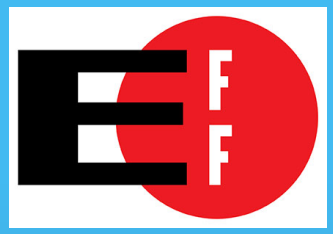


# Defending Against the Digital Dragnet

Stephanie Lacambra
Criminal Defense Staff Attorney
Electronic Frontier Foundation

# Reining in Digital Searches

# Digital searches trigger 4th Amend

- *US v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) - "Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."
- *US v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc): The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities. "Forensic" border search of digital device is "non-routine" & requires reasonable suspicion
- Riley v. CA, 134 S.Ct. 2473, 2493 (2014) - warrant is generally required to forensically search a cell phone, even when seized incident to arrest.

# DOJ's 2-step approach:

- DOJ's Manual for Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations (eff.org/DOJDSM2009)
- Two-Step approach detailed on pp.76, 86-87 (2009):
  1. the overseizure – or "imaging" – government physically seizes a digital storage device and makes a complete digital copy or "image" of its contents, and
  2. the general search of the seized information – or "analysis" – government analyzes the digital copy using forensic software.

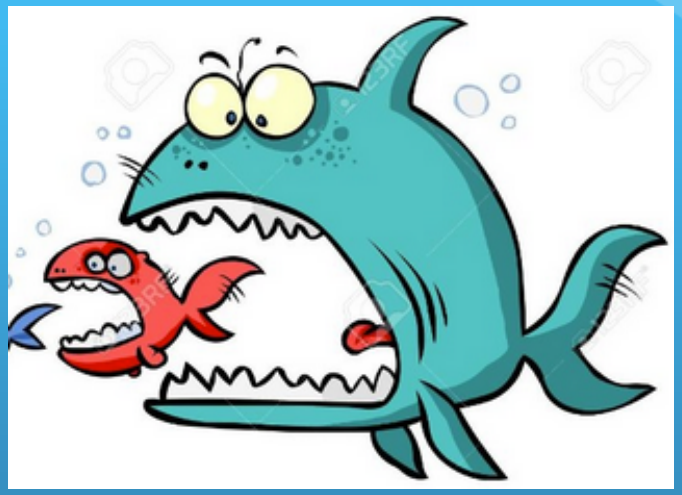
# DOJ's 2-step approach:

## D. Forensic Analysis

### 1. The Two-Stage Search

In the vast majority of cases, forensic analysis of a hard drive (or other computer media) takes too long to perform on-site during the initial execution of a search warrant. Thus, as discussed in Section C.3 above, investigators generally must remove storage media for off-site analysis to determine the information that falls within the scope of the warrant. This process has two steps: *imaging*, in which the entire hard drive is copied, and *analysis*, in which the copy of the hard drive is culled for records that are responsive to the warrant.

# Plain View



- When applied in the digital space - becomes the exception that swallows the 4th Am rule against general searches

# Arguments for rejecting plain view

- United States v. Tamura, 694 F.2d 591 (9th Cir. 1982)

1. Court recognized intermingling of items described in a warrant and other material that the government had no probable cause to seize
2. "wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'" p. 595-96 (quoting US v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980))

# Arguments for rejecting plain view

- US v. Comprehensive Drug Testing, Inc (CDT), 621 F.3d 1162 1177 (9th Cir. 2010)(en banc)

1. Govt got warrant for drug testing records of 10 baseball players, but seized electronic storage devices and copied a directory containing information about hundreds of players, in addition to the ten mentioned in the warrant, and searched all of the files in the directory, despite conditions in the warrant that precluded them from doing so

# Arguments for rejecting plain view

- US v. CDT

2. When, as here, the government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof.
   P. 1174.

3. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect. P. 1177

# Kozinski's guidance for digital searches in CDT (1177-79)

1. Govt must waive reliance upon the plain view doctrine
2. Forensic analysis must be done either by specialized personnel or an independent third party.
3. Govt must disclose the actual risks of destruction & other avenues of access
4. search protocol must be designed to uncover only information for which govt has probable cause
5. Govt must destroy or return non-responsive data

# Dangers of plain view:

- US v. Gurczynski, 76 M.J. 381 (C.A.A.F. 2017) - evid of child porn was outside scope of SW, thus search of thumb drive was constitutionally unreasonable:
  1. extraordinary length of time between the issuance of the warrant and the digital examination of the thumb drive—over nine months -p.387
  2. Govt no longer had a legitimate interest in searching for evidence following Appellee's convictions -p.387

# Dangers of plain view:

- US v. Gurczynski, 76 M.J. 381 (C.A.A.F. 2017)
  3. Govt's order to Digital Forensic Examiner to go beyond the scope of the warrant was unreasonable –p.386
  4. "We decline to grant the Government the unbridled discretion to conduct what is functionally a "general, exploratory rummaging in a person's belongings," *Coolidge*, 403 U.S. at 467, by relying on a warrant no longer justified by any legitimate government interest to assert that other evidence was in plain view" -p.387

# What PC for digital info should be:

US v. Griffith, 867 F.3d 1265,
(DC Cir. Aug 18, 2017)

- pervasiveness of cell phones and cell phone use insufficient to support PC for warrant to search suspect's home – 1273
- warrant invalid for overbreadth in allowing the seizure of all electronic devices found in the residence regardless of ownership – p.1276

# What PC for digital info should be:

US v. Griffith, 867 F.3d 1265,
(DC Cir. Aug 18, 2017)

the assumption that most people own a cell phone would not automatically justify an open-ended warrant to search a home anytime officers seek a person's phone

# What PC for digital info should be:

US v. Griffith, 867 F.3d 1265,
(DC Cir. Aug 18, 2017)

We are aware of no case, and the govt identifies none, in which police obtained authorization to search a suspect's home for a cell phone without any particularized information that he owned one

# What PC for digital info should be:

US v. Griffith, 867 F.3d 1265,
(DC Cir. Aug 18, 2017)

Yet the warrant did not stop with any devices owned by Griffith, which already would have gone too far. It broadly authorized seizure of *all* cell phones and electronic devices, without regard to ownership. That expansive sweep far outstripped the police's proffered justification for entering the home—viz., to recover any devices owned by Griffith.

# Make objections from *Griffith*:

SW affidavit failed to establish client owned a cell phone. (p.1272)

1. no observation client used a cell phone
2. no info that anyone received a cell phone call or text message from client
3. no record of officers recovering any cell phone in client's possession

But the affidavit in this case conveyed no reason to think that Griffith, in particular, owned a cell phone. There was no observation of Griffith's using a cell phone, no information about anyone having received a cell phone call or text message from him, no record of officers recovering any cell phone in his possession at the time of his previous arrest (and confinement) on unrelated charges, and no indication otherwise of his ownership of a cell phone at any time.

# Great objections from *Griffith*:

SW affidavit failed to establish police had reason to think they'd find client's cell at home. (p.1273)


SW affidavit failed to establish client's cell would contain incriminating evidence about suspected offense. (p.1273)

# Great objections from *Griffith*:

To justify a search of the apartment to seize any cell phone owned by Griffith, moreover, police needed reason to think not only that he possessed a phone, but also that the device would be located in the home and would contain incriminating evidence about his suspected offense.

# Favorite Quote from *Griffith*:

given that police did not know whether Griffith owned a cell phone or any other electronic device, they could not describe ex ante the devices they would search for and seize. But it was no solution to rely on a catchall provision authorizing seizure of every device they might happen to find in the house. Nothing in the affidavit or warrant supported—or could have supported—probable cause to seize any and all phones, tablets, computers, and other electronic devices in the apartment.

U.S. v. Griffith, 867 F.3d 1265, 1278 (D.C. Cir. 2017)

# Ex ante search protocols:

- Commonwealth of MA v. James Keown:
  1. EFF amicus - https://www.eff.org/Keown
  2. EFF asks the Court to set a series of ex-ante search protocols – explicit limits on the scope of digital searches by outlining concrete categories of relevant info before the warrant's execution to ensure that the govt does not exceed its authority when searching digital devices and information

# Ex ante search protocols:

- Potential limiting factors:
  1. Keywords
  2. Date range
  3. Identify specific accounts or applications to be searched
  4. Email or texts of specific identifiable actors or handles
  5. Limiting to messages sent or received by specific actors
  6. File type limits
  7. File size limits

- *US v. Keith Gartenlaub*, 2016 WL 3607154 (C.D. CA 2016)
  1. EFF amicus on challenging FISA warrants and seizures: https://www.eff.org/Gartenlaub
  2. P.11-15 set forth arguments for ex ante search protocols

# Ex ante search protocols:

- Potential limiting factors:
  1. Keywords
  2. Date range
  3. Identify specific accounts or applications to be searched
  4. Email or texts of specific identifiable actors or handles
  5. Limiting to messages sent or received by specific actors
  6. File type limits
  7. File size limits

- *US v. Keith Gartenlaub*, 2016 WL 3607154 (C.D. CA 2016)
  1. EFF amicus on challenging FISA warrants and seizures: https://www.eff.org/Gartenlaub
  2. P.11-15 set forth arguments for ex ante search protocols

# Judicial oversight of digital searches:

1. Appoint a special master to do an initial overview of the digital data to identify the structure of how information is stored and then submit a report under seal to the court about what categories of directories and files are available for search*
2. Court determines which directories or files are appropriately tethered to the information that the government seeks in its warrant application and has provided probable cause to search and limits the special master's query to these file locations*
    a. Court should generally prohibit the wholesale search of all files within the seized devices/ accounts unless the government can prove file obfuscation by clear and convincing evidence

# Judicial oversight of digital searches:

3. require the government to articulate its query for the seized data with specific parameters designed to limit the information sought to be within the scope of the probable cause articulated in the warrant, such as:
   a. keyword search terms,
   b. date and time range,
   c. specific accounts, handles or identifiers,
      i. specific recipients
      ii. specific authors
   d. specific applications,
   e. File types, and
   f. file sizes.

# Judicial oversight of digital searches:

4. Review the search parameters requested by the government and permit defense to make any objections to the search terms or protocol in a contested hearing that allows for the presentation of evidence
5. rule on the objections and issue a written order with the search protocol for the special master to execute
6. require that any non-responsive information be sealed and stored with the court until the conclusion of the case, at which point the information should be returned or destroyed.

# But see *Richards* on ex ante:

- US v. Richards, 659 F.3d 527 (6th Cir. 2011)
  1. The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence....
  2. The proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation." (citing *US v. Meek*, 366 F.3d 705, 716 (9th Cir.2004)).

# But see *Richards* on ex ante & plain view:

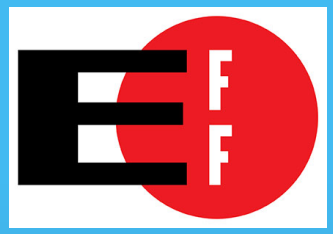
- US v. Richards, 76 M.J. 365 (C.A.A.F. 2017):
  1. Search authorization for "any communication that related to his possible violation of the Florida statute in his relationship with AP" is not overbroad - p.370
  2. Temporal limitation is not a requirement – p.370
  3. authorization allowed for a search of the unallocated space and through potential communications materials that did not have an immediately clear date associated with them – p.370
  4. discovery of the child pornography images within the folder of unallocated materials was consistent with *Horton v. CA* and the plain view exception to the Fourth Amendment. – p.371

# Beware the good faith exception:

- US v. Stavros Ganias, 824 F.3d 199 (2nd Cir. May 27, 2016) (en banc)(cert denied 12/5/16)
  1. law enforcement agents relied in good faith on search warrant in searching copies of mirrored hard drives
  2. Chin's Dissent and original panel decision - Government violated Ganias's Fourth Amendment rights when it retained Ganias's non-responsive files under 2003 warrant for nearly two-and-a-half years and then reexamined the files for evidence of additional crime under 2006 warrant. Not excused by good faith.
  3. EFF amicus: https://www.eff.org/Ganias

# Beware the good faith exception:

- US v. Blake, 868 F.3d 960, p.7-9 (11th Cir. Aug 22, 2017)
  1. MS warrant ok because: “It limited the emails to be turned over to the government, ensuring that only those that had the potential to contain incriminating evidence would be disclosed. Those limitations prevented “a general, exploratory rummaging” through Moore's email correspondence.” P. 8
  2. FB warrant more problematic, but saved by good faith. “The Facebook warrants are another matter. They required disclosure to the government of virtually every kind of data that could be found in a social media account.” P.8



# Questions?

Stephanie Lacambra
Criminal Defense Staff Attorney
Electronic Frontier Foundation
815 Eddy St., San Francisco, CA 94109
415-436-9333 x130
stephanie@eff.org