6103607662
6103607662	6/13/2006 8:12	6/13/2006 8:12	1111	6103607662
6103607662	6/13/2006 17:20	6/13/2006 17:20	6103607662	6103609438
6103607662	6/13/2006 17:49	6/13/2006 17:49	6103607662	6103609438
6103607662	6/13/2006 20:21	6/13/2006 20:21	endofitem@ebay.com	6103607662
6103607662	6/13/2006 7:52	6/13/2006 7:52	1111	6103607662
6103607662	6/13/2006 7:52	6/13/2006 7:52	1111	6103607662

Sample CSG Report

Destination IP Addresses Captured During an Internet Session

Mobile IP Address	Conn Start Date/Time	Duration	Dest IP Address	Ip Stats Upload Cnt	Ip Stats Download Cnt
75.207.161.57	7/2/2008 2:14	0	209.170.115.104	88	48
75.207.161.57	7/2/2008 2:14	0	64.236.115.12	1496	3033
75.207.161.57	7/2/2008 2:14	0	209.62.176.115	88	48
75.207.161.57	7/2/2008 2:14	4	206.46.230.134	1008	4246
75.207.161.57	7/2/2008 2:14	300	69.78.96.14	71	236
75.207.161.57	7/2/2008 2:14	2	209.62.182.190	716	887
75.207.161.57	7/2/2008 2:14	4	209.170.115.104	1420	15312
75.207.161.57	7/2/2008 2:14	4	209.170.115.104	1400	13275
75.207.161.57	7/2/2008 2:14	4	206.46.230.134	1860	9263
75.207.161.57	7/2/2008 2:14	1	206.46.230.68	1581	413
75.207.161.57	7/2/2008 2:14	12	206.46.232.39	12867	56132
75.207.161.57	7/2/2008 2:14	1	206.46.232.39	3156	5208

Sample AAA Report

Session Information for Internet Usage

ELEMENT	CALL_START	EVNT_STOP	MBL_IP_ADDR	SID	MSCID	CELL	MDN	GMT_START
AAA04ROCA	6/30/2008 7:44	6/30/2008 8:21	75.204.165.228	80	2	300	9089309080	6/30/2008 11:44
AAA04ROCA	6/30/2008 15:20	6/30/2008 16:00	75.205.207.121	80	2	300	9089309080	6/30/2008 19:20
AAA04ROCA	6/30/2008 21:57	6/30/2008 22:46	75.205.241.1	80	2	300	9089309080	7/1/2008 1:57
AAA04ROCA	7/1/2008 21:15	7/1/2008 22:15	75.207.161.57	80	2	300	9089309080	7/2/2008 1:15

- **Target assigned dynamic IP address for each session**
- **Cell Site Locations available for session's start**

Third Party Records

- BIG QUESTIONS!
- Content of stored communication rather than subscriber or billing records
- i.e. – Your Emails and Texts
- Not just the date and time of transmission.
- *U.S. v. Miller,* 425 U.S. 436 (1976) says no expectation of privacy in Third Party Records
  - i.e.: Bank Records, etc.

Millions of Subpoena Requests by Law Enforcement

- State and Federal law enforcement are making millions of requests on cell phone providers for records

U.S. v. Pineda-Moreno

- In a companion case to *Jones*
  - 9th Circuit Chief Judge *Kozinski* dissented to the denial of rehearain en banc: "1984 may have come a bit later than predicted, but it's here at last."
- "If you have a cell phone in your pocket, then the government can watch you. At the government's request, the phone company will send out a signal to any cell phone connected to its network, and give the police its location. Last year, law enforcement agents pinged users of just one service provider-Sprint-over eight million times. The volume requests grew so large that the 110-member electronic surveillance team couldn't keep up, so Sprint automated the process by developing a web interface that gives agents direct access to users' location data."

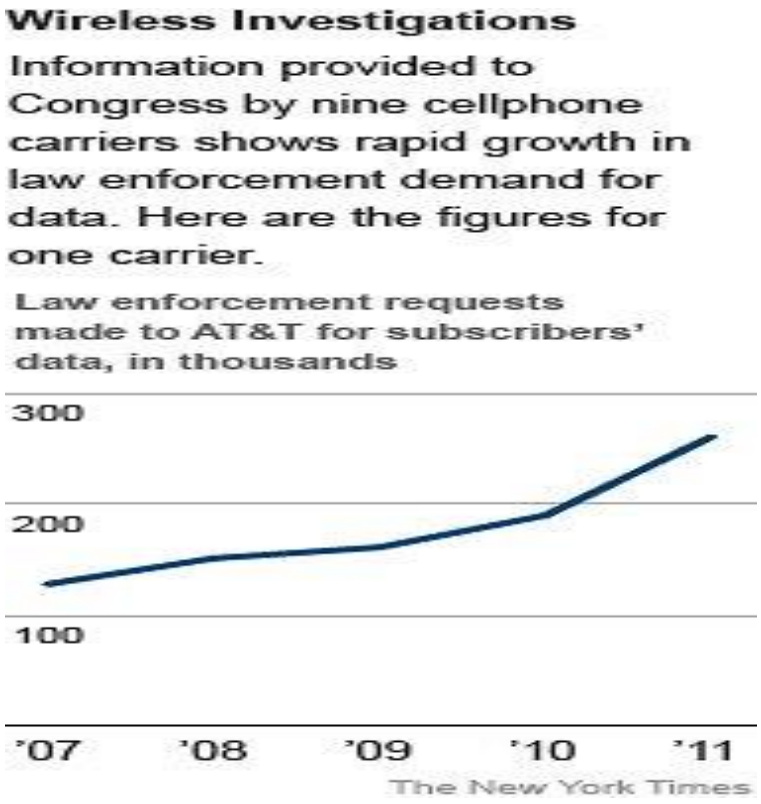
More Demands on Cell Carriers in Surveillance

NYTimes.com – Eric Lictblau – July 8, 2012

In the first public accounting of its kind, cellphone carriers reported that they responded to a startling **1.3 million demands for subscriber information** last year from law enforcement agencies seeking **text messages, caller locations and other information in the course of investigations.**

CONGRESS GETS INVOLVED

The cellphone carriers' reports, which come in response to a Congressional inquiry, document an explosion in cellphone surveillance in the last five years, with the companies turning over records thousands of times a day in response to **police emergencies, court orders, law enforcement subpoenas and other requests.**



ALL LEVELS OF LAW ENFORCEMENT

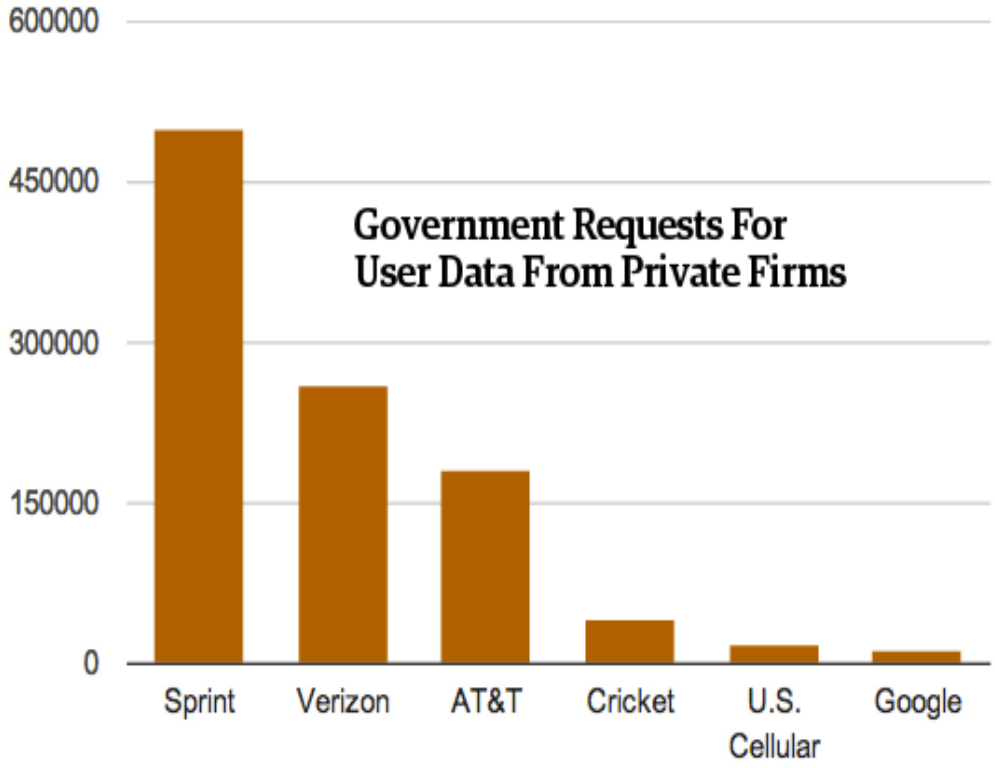
While the cell companies did not break down the types of law enforcement agencies collecting the data, they made clear that the **widened cell surveillance cut across all levels of government — from run-of-the-mill street crimes handled by local police departments to financial crimes and intelligence investigations at the state and federal levels**.

Here's How Often AT&T, Sprint, And Verizon Each Hand Over Users' Data To The Government

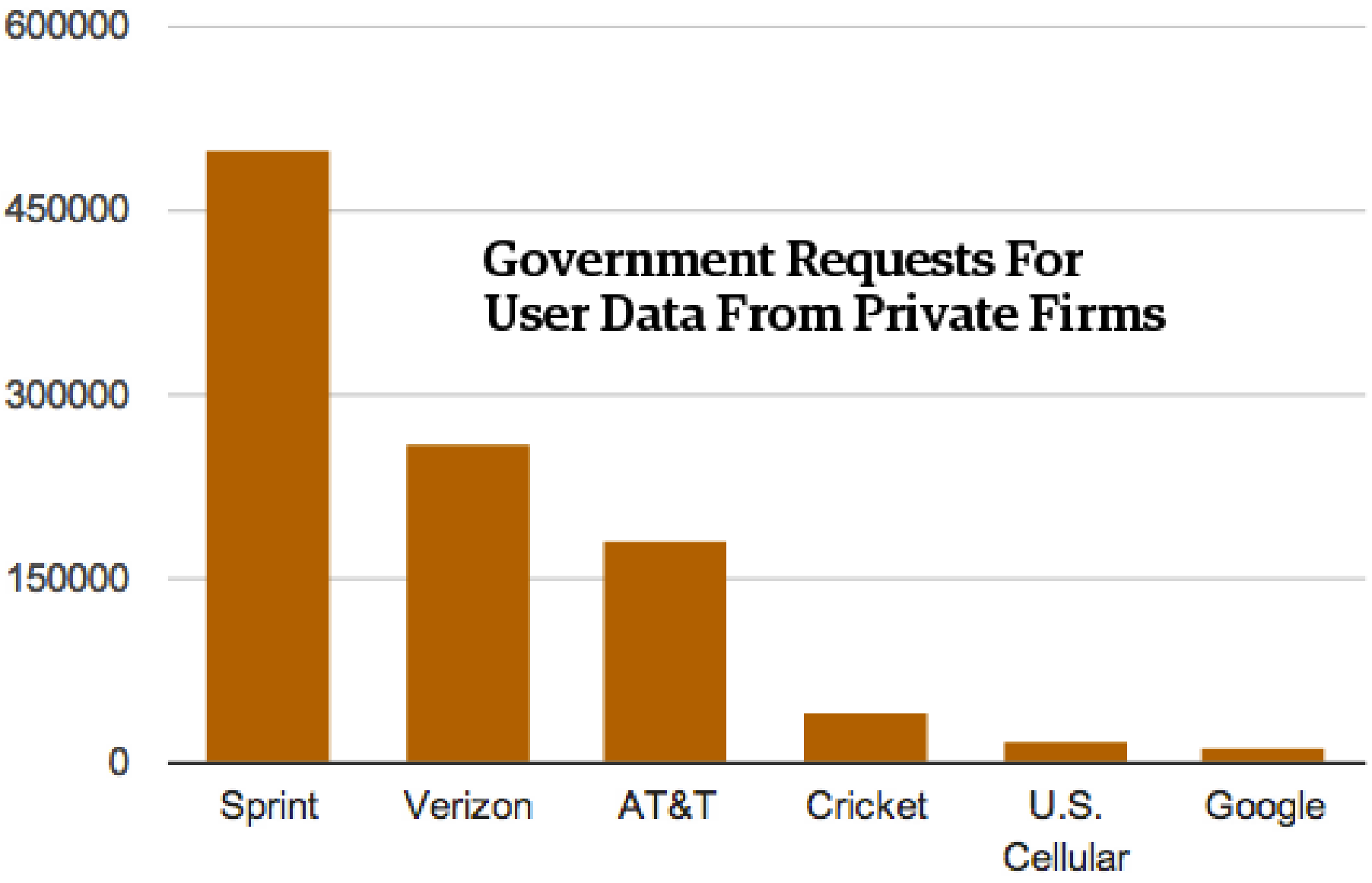
Forbes.com – By: Andy Greenburg – July 7, 2012

The vast majority of law enforcement's demands that phone carriers and Internet services hand over users' private data **don't require a warrant, and occur with little or no accountability**. It's not just that we don't know how much surveillance takes place.

To paraphrase Donald Rumsfeld, we don't even know *what we don't know* about how much the government knows about us.



It's important to remember that the information revealed Monday includes **"tower dumps,"** too, says Chris Calebrese, an attorney with the ACLU. "Just the sheer volume of orders is amazing, but a significant chunk are dumps from entire cell towers," he says. **"That means tons of people's information is being grabbed with a single one of these orders."**


600000
450000
300000
150000
0
Government Requests For
User Data From Private Firms
Sprint
Verizon
AT&T
Cricket
U.S. Cellular
Google

Retention Periods of Major Cellular Service Providers

Data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice

	Verizon	T-Mobile	AT&T/Cingular	Sprint	Nextel	Virgin Mobile[1]
Subscriber Information	Post-paid: 3-5 years*	5 years	Depends on length of service	Unlimited	Unlimited	Unlimited
Call detail records	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Pre-paid: varies Post-paid: 5-7 years	18-24 months	18-24 months	2 years
Cell towers used by phone	1 rolling year	Officially 4-6 months, really a year or more.	From July 2008	18-24 months	18-24 months	Not retained - obtain through Sprint
Text message detail	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Post paid: 5-7 years	18 months (depends on device)	18 months (depends on device)	60-90 days
Text message content	3-5 days	Not retained	Not retained	Not retained	Not retained	90 days (search warrant required with "text of text" request)
Pictures	Only if uploaded to website (customer can add or delete pictures any time)	Can be stored online and are retained until deleted or service is canceled	Not retained	Contact provider	Contact provider	Not retained
IP session information	1 rolling year	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
IP destination information	90 days	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
Bill copies (post-paid only)	3-5 years, but only last 12 months readily available	Not retained	5-7 years	7 years	7 years	n/a‡
Payment history (post-paid only)	3-5 years, check copies for 6 months*	5 years	Depends on length of service	Unlimited	Unlimited	n/a‡
Store Surveillance Videos	Typically 30 days	2 weeks	Depends. Most stores carry for 1-2 months	Depends	Depends	n/a
Service Applications	Post-paid: 3-5 years*	Not retained	Not retained	Depends	Depends	Not retained

* May vary by former company

** For records older than mid-Nov. 2007, Sprint can only provide bill reprints with outgoing info

‡ No bill copies, but list of credit card transactions does not expire

[1] Virgin Mobile is now owned by Sprint. Since companies have separate compliance offices, for now they are listed separately.

Law Enforcement Use Only

Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps

Forbes.com – By: Andy Greenburg – April 3, 2012

Wiretaps

T-Mobile charges law enforcement a flat fee of $500 per target.

Sprint's wireless carrier Sprint Nextel requires police pay $400 per "market area" and per "technology" as well as a $10 per day fee, capped at $2,000.

AT&T charges a $325 activation fee, plus $5 per day for data and $10 for audio.

Verizon charges a $50 administrative fee plus $700 per month, per target.

Voicemail & Text Messages

AT&T demands $150 for access to a target's voicemail

Verizon charges $50 for access to text messages.

Sprint asks $120 for pictures or video, $60 for email, $60 for voice mail and $30 for text messages.

Cell Tower Dumps

AT&T charges $75 per tower per hour, with a minimum of two hours.

Verizon charges between $30 and $60 per hour for each cell tower.

T-Mobile demands $150 per cell tower per hour.

Sprint charges $50 per tower, seemingly without an hourly rate.

Real Time Location Data

Sprint charges $30 per month per target to use its L-Site program for location tracking.

AT&T's E911 tool costs $100 to activate and then $25 a day.

T-Mobile charges a much pricier $100 per day.

Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps

Forbes.com – By: Andy Greenburg – April 3, 2012

Wiretaps

T-Mobile charges law enforcement a flat fee of $500 per target.

Sprint's wireless carrier Sprint Nextel requires police pay $400 per "market area" and per "technology" as well as a $10 per day fee, capped at $2,000.

AT&T charges a $325 activation fee, plus $5 per day for data and $10 for audio.

Verizon charges a $50 administrative fee plus $700 per month, per target.

Voicemail & Text Messages

AT&T demands $150 for access to a target's voicemail

Verizon charges $50 for access to text messages.

Sprint asks $120 for pictures or video, $60 for email, $60 for voice mail and $30 for text messages.

Cell Tower Dumps

AT&T charges $75 per tower per hour, with a minimum of two hours.

Verizon charges between $30 and $60 per hour for each cell tower.

T-Mobile demands $150 per cell tower per hour.

Sprint charges $50 per tower, seemingly without an hourly rate.

Real Time Location Data

Sprint charges $30 per month per target to use its L-Site program for location tracking.

AT&T's E911 tool costs $100 to activate and then $25 a day.

T-Mobile charges a much pricier $100 per day.


TROOPERS IN MICHIGAN ARE DOWNLOADING DATA FROM DRIVERS' CELL PHONES DURING ROUTINE TRAFFIC STOPS
REMEMBER WHEN IT READ "STATE POLICE"?
POLICE
STATE
MIKETHOMPSON© DETROIT FREE PRESS

Example of Cellebrite use

cellebrite
delivering mobile expertise

UFED TOUCH ULTIMATE

All-inclusive Mobile Forensic Solution

UFED series

UFED TOUCH ULTIMATE

All-inclusive Mobile Forensic Solution

Cellebrite's UFED Touch Ultimate is a high performance mobile forensic solution. With its intuitive GUI and easy-to-use touch screen, the UFED Touch Ultimate enables the physical, logical and file system extraction of all data and passwords (even if they've been deleted) from the widest range of popular mobile phones, portable GPS devices and tablets.

The UFED Touch Ultimate includes:

- **UFED Physical Analyzer**: A powerful mobile forensic application enabling advanced decoding, analysis and reporting
- **UFED Phone Detective**: For instant mobile phone identification
- **UFED Reader**: Enables sharing of information with any authorized personnel

The UFED Touch Ultimate is a mission-ready solution for investigations in the field or lab and available in both standard and ruggedized versions.

The UFED Touch Ultimate Advantage

Setting the industry standard for mobile data forensic solutions, the UFED Touch Ultimate provides investigators with maximum capabilities:

- Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth, etc.
- Widest support for Apple devices running iOS3+
- Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including HTC, Motorola, Samsung Galaxy SIII family and more
- Physical extraction from Nokia BB5 devices – password extraction from selected devices
- File system extraction from any device running Windows phone 7.5 and 8 including Nokia, HTC, Samsung, Huawei and ZTE
- The most powerful solution for phones with Chinese chipsets
- TomTom® trip-log decryption, and data extraction from other portable GPS devices
- Obtain existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes etc.
- Proprietary technology and boot loaders ensure forensically sound extractions
- Frequent updates to ensure compatibility with new phones as they enter the market

Mission-Ready

The all-inclusive standard and ruggedized mobile forensic kits contain a full range of peripherals and accessories for successful investigations in the field or lab. Complete with lightweight phone connector tips, an embedded work shelf in the ruggedized case, integrated long-life battery and external hard drive makes mobile investigations quicker, easier and more efficient.

RUGGEDIZED KIT

STANDARD KIT

UFED Physical Analyzer

The UFED Physical Analyzer is the most powerful and technologically advanced mobile forensic application available. It exposes every segment of a device's memory data and provides in-depth decoding, analysis and reporting methods. Features include:

- **Malware Detection** – On-demand searches for viruses, spyware, Trojans and other malicious payloads in files
- **Project Analytics** – View statistics on communications and identifying relationship strengths
- **Rich Set of Data** – Includes calendar, call logs, contacts, SMS, MMS, chats, applications
- **Advanced Search** – Based either on open text or specific parameters
- **Timeline** – Monitor events in a single chronological view
- **Watch List** – Ability to highlight information based on predefined list of values
- **Image Carving** – Powerful feature used to recover deleted image files and fragments when only remnants are available
- **Conversation View** – View communications between sources in date and time order
- **Report Generator** – Generate and customize reports in different formats e. g. PDF, HTML, XML and Excel
- **SQLite Databases Viewer** – Viewing, searching and exporting tables and content (including deleted data) from SQLite database files
- **Hex Viewer** – Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more
- **Highlighted Parsed Content in the Hex** – Highlights the exact position for each decoded content entry, enabling full tractability between the analyzed data and the Hex
- **Python Scripting** – Using the Python shell, enhances the capabilities for content decoding
- **Plugin and Chain Management** – Run Python scripts via plugins; edit and create new decoding chains

The UFED Phone Detective

The UFED Phone Detective appliaction comes with the UFED Touch kit, helping investigators identify a mobile phone at the start of an investigation. This eliminates the need to open the phone, risking phone lock. To identify a phone, users answer questions about the phone's attributes. UFED Phone Detective provides details on extraction capabilities, connectivity, device characteristics and more.

UFED Reader

UFED Reader allows authorized personnel to share examination results with others, regardless of whether they own UFED software. Simply forward the application and the extraction report to users for viewing and searching within the extracted data.

UFED CHINEX

Available as an add-on to the UFED Touch Ultimate is UFED CHINEX; the premium, field-ready solution for the extraction of evidentiary data from phones manufactured with Chinese chipsets. The kit contains:

- Enhanced phone adapter
- Adapter cables
- A large selection of individual connectors
- USB cable
- Quick user guide

Applications: UFED Physical Analyzer – UFED Reader – UFED Phone Detective

Hardware: UFED Touch Device – UFED Solid Protective Case – Tips & Cables Set – Tips & Cables Organizer – UFED Power Supply – Standard Carrying Case – Ruggedized Carrying Case* – Case Embedded Work Surface* – UFED Touch Screen Cover* – UFED External Hard Drive* – SIM ID Cloning Cards X3 – SIM ID Cloning Cards X5* – Micro SIM ID Cloning Cards X3 – Micro SIM ID Cloning Cards X5* – Micro SIM Adapter – Car Power Adaptor – UFED To PC Cable – Phone Power Up Cable – USB Flash Drive (8 GB) – DC 5v To 6v Adapter – Cleaning Brush For Phone Connectors – UFED Phone Charger* – UFED Forensic Memory Card Reader* – Faraday Bag* – User Manual

* Available in ruggedized version only

About Cellebrite

Founded in 1999, Cellebrite is a global company known for its technological breakthroughs in the cellular industry. A world leader and authority in mobile data technology, Cellebrite established its mobile forensics division in 2007, with the Universal Forensic Extraction Device (UFED). Cellebrite's range of mobile forensic products, UFED Series, enable the bit-for-bit extraction and in-depth analysis of data from thousands of mobile devices, including feature phones, smartphones, portable GPS devices, tablets and phones manufactured with Chinese chipsets.
Cellebrite's UFED Series is the prime choice of forensic specialists in law enforcement, military, intelligence, corporate security and eDiscovery agencies in more than 60 countries.

Cellebrite is a wholly-owned subsidiary of the Sun Corporation, a listed Japanese company (6736/JQ)

www.ufedseries.com
sales@cellebrite.com

HEADQUARTERS
Cellebrite Ltd.
94 Em Hamoshavot St.
Petah Tikva 49130
Israel
Tel: +972 3 926 0900
Fax: +972 3 924 7104

USA
Cellebrite USA Inc.
266 Harristown Rd., Suite 105
Glen Rock, NJ 07452
USA
Tel: +1 201 848 8552
Fax: +1 201 848 9982

GERMANY
Cellebrite GmbH
Am Hoppenhof 32a
33104 Paderborn
Germany
Tel: +49 52 51 54 64 90
Fax: +49 52 51 54 64 9 49

cellebrite
delivering mobile expertise

TOUCH ULTIMATE

inclusive Mobile
rensic Solution

UFED Touch Ultimate is a high
e mobile forensic solution. With its
I and easy-to-use touch screen, the
h Ultimate enables the physical,
file system extraction of all data and

The UFED Touch Ultimate Advantage

Setting the industry standard for mobile data forensic solutions, the UFED Touch Ultimate provides investigators with maximum capabilities:

- Physical extraction from BlackBerry® devices running OS 4-7. Exclusive decoding: BBM data, apps, emails, Bluetooth, etc.
- Widest support for Apple devices running iOS3+
- Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including HTC, Motorola, Samsung Galaxy SIII family and more
- Physical extraction from Nokia BB5 devices – password extraction from selected devices
- File system extraction from any device running Windows phone 7.5 and 8 including Nokia, HTC, Samsung, Huawei and ZTE
- The most powerful solution for phones with Chinese chipsets
- TomTom® trip-log decryption, and data extraction from other portable GPS devices
- Obtain existing and deleted data: apps, passwords, emails, call history, SMS, contacts, calendar, media files, geotags, location information, GPS fixes etc.
- Proprietary technology and boot loaders ensure forensically sound extractions
- Frequent updates to ensure compatibility with new phones as they enter the market

Government Software Surveillance Programs

- PRIZM
- Carnivore
- Echelon

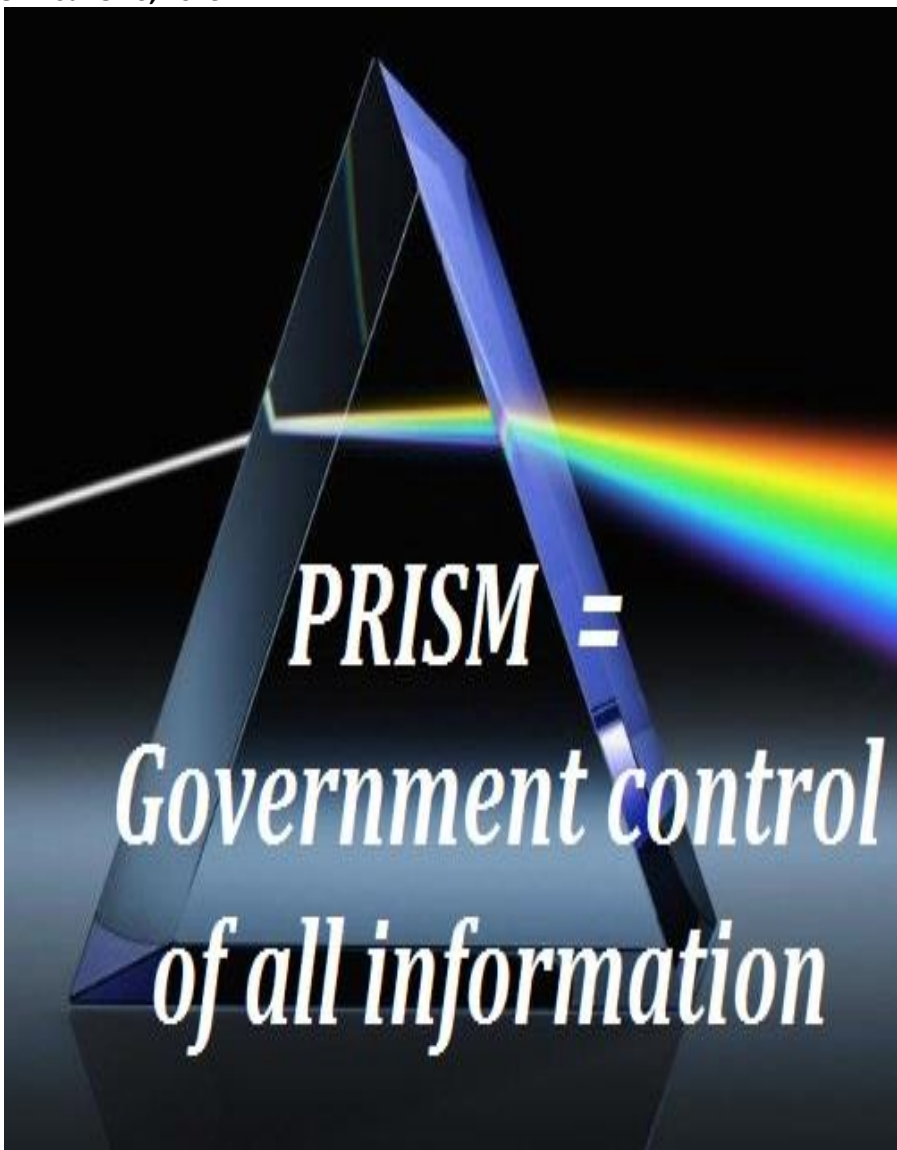
What's in the Rest of the Top-Secret NSA PowerPoint Deck?

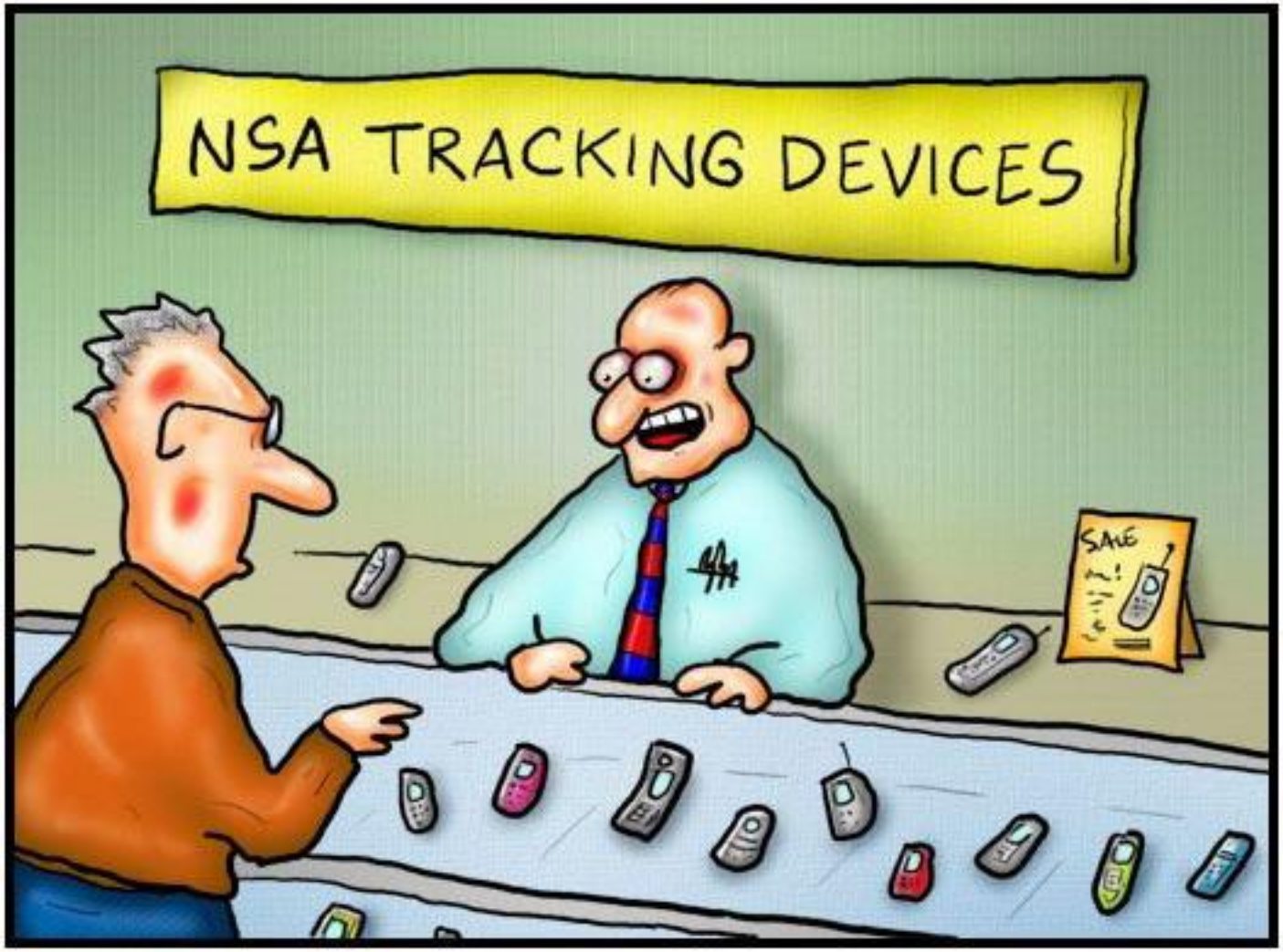
Wired.com – By: Kevin Poulsen – June 10, 2013

Now that Snowden has revealed himself to the world as the NSA whistleblower, details about his interaction with the press are surfacing. And at the center of the drama is a still mostly unpublished 41-slide presentation, classified top secret, that Snowden gave to the *Washington Post* and the *Guardian* to expose the NSA's internet spying operation "PRISM."

Only five slides from the presentation have been published. The other 36 remain a mystery

Both the *Guardian*'s Glenn Greenwald and the *Post*'s Barton Gellman have made it clear that the rest of the PowerPoint is dynamite stuff … which we're not going to be seeing any time soon. "If you saw all the slides you wouldn't publish them," wrote Gellman on Twitter, adding in a second tweet: "I know a few absolutists, but most people would want to defer judgment if they didn't know the full contents."





"Yeah - we used to call them cell phones."

TOP SECRET NSA PRISM POWERPOINT

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted]

April 2013

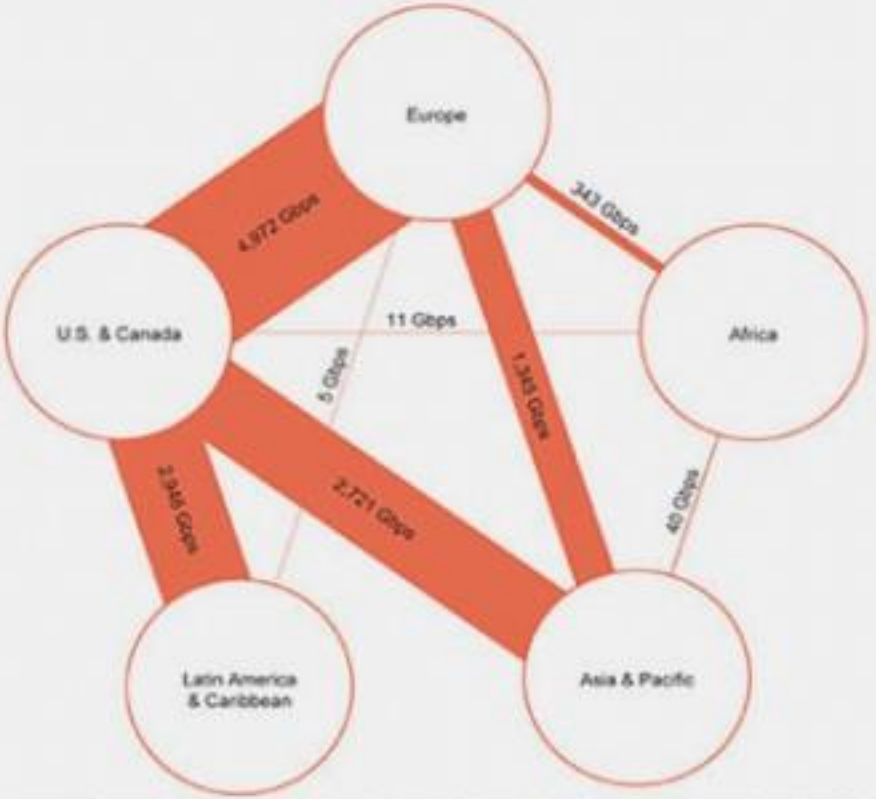
Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

(TS//SI//NF) PRISM Collection Details

Current Providers

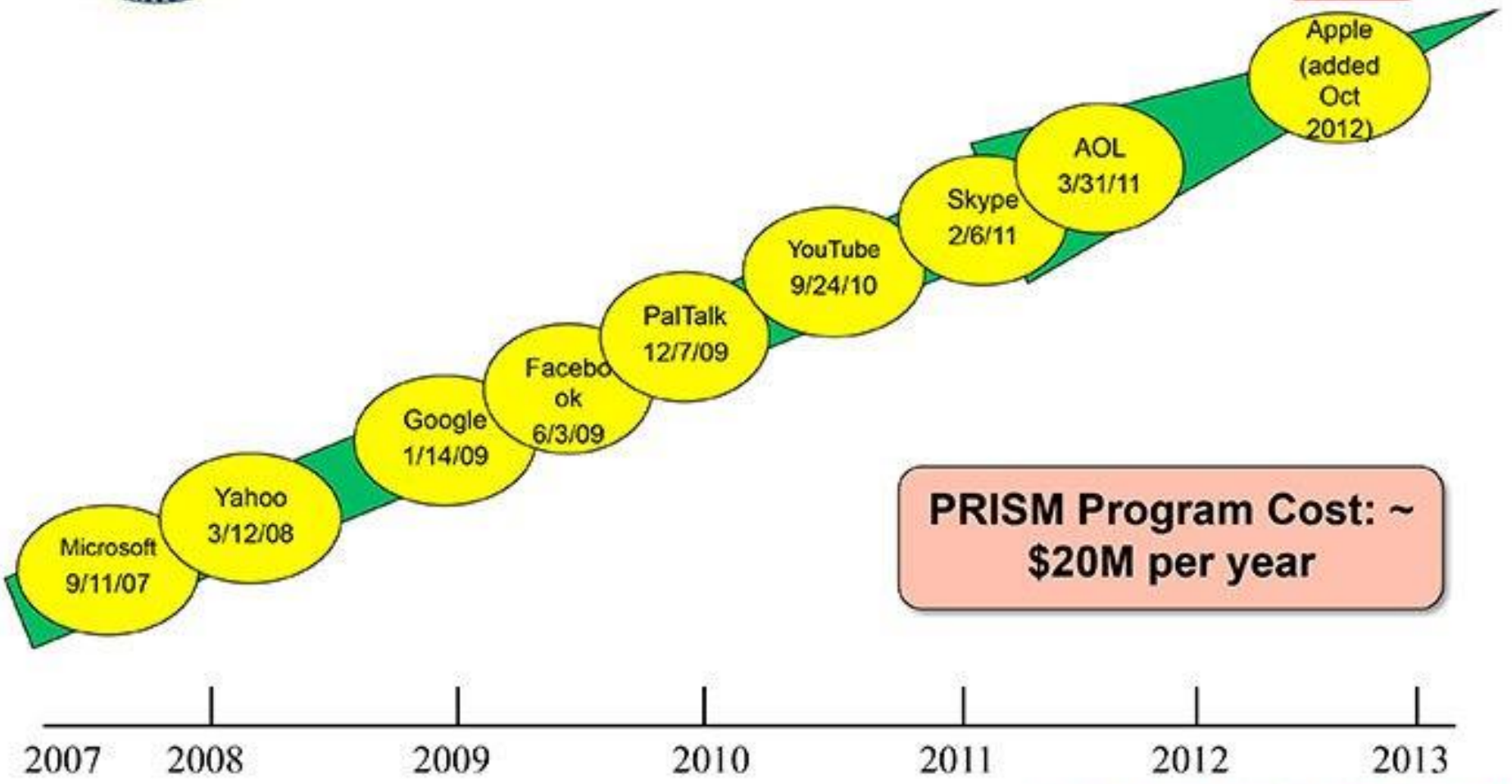
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, [redacted] BLARNEY, [redacted])

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)

By: James Bamford – March 15, 2012

Wired.com

Under construction by contractors with top-secret clearances, the blandly named **Utah Data Center** is being built for the National Security Agency. A project of immense secrecy, it is the final piece in a complex puzzle assembled over the past decade.

ITS PURPOSE:

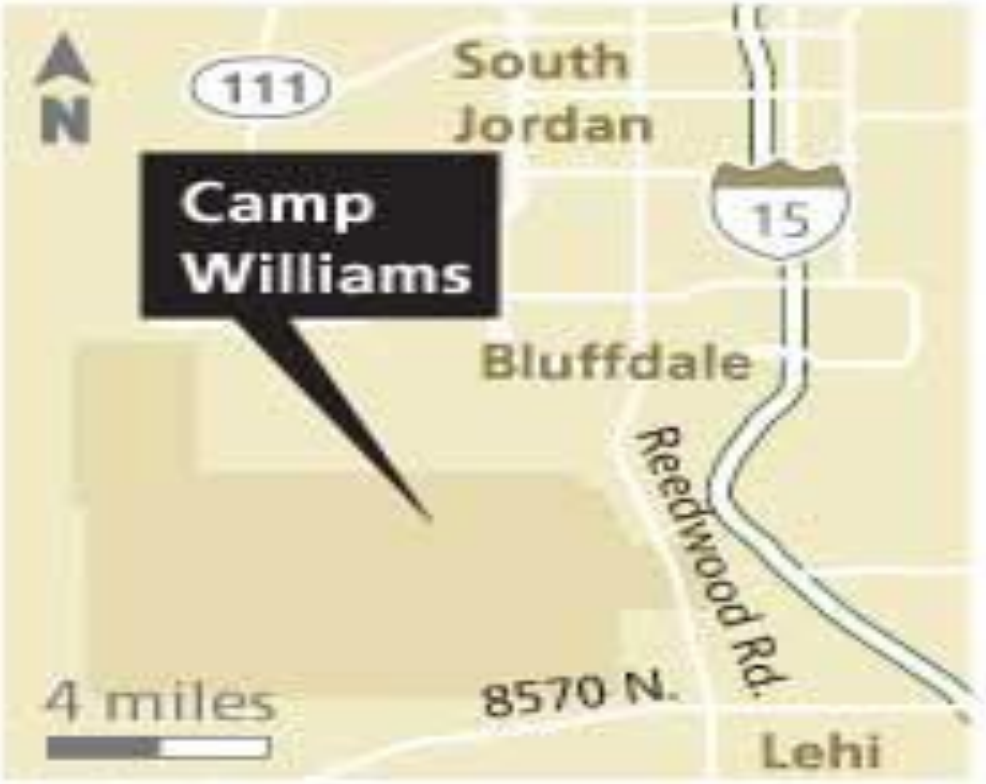
To intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks. The heavily fortified $2 billion center should be up and running in **September 2013.**

WHAT THEY ARE STORING:

Flowing through its servers and routers and stored in near-bottomless databases will be **all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter.**" It is, in some measure, the realization of the "total information awareness" program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after **it caused an outcry over its potential for invading Americans' privacy.**

Utah spy plant at Camp Williams

The National Security Agency is planning to build a 1 million-square-foot data center on a 200-acre site at Utah's Camp Williams.



The Salt Lake Tribune

The "StingRay" Cell Phone Spying Device

Global Research – By: Clarence Walker – April 13, 2013

Originally intended for terrorism investigations, the feds and local law enforcement agencies are now using the James Bond-type surveillance to track cell phones in drug war cases across the nation without a warrant. Federal officials say that is fine — responding to a Freedom of Information Act (FOIA) request filed by the Electronic Freedom Foundation (EFF) and the First Amendment Coalition, the Justice Department argued that **no warrant was needed to use StingRay technology.**

"If a device is not capturing the contents of a particular dialogue call, the device does not require a warrant, but only a **court order under the Pen Register Statute** showing the material obtained is relevant to an ongoing investigation," the department wrote.

Federal Prosecutors try to "Fool" Judges

The StingRay technology is so new and so powerful that it not only raises Fourth Amendment concerns, it also **raises questions about whether police and federal agents are withholding information about it from judges to win approval to monitor suspects without meeting the probable cause standard required by the Fourth.** At least one federal judge thinks they are. Magistrate Judge Brian Owsley of the Southern District of Texas in Corpus Christi told the Yale conference federal prosecutors are using clever techniques to fool judges into allowing use of StingRay. **They will draft surveillance requests to appear as Pen Register applications, which don't need to meet the probable cause standards.**

"After receiving a second StingRay request," Owsley told the panel, "I emailed every magistrate judge in the country telling them about the device. And **hardly anyone understood them."**

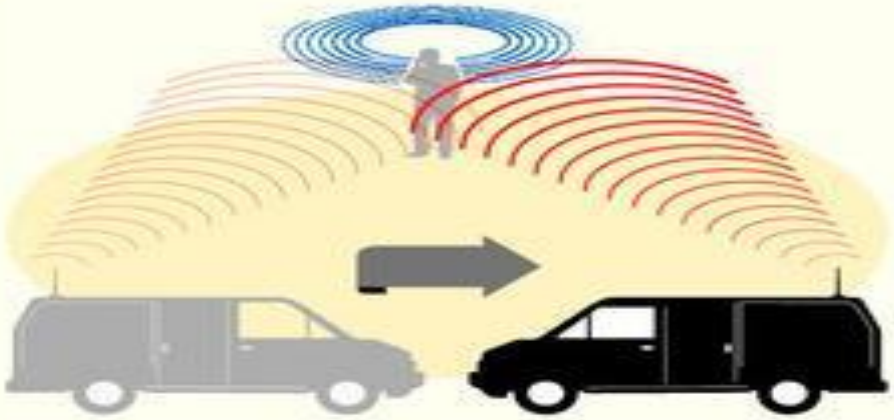
How a 'Stingray' Cellphone Tracking Device Works

Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.

1. Often the device is used in a vehicle along with a computer with mapping software.

2. The stingray system, which mimics a cellphone tower, gets the target phone to connect to it.

3. Once the cellphone is detected by the stingray, the phone's signal strength is measured.



4. The vehicle can then move to another location and again measure the phone's signal strength.

5. By collecting signal strength in several locations, the system can triangulate and map a phone's location.

Judges Questioned Use of Cellphone Tracking Devices

WSJ.com – By: Jennifer Valentino-DeVries – March 27, 2013

Feds Aren't Giving Judges the Whole Story

Judges in California, like a few others across the country, have raised concerns about federal use of cellphone tracking devices known as **"stingrays,"** suggesting that **investigators have been using the technology without explaining to judges exactly what they are doing.**

A handful of federal judges have now expressed concerns about similar cellphone tracking technologies, particularly because **federal officers have been using them after getting lower court orders that don't meet the same standard as search warrants.**

Stingray Use is Hidden Within Pen Register Applications

In California, emails written by several U.S. attorneys in 2011 indicate that this has become what they describe as a "problem" in that state as well. One of the emails explains that **magistrate judges there have "collective concerns" about whether the court orders, known as pen register orders, are "sufficient to authorize the use" of the technology.**

"It has recently come to my attention that **many agents are still using [stingray] technology in the field although the pen register application does not make that explicit,"** one of the attorneys wrote, adding that the office was working on a "long term fix."

Pen registers are tools that gather signals from phones such as numbers dialed but don't receive the content of conversations. **To use them, investigators don't have to show probable cause, the way they would with a search warrant.** But pen registers were designed before the widespread use of cellphones, which can transmit more data than landline phones and can be used to pinpoint a person's location. **The template that investigators use when writing pen register requests doesn't necessarily indicate when the device being used is actually a stingray**, the California emails suggest.

Emails Show Law Enforcement Officers Authorized to Use Pen Registers Also Use “Stingrays” w/o Authorization

Kenney, Patricia (USACAN)

From: Waldinger, Kyle (USACAN)
Sent: Monday, May 23, 2011 12:48 PM
To: Beausey, Karen (USAMA); USACAN-Attorneys-Narcotics
Subject: RE: IMPORTANT INFORMATION RE: PEN REGISTERS

And just to be super clear, the agents may not use the term "WIT" (or "WITT") but rather may be using the term "Triggerfish" or the term "Stingray," so please make sure that the agents know what you are referring to.

From: Beausey, Karen (USACAN)
Sent: Monday, May 23, 2011 12:17 PM
To: USACAN-Attorneys-Narcotics
Subject: FW: IMPORTANT INFORMATION RE: PEN REGISTERS
Importance: High

Hi everyone. Miranda asks 4 questions, but I think we need an answer to a 5th one as well: whether or not the initial intended purpose of the pen register was to use the WIT technology to locate someone, did the agents eventually use the pen in that way? In other words, a pen might have started out as just a pen, and later the agents decided to use the order to also attempt to locate the target. They may or may not have told you about this decision. So, check in with your agents and find out whether they have been using pen register orders to locate targets with the WIT boxes, whether or not they started out intending to do so.

Thanks.

Karen

From: Kane, Miranda (USACAN)
Sent: Monday, May 23, 2011 11:55 AM
To: USACAN-Attorneys-Criminal
Subject: IMPORTANT INFORMATION RE: PEN REGISTERS
Importance: High

Effective immediately all pen register applications and proposed orders must be reviewed by your line supervisor before they are submitted to a magistrate judge.

As some of you may be aware, our office has been working closely with the magistrate judges in an effort to address their collective concerns regarding whether a pen register is sufficient to authorize the use of law enforcement's WIT technology (a box that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with some specificity) to locate an individual. It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit.

While we continue work on a long term fix for this problem it is important that we are consistent and forthright in our pen register requests to the magistrates which is why I am

adding this additional review. I anticipate that I will be able to eliminate the line supervisor approval requirement once we have an opportunity to discuss the issue with the bench and revise the language in our common application. In the meantime, I appreciate your cooperation in this matter.

In addition, if you have requested a pen register in the last six months — since January 2011 - please provide the following information to your supervisor as soon as possible: 1) Was the pen register approved by a magistrate? 2) Which magistrate reviewed it? 3) Was the purpose of the pen register to locate a person? 4) Did the agency requesting the pen register use WIT technology? This information will be extremely valuable to me in my discussions with the magistrate judges.

Again, thank you in advance for your assistance. I will update everyone about the status of this issue at our Criminal Division Meeting on June 7, 2011.

Miranda

Carrier IQ

- Carrier IQ is a program for mobile devices that records every keystroke and every piece of data that comes in or out of your device.
- The data is sent back to Carrier IQ's servers.
- The program cannot be turned off and is very hard to track.
- It is believed to be used on HTC, Android and Blackberry phones. There is some evidence that it exists on Apple products as well.
- AT&T confirms that it uses the software while Verizon and Nokia deny that it exists on there phones.

Carrier IQ

- The rational is that the information collected will help the device manufacturers and software developers create better products and services for the consumer.
- Problem: Can the government access this information?
- We could see class-action litigation over these issues.
- *Source:* http://www.washingtonpost.com/business/technology/what-is-carrier-iq/2011/12/01/gIQApql1GO_story.html

APP- TRACKING

S.B. 1052

Sec. 5A. WARRANT ISSUED IN THIS STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS.

(a) This section applies to a warrant required under Section 4 to obtain electronic customer data, including the contents of a wire communication or electronic communication.

(b) On the filing of an application by an authorized peace officer, a district judge may issue a search warrant under this section for electronic customer data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage, by a provider of an electronic communications service or provider of a remote computing service described by Subsection (g), regardless of whether the customer data is held at a location in this state or at a location in another state. An application made under this subsection **must demonstrate probable cause for the issuance of the warrant and must be supported by the oath or affirmation of the authorized peace officer.**

(c) A search warrant **MAY NOT** be issued under this section unless the sworn affidavit required by Article 18.01(b) sets forth **sufficient and substantial facts to establish probable cause** that:

(1) a specific offense has been committed; and

(2) the electronic customer data sought:

(A) constitutes evidence of that offense or evidence that a particular person committed that offense; and

(B) is held in electronic storage by the service provider on which the warrant is served under Subsection (h).

(d) Only the electronic customer data described in the sworn affidavit required by Article 18.01(b) may be seized under the warrant.


HELLO, VERIZON?
I'M INTERESTED IN YOUR
SHARE EVERYTHING PLAN...