Surveillance today
Location Tracking, Face Recognition and Other Surveillance Techniques


Lee Tien, Senior Staff Attorney and Adams Chair for Internet Rights
Electronic Frontier Foundation, San Francisco, CA
Overview

• The technology—CSLI, Stingrays, Hemisphere, ALPR, face recognition & biometrics, government hacking (NITs), “Upstream” and Section 702

• What data are they capturing and what can be learned from it?

• What laws apply & how to challenge?
The Technology—Cell Site Location Info (Cell Towers), Stingrays, & Hemisphere
Cell Site Location Info
Cell Site Location Info

- 32 towers within 1 mile radius of here
- More towers = more detailed & accurate location info
Historical Cell Site Location Info—

*U.S. v. Graham* 12-4659 (4th Cir. 2012)

- 221 days of worth of Graham’s cell site records obtained without a warrant.
- Determined 29,659 location points
Historical Cell Site Location Info—
People of the State of N.Y. v. Moalawi (NY 2015)
Stingrays
Stingrays—How They Work

**HOW STINGRAY WORKS**
A Stingray is a mobile device that masquerades as a cellphone tower. It’s usually mounted in a police surveillance vehicle.

**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.

**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.

Stingrays—“A Rose by Any Other Name . . .”

• AKA:
  – IMSI catcher
  – Digital analyzer
  – Triggerfish
  – Kingfish
  – Amberjack
  – Hailstorm
  – “Confidential source”
  – WITT
  – Pen register
  – Mobile tracking device
  – Cell site simulator, emulator, or monitor

• Questions to ask:
  – How did govt figure out client’s number? Locate him/her?
  – Is “source” human?
Stingrays—“A Rose by Any Other Name . . .”

From: Kenneth Castro [mailto:Kenneth.Castro@sarasotagov.com]
Sent: Wed 4/15/2009 11:25 AM
To: Terry Lewis
Cc: Tom Laughlin; Curt Holmes; Paul Sutton
Subject: Trap and Trace Confidentiality

Good Morning Chief,

In where the detective specifically outlined the investigative means used to locate the suspect. As you are aware for some time now, the US Marshalls and I believe FDLE have had equipment which enables law enforcement to ping a suspects cell phone and pin point his/her exact location in an effort to apprehend suspects involved in serious crimes. In the past, and at the request of the U.S. Marshalls, the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions we simply refer to the assistance as "received information from a confidential source regarding the location of the suspect." To date this has not been challenged, since it is not an integral part of the actual crime that occurred.

The ASA was not sure what agency your Detective Sinehth used that had the equipment that enabled him/her to locate his suspect. They were concerned as we all are, that by providing these specifics on a pca, could jeopardize future investigations attempting to locate fugitives. The Tampa Office of the US Marshalls was not involved in the case, and they are not aware of who was. If this is in fact one of your cases, could you please entertain either having the Detective submit a new PCA and seal the old one, or at minimum instruct the detectives for future cases, regarding the fact that it is unnecessary to provide investigative means to anyone outside of law enforcement, especially in a public document. Please note that I am passing information on to you, and I have not been able to confirm that the case or detective are affiliated with NPPD.
The San Bernardino Sheriff’s Department shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State’s case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI. If the San Bernardino Sheriff’s Department learns that a District Attorney; prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology in a manner that will cause law enforcement sensitive information relating to the technology to be made known to the public, the San Bernardino Sheriff’s Department will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.
From: Kenneth Castro [mailto:Kenneth.Castro@sarasotagov.com]
Sent: Wed 4/15/2009 11:25 AM
To: Terry Lewis
Cc: Tom Laughlin; Curt Holmes; Paul Sutton
Subject: Trap and Trace Confidentiality

Good Morning Chief,

I just received a phone call from one of our detectives (Tom Laughlin) who is assigned to the U.S. Marshalls Task Force out of Tampa. He received a call from the ASA Craig Schaefer regarding some concerns. Schaefer advised him that they received a PCA regarding a North Port PD Case 09-031066 in where the detective specifically outlined the investigative means used to locate the suspect. As you are aware for some time now, the US Marshalls and I believe FDLE have had equipment which enables law enforcement to ping a suspects cell phone and pin point his/her exact location in an effort to apprehend suspects involved in serious crimes. In the past, and at the request of the U.S. Marshalls, the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions we simply refer to the assistance as " received information from a confidential source regarding the location of the suspect." To date this has not been challenged, since it is not an integral part of the actual crime that occurred.

The ASA was not sure what agency your Detective Sinehth used that had the equipment that enabled him/her to locate his suspect. They were concerned as we all are, that by providing these specifics on a pca, could jeopardize future investigations attempting to locate fugitives. The Tampa Office of the US Marshalls was not involved in the case, and they are not aware of who was. If this is in fact one of your cases, could you please entertain either having the Detective submit a new PCA and seal the old one, or at minimum instruct the detectives for future cases, regarding the fact that it is unnecessary to provide investigative means to anyone outside of law enforcement, especially in a public document. Please note that I am passing information on to you, and I have not been able to confirm that the case or detective are affiliated with NPPD.
“In the past, and at the request of the U.S. Marshalls, the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without knowledge of the criminal element, in reports or depositions we simply refer to the assistance as ‘received information from a confidential source regarding the location of the suspect.’”
Stingrays—*A Rose by Any Other Name* . . .

The Court therefore ORDERS, pursuant to Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117; and Title 28, United States Code, Section 1651, that Verizon Wireless, within ten (10) days of the signing of this Order and for a period not to exceed 30 days, unless extended by the Court, shall provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the Target Broadband Access Card/Cellular Telephone, and shall monitor such transmissions, to extend to any time of the day or night as required, including the monitoring of the Target Broadband Access Card/Cellular Telephone while the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is (a) inside private residences, garages and/or other locations not open to the public or visual surveillance; and (b) anywhere else the Target Broadband Access Card/Cellular Telephone may be present within the United States, pursuant to Title 18, United States

Stingrays—“A Rose by Any Other Name . . .”

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

https://www.aclu.org/technology-and-liberty/us-v-rigmaiden-doj-emails-stingray-applications
XIV. Cell Site Simulators/Digital Analyzers/Triggerfish

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," i.e., telephone number) and electronic serial number ("ESN," i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signalling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).

Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.
XIV. Cell Site Simulators/Digital Analyzers/Triggerfish

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," i.e., telephone number) and electronic serial number automatically when the cellular telephone is turned off. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).

Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.
Judge threatens detective with contempt for declining to reveal cellphone tracking methods

By Justin Fenton
The Baltimore Sun
contact the reporter

Judge threatened to hold Baltimore detective in contempt for refusing to discuss cellphone tracking technology

On topic of cell phone tracking, @BaltimorePolice say one technique is prohibited by "nondisclosure agreement"

Do Baltimore Police use stingrays? Prosecutors toss key evidence rather than allow detective to disclose.

Baltimore prosecutors withdrew key evidence in a robbery case Monday rather than reveal details of the cellphone tracking technology police used to gather it.

The surprise turn in Baltimore Circuit Court came after a defense attorney pressed a city police detective to reveal how officers had tracked his client.
is that we would submit on the Defense motion to suppress what was recovered in the house during the execution of the search warrant and specifically what I’m referring to, there was a .45 caliber handgun, a magazine, eight rounds, and in the Defendant’s possession was a cell phone recovered in his pocket. I believe that’s the crux of the Defendant’s motion to suppress. We’re still prepared to proceed with the rest of the case.
Secrecy around police surveillance equipment proves a case’s undoing

By Ellen Nakashima  February 22  Follow @nakashimae

TALLAHASSEE — The case against Tadrae McKenzie looked like an easy win for prosecutors. He and two buddies robbed a small-time pot dealer of $130 worth of weed using BB guns. Under Florida law, that was robbery with a deadly weapon, with a sentence of at least four years in prison.

But before trial, his defense team detected investigators’ use of a secret surveillance tool, one that raises significant privacy concerns. In an unprecedented move, a state judge ordered the police to show the device — a cell-tower simulator sometimes called a StingRay — to the attorneys.

Rather than show the equipment, the state offered McKenzie a plea bargain.
Stingrays—Who Has Them?
Stingrays—Who Has Them?

https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them
Stingrays—Changes on the Horizon?

Tacoma police change how they seek permission to use cellphone tracker

BY ADAM LYNN
Staff writer  November 15, 2014

Pierce County judges didn’t know until recently that they’d been authorizing Tacoma police to use a device capable of tracking someone’s cellphone.

That’s now changed.

The county’s 22 Superior Court judges, who first learned of the police department’s cell site simulator from The News Tribune’s reporting, now require language in pen register applications that spells out police intend to use the device.

Law enforcement agencies that want to deploy the device also must swear in their affidavits that they will not store data collected from people who are not the target of the investigation, said Judge Bryan Chushcoff, who requested the verbiage during recent meetings with police officials.

“They said they could live with that,” Chushcoff said.
Stingrays—Changes on the Horizon?

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology

LEGAL PROCESS AND COURT ORDERS

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent), except as provided below.

Information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department’s law enforcement and national security missions, as well as the Department’s commitments to accord appropriate respect for individuals’ privacy and civil liberties. This policy provides additional guidance and establishes common principles for the use of cell-site simulators across the Department. The Department’s individual law enforcement components may issue additional specific guidance consistent with this policy.

Latest on Stingrays

- August 2016: FCC complaint about police Stingray use filed by Center for Media Justice, Color of Change, New America’s Open Technology Institute

- Alleges that Baltimore police violate federal Communications Act by using Stingrays
  - *Interference with cellular network, disrupting calls*
  - *With disproportionate impacts on communities of color*

- Map in FCC complaint plots hundreds of addresses where *USA Today* discovered BPD was using Stingrays over map of Baltimore’s
Hemisphere
Los Angeles Hemisphere
LAw Enforcement Sensitive

HIGH INTENSITY DRUG TRAFFICKING AREA
Office of National Drug Control Policy

http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html#p1
Hemisphere
What is it & What Can You Learn From It?

• **AT&T keeps database of CDRs—available in near real time regardless of carrier**
  – Includes records made 2 hours after a call
  – Results returned in hours for exigent circumstances and 2-5 days for routine requests
  – At least 10 years worth of records

• **Used to:**
  – Find dropped/new/additional phones
  – Determine some location information
  – CDRs on international numbers
DEA - Seattle 2011

- During a wire intercept conducted from Jan 2011 to April 2011, targets would continually rotate their pre-paid phones
  - Utilized Hemisphere extensively to identify dropped phones and verify targets
  - Hemisphere identified a significant amount of the new numbers
- Based on this wire intercept investigation DEA was able to seize;
  - 136 kilos of cocaine
  - 2000 pounds of marijuana
  - Approximately 2.2 million dollars
  - Several residences, vehicles, and other assets.
- “Plus, we really pissed off the Hells Angel’s in Canada”
Kennard Walters, allegedly impersonating a 2 Star General, was asked to show an identification card at Naval Base San Diego.

He stated he left the card in his vehicle and drove off.

Walters physically assaulted and subsequently ran over a Naval Criminal Intelligence Service Special Agent and fled the base.

After the initial incident, the suspect changed his phone number and drove to northern California.

After a return to the Los Angeles area, he then drove to Tehama County in Northern California where he was apprehended.

Hemisphere was able determine his new telephone number, and provide cell site data leading to his arrest.
Hemisphere

“First Rule of Fight Club, Don’t Talk About Fight Club”

All requestors are instructed to never refer to Hemisphere in any official document. If there is no alternative to referencing a Hemisphere request, then the results should be referenced as information obtained from an AT&T subpoena.
“Protecting” Hemisphere

• Administrative subpoena to get Hemisphere records
• “Parallel subpoenaing”
  – Hemisphere used as a “pointer” system to be followed up by a subpoena to carrier
• No reference to Hemisphere in official reports or court documents
  – Just reference to follow-up subpoenas
US v. Ortiz, 12cr119 (NDCal)

- Defense obtained 17(c) subpoena ordering disclosure of:
  - Court orders authorizing HIDTA to release CDRs to law enforcement
  - Correspondence between law enforcement and Hemisphere

DEA Bulk Records Collection

• Collection of phone records made from US to 116 countries from 1992-2013
  – numbers, time and date of call and length of call
• Database queried if reasonable articulable suspicion phone associated with criminal activity
• DEA’s SOD passed info as tips to field agents and local law enforcement
  – Database not referenced in official reporting
Metadata & What You Can Learn From It
What is “Metadata” . . .

• Data about the data
• Data not traditionally considered content
• Who you send a letter to, rather than what is in the letter
• Phone numbers we dial, the bank account information we share with our bank, the people we email, where we go and when
Metadata is a Proxy for Content
What Can We Learn from Metadata?

• Who you know, how you know them, how long you’ve known them, who they know
• Your political & religious beliefs
• Your health information
• Where you’ve been and where you’re going
• Who you are
What Can We Learn From Metadata?

“Call Detail Records”
What Can We Learn From Metadata?

Email Data
Other new technologies

• Automated license plate recognition
  – ALPR increasingly used for mass tracking

• Facial recognition (biometrics)
  – Georgetown “perpetual lineup” study
  – 1 year + >100 FOIAs + dozens of interviews +
    science lit + 2 companies + 50 state law surveys +
    2 site visits

• Government hacking, Rule 41
  – Network investigative techniques?

• Encryption and passwords

• NSA surveillance (Section 702 notices)
ALPR: what it is

- Automated high-speed camera system
  - Usually mounted on cars or fixed objects (light poles) that automatically detect when license plate enters camera’s field, capture image of car and surroundings (including plate), and convert the plate image into alphanumeric data
  - In effect “reading” the plate
- Also records date/time/place
- Up to 1800 plates/min
  - Squad car can get 14,000 plates in one shift
ALPR: what police do with it

• Use is exploding
  – LA sheriff +PD: 3 million vehicles/week
  – September 2009 survey reported that out of 305 randomly selected police departments nationwide, 70 (or 23%) used ALPRs.
  – 2011 Police Executive Research Forum survey of more than 70 of member police departments showed that 71% used ALPR technology and 85% expected to acquire or increase use in the next five years.

• Like Stingrays, commercial vendors push
WSJ: “Gun-Show Customers’ License Plates Come Under Scrutiny”

• 2010 ICE plan: local police officers drive around parking lot at SoCal gun shows, use ALPR to collect data from cars
  – E.g., Crossroads of the West gun show in Del Mar, Calif., not far from Mexican border
  – Maybe 6-9k plates (estimate of Crossroads visitors)?
  – Agents compared gun-show-plate data to cars that crossed the border, hoping to find gun smugglers

• ICE agents planned to keep doing at other SoCal gun shows, but agency officials couldn't confirm whether they had.
ALPR: plates can be misread

• 2009: SF cops pulled over woman driving her own car. At gunpoint, they handcuffed her, forced to her knees, and then searched her and her car—because ALPR identified her car as stolen.
  – Error 1: misread her plate, recording a “3” as a “7.”
  – But many human errors:
    • First cop didn’t visually verify that Green’s plate matched ALPR “hit”—even after dispatch matched it to vehicle that didn’t look like Green’s
ALPR: transparency

• Analyzed eight days of ALPR data provided by City of Oakland under CA Public Records Act
  – https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data

• Also discovered security vulnerabilities

• **Issue:** who should have access to mass surveillance data?
Facial recognition: “perpetual lineup”

- Key findings of Georgetown study just released Tuesday
  - #1: Law enforcement face recognition is more pervasive & advanced than people realize.
  - #2: Law enforcement face recognition will have a disparate impact on African Americans.
  - #3: Law enforcement face recognition is not under control.
- http://www.perpetuallineup.org
How pervasive and advanced is FR?

- GAO Report this summer reported
  - 64 million face photos in 16 states
  - **WRONG!**
  - 119 million face photos in 30 states
  - 53% of adults in US

- **What databases?**
  - In some states, DL photos + mug shots + corrections
  - Includes real-time/dragnet surveillance using social media photos
Systems not built for diversity

• FR accuracy depends on statistical properties of training data (like most machine learning)
  – But LE data not population-representative

• From Pennsylvania JNET Manual

10.3.4.1.3 Generating the 3D Model

Once the feature points have been adjusted (if necessary), it is time to generate the 3D model representing each subject.

• Metadata Category: Select the category from the drop-down list that best represents the subject in the photograph. You can choose, Generic Male, Generic Female, Asian Male, Asian Female, Caucasian Male, Caucasian Female or Middle Eastern Male.
NIST hasn’t tested for bias since 2010

• FBI accuracy: 86% accurate (n = 1 million)
  – 1 of 7 searches yields 2-50 innocent people
  – Errors are not evenly distributed
• 2012: FBI* study: 5-10% less accurate on African Americans, women, 18-30 yo
• Vendors ignore bias:
  – “Q: Is the Booking Photo Comparison System biased against minorities[?]”
  – “A: No... it does not see race, sex, orientation or age.”
• FAQ, Seattle South Sound 911
Exacerbated by bias in DBs

- African Americans at least twice as likely to be arrested as members of any other race in US and, by some estimates, up to 2.5 times more likely to be targeted by police surveillance.
- Overrepresentation in both mug shot databases and surveillance photos will compound impact of disparity in accuracy rates.
- Thus, African Americans not only more likely to be misidentified by FR—also more likely to be in both mug shot and surveillance photos.
Imagine robbery caught on camera

• When police run video still of suspect’s face against their FR DB, they get 10 possible matches, but none perfectly matches suspect.

• Closest match probably treated as a lead, which could easily be an innocent person.

• Statistically, this scenario more likely for African Americans due to overrepresentation in DB.

• 2012 mug shot study: FR algorithm recognized members of the race in its training set more readily than members of any other
Unregulated and uncontrolled

- No comprehensive federal or state law
- 20% clearly require individual suspicion
- 1 of 52 agencies limited to certain crimes
- 1 of 52 clearly prohibited searches to conduct religious, political surveillance
- 4 of 52 had a public use policy
- 1 of 52 required legislative approval
- 1 of 52 had clearly functioning audits
Biometrics more than face

- MORIS Multi-modal Biometric Mobile ID Device
  - Iris + face + fingerprint scanning
- California
  - Orange County Sheriff's Department: iris recognition
  - Los Angeles Sheriff’s Department’s biometrics system includes tattoo recognition
- FBI Next-Generation ID system
  - FBI seeks to avoid Privacy Act accuracy requirements
  - Includes DNA but FP catalyzed opposition (“color blindness”)
Encryption and passwords
Encryption and passwords

• Continued unclarity about compelling suspects to decrypt
  – EFF/ACLU amicus brief covers cases up to April 2016
  – Focus on privilege against self-incrimination, “foregone conclusion” doctrine per *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012).

• And of course compelling companies like Apple to decrypt under All Writs Act

• Don’t be surprised if FBI pushes crypto bill next year
Resources: street-level surveillance

• https://www.eff.org/sls/defense-attorneys
  – Amicus briefs in a variety of surveillance cases
  – Documents about government surveillance from our FOIA litigation
  – Documents from ACLU, etc., from FOIA and PRA work across country
Government hacking, Playpen, R41 & the 4th Amendment
Government hacking and NITs

• “Malware” = catchall
  – Code designed or intended to be used for covert remote access, control of devices, disruption of operations, display of unwanted ads…. like NIT

• Focus on NIT (network investigative technique)
  – Similar to RAT (remote access tool): keystroke logging, file system access, control of mike/webcam
  – NIT (“payload”) was installed on user computers
  – Some “exploit” permitted installation; we believe but don’t know FBI exploited weakness in the
“Playpen”

• FBI got tip from “foreign LEA” about child porn site hosted on Tor network as “hidden service”*
  – Tip: IP address of actual server located in US
  – Got warrant to seize Playpen server (Naples, FL)

• Then ED Va warrant authorized gov’t to
  – Install NIT on of “any user or administrator who logs into [Playpen] by entering a username and password”
Playpen by the numbers

- During the 2 weeks, FBI harvested approximately 1,300 IP addresses, and around 137 people have been charged so far
  - Estimated more than 100,000 Playpen users total
  - Searches in Arkansas, California, Louisiana, Massachusetts, Oklahoma, Ohio, Pennsylvania, Texas, Washington, and Wisconsin—I think Kansas, too.
  - Probably also international computers
4th A issues

• Series of searches and seizures *per deployment*
  – Installing NIT = seizure of computer
  – Operating NIT = search of private areas
  – Copying data = seizure of private data

• Particularity
  – Any/all “activating computers”: Could have been hundreds of thousands, although in fact much fewer.
  – But government had seized server logs and other info about Playpen users, so could have been more specific
Rule 41 and magistrate judges

• Rule 41 MJ extraterritoriality
  – ED Va MJ was told “located in” ED Va
  – Server was, but government couldn’t know all the “premises to be searched” were
    • Affidavit never mentioned that most site users were possibly or probably outside ED Va or that gov’t didn’t know
  – Courts going in all directions
  – International aspects: location; violate foreign law?

• New Rule 41
  – Anywhere, if technological means (Tor, VPN) used to obscure location
Discovery, motions to suppress

- Focus on code for NIT, but also exploit
  - Mixed results: Michaud, Feb. order to FBI to provide defense with all code used to hack Michaud's computer.
  - “Much of the details of this information is lost on me . . but it comes down to a simple thing. You say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question.” (WD WA Dist. Judge Bryan)

- Colin Fieman, FD in WD Wa: Dropbox repository of Playpen resources
NSA surveillance, parallel construction, defendant notice under 702
NSA shares with DEA (SOD)

- FISA, Sec. 702: supposedly for FI purposes but can be used for crime post 9/11, e.g. DEA Special Operations Division
  - "You'd be told only, 'Be at a certain truck stop at a certain time and look for a certain vehicle.' And so we'd alert the state police to find an excuse to stop that vehicle, and then have a drug dog search it," the agent said.
Parallel construction

- NSA tips obscured (Reuters)
  - After an arrest was made, agents then pretended that their investigation began with the traffic stop, not with the SOD tip, the former agent said.
  - The two senior DEA officials, who spoke on behalf of the agency but only on condition of anonymity, said the process is kept secret to protect sources and investigative methods. "Parallel construction is a law enforcement technique we use every day," one official said. "It's decades old, a bedrock concept."
FAA702 Operations
Two Types of Collection

**Upstream**
- Collection of communications on fiber cables and infrastructure as data flows past.
  (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

**PRISM**
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple.
Government notice of 702

• *Clapper* case: SG Verrilli told SCt that if government wanted to use 702 evidence for prosecution, it would have to disclose the source—and such defendants had standing to challenge 702 (Oct 2012)
  • SCt relied on Verrilli’s concession to rule against Al.
  • See 50 USC § 1806(c); 50 USC § 1881e(a)

• Feinstein, 12/2012, had listed 702 “successes”—but defense lawyers hadn’t gotten notice (e.g., *Daoud*)

• “it turned out that … national security prosecutors … had not been alerting such defendants that evidence in their cases had stemmed from wiretapping their conversations without a warrant.” (NYT, 10/17/2013)
Which Laws Apply?
How to Challenge?
Discovery

- **Brady v. Maryland**, 373 U.S. 83 (1963)
  - “favorable to an accused”
  - “material either to guilt or to punishment”

- **Fed. R. Crim. Pro. 16(a)(1)(E)(i)**
  - Docs or data “material” to preparing defense

- **“Material”**
  - “reasonable probability that its disclosure would have affected the outcome of the proceedings”
    - **US v. Guzman-Padilla**, 573 F.3d 865, 890 (9th Cir. 2009)
What’s “Material?”

- Relevant to suppression challenge

- Bearing on the reliability of a source
  - *Giglio v. US*, 405 U.S. 150 (1972); *US v. Thomas*, 726 F.3d 1086, 1096 (9th Cir. 2013)

- Necessary to raise a *Franks* Challenge
  - *US v. Barton*, 995 F.2d 931, 934 (9th Cir. 1993)
In this motion, we seek to have the Court order disclosure of StingRay information for each of the named clients and order the release of the names of all clients of the Sacramento Public Defender whose cell phones and other mobile devices have been illegally monitored, seized, or taken over by a StingRay device.
October 23, 2014

Sheriff Scott R. Jones
Sheriff Sacramento County
711 G St
Sacramento CA 95814

Re: Public Records Act Request For “Stingray” Surveillance Documents

The Sacramento County Public Defender’s Office, on behalf of our clients who are enumerated on the list attached to this letter as Exhibit A, is making a Public Records Act request. The Public Defender represents thousands of people each year. Exhibit A is a select list of approximately 200 clients over a three month period. We have selected only clients who were set for preliminary examination in this time period and we have attempted to select among that larger list a reduced list that contains cases that are more likely to have had a stingray used in their case, roughly based on the charge offense.

Pursuant to the rights under the California Public Records Act (Government Code Section 6250 et seq.), we ask to inspect and/or obtain a copy of the following:

1. During the previous 12 month period, please provide us with all documents and records showing or suggesting that any of the people listed on Exhibit A had any wiretap, cell tower emulator, cell-site simulator, stingray or similar device used in order to capture the unique numeric identifier associated with a mobile device, computer or tablet device to locate that person or their device, and/or to intercept any
“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

“We must assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted but it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case.”

Expectations of Privacy

  – Must “have a source outside of Fourth Amendment” by reference to “understandings that are recognized and permitted by society”

  – Privacy interests depend on the quality and quantity of information revealed
  – Older cases involving physical items or less intrusive government action don’t control digital searches or surveillance
Statutory Framework: ECPA

- **Wiretap Act** (18 USC §§ 2510-2522)
  - Real time interception of communications

- **Stored Communications Act** (18 USC §§ 2701-2712)
  - Stored electronic and wire content and metadata

- **Pen Register/Trap & Trace Act** (18 USC §§ 3121-3127)
  - Electronic & wire dialing/routing info
  - Cannot be “solely used” to obtain location info (47 USC § 1002(a))
Statutory Framework: ECPA

- ECPA Wiretap: Super Warrant
  - R.41 Warrant: "probable cause"
  - SCA: "specific and articulable facts" records are "relevant and material"
  - PR/TT: "Relevant"
Historical CSLI—Federal Cases

• Warrant constitutionally required
  – *US v. Graham*, ___ F.3d ___, 2015 WL 4637931 (4th Cir. Aug. 5, 2015);

• Warrant may be required
  – *In re US for an Order Directing…*, 620 F.3d 304 (3d Cir. 2010)

• Warrant not required
  – *In re US for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)
  – *US v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc)
Historical CSLI—State Cases & Statutes

• Warrant constitutionally required (under state or fed. constitution)
  – Tracey v. State, 152 So.3d 504 (Fla. 2014)
  – State v. Earls, 70 A.3d (NJ 2013)

• Warrant statutorily required
  – Historical & real time: CO, ME, MN, MT, TN, UT
  – Real time only: IL, IN, MD, VA, WI, WA (stingrays)
How to Challenge—*Distinguish* Smith v. MD (3rd Party Records)

  - “expectation of privacy” must “have a source outside of Fourth Amendment” by reference to “understandings that are recognized and permitted by society”

- Subjective expectation of privacy
  - Location info revealing, especially when aggregated
    - Phone records protected under CA constitution

- Privacy expectation is objectively reasonable
  - Growing body of case law and statutory protection reflect changing “understanding”
How to Challenge—*Distinguish* Smith v. MD
(3rd Party Records)

- *US v. Nerber*, 222 F.3d 597, 601 (9th Cir. 2000)
  - “…legitimacy of a citizen’s expectation of privacy in a particular place may be affected by the nature of the intrusion that occurs.”

- *US v. Graham,*
Other Constitutional Challenges—Stingrays

- Invalid general “search” & “seizure”
- Need a warrant
  - Not a third party record
  - Can’t use pen register to obtain location info
    - 47 USC § 1002(a)
- Warrant can never be particular
How to Challenge—Avoid Good Faith Exception

  – No exclusion when police in good faith rely on a warrant later found to be invalid

• **Cannot rely on “facially deficient” order**
  – Can’t use pen register order to obtain location info
    • Violation of 47 USC 1002(a), enacted in 1994
  – CA law enforcement must get warrant to obtain cell site records
    • CA Penal Code § 1326.1(b)
How to Challenge—Avoid Good Faith Exception

• *Davis v. US*, 131 S.Ct. 2419 (2011)
  – No exclusion of evidence obtained “in objectively reasonable reliance on binding appellate precedent”

• Courts split on application
  – Applying *Davis* when prior case specifically involved GPS
    • *US v. Pineda-Moreno*, 688 F.3d 1087 (9th Cir. 2012); *US v. Barraza-Maldonado*, 732 F.3d 865 (8th Cir. 2013)
  – Applying *Davis* based on *Knotts/Karo*
    • *US v. Sparks*, 711 F.3d 58 (1st Cir. 2013); *US v. Aguiar*, 737 F.3d 251 (2d Cir. 2013); *US v. Brown*, 744 F.3d 474 (7th Cir. 2014)
  – Declining *Davis* when no specific GPS case law
Questions?

tien@eff.org
415 436 9333 x 102
www.eff.org