



U.S. Department of Justice

Criminal Division

Office of Enforcement Operations

Washington, D.C. 20530

VIA Electronic Mail

March 17, 2020

Jonathan Manes, Esq.
Roderick & Solange MacArthur Justice Center
160 E. Grand Ave., Sixth Floor
Chicago, IL 60611
jonathan.manes@law.northwestern.edu

Request No. CRM-300680988
Privacy International et al. v. Federal
Bureau of Investigation, et al., 18-cv-1488
(W.D.N.Y.)

Dear Mr. Manes:

This is the fourth installment of the Criminal Division's rolling production regarding your Freedom of Information Act request dated September 10, 2018, for certain records pertaining to "computer network exploitation" or "network investigative techniques." Your request is currently in litigation, Privacy International, et al. v. Federal Bureau of Investigation, et al., 18-cv-1488 (W.D.N.Y.). You should refer to this case number in any future correspondence with this Office. This request is being processed in accordance with the interpretation and parameters set forth by defendants in the July 12, 2019, letter to you from Senior Trial Counsel Marcia Sowles, as well as subsequent conversations regarding the Criminal Division's processing of the request.

Please be advised that a search has been conducted in the appropriate sections, and we are continuing to review and process potentially responsive records. After carefully reviewing 518 pages of records, I have determined that forty-six pages are responsive to your request: thirty-two pages are appropriate for release in full, copies of which are enclosed. Additionally, five pages are appropriate for release in part and nine pages are exempt from disclosure pursuant to:

5 U.S.C. § 552(b)(5), which concerns certain inter- and intra-agency communications protected by the deliberative process privilege and the attorney work-product privilege;

5 U.S.C. § 552(b)(6), which concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties;

5 U.S.C. § 552(b)(7)(A), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to interfere with enforcement proceedings;

5 U.S.C. § 552(b)(7)(C), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties; and

5 U.S.C. § 552(b)(7)(E), which concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact Senior Trial Counsel Marcia K. Sowles by phone at (202) 514-4960, by email at Marcia.Sowles@usdoj.gov, or by mail at the Civil Division, Federal Programs Branch, 1100 L Street, N.W., Room 10028, Washington, D.C. 20005, for any further assistance and to discuss any aspect of your request.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to an administrative appeal of this determination. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account on the following website: <https://foiastar.doj.gov>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



Amanda Marchand Jones
Chief
FOIA/PA Unit

cc: Marcia K. Sowles
Senior Trial Counsel
Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11028
Washington, D.C. 20005
Marcia.Sowles@usdoj.gov

Michael S. Cerrone
michael.cerrone@usdoj.gov

Enclosures

TOR Overview and Investigations



Jim Fottrell, Director HTIU

Outline

1. Techniques to Hide Your Identity Online
2. How Tor works
3. Tor Hidden Services
4. Online Communities on TOR
5. Investigating Anonymization Users
6. Network Investigative Technique (“NIT”)
7. Tor-based Investigations

Necessary Legal Authorization

- Search warrant
 - Note: data collected is non-content, search authorization is for the technique
- Where to go for authorization if offender location unknown
 - Where will you install it (website location?)

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

In the Matter of the Search of)
(*Briefly describe the property to be searched*))
(*or identify the person by name and address*))
OF COMPUTERS THAT ACCESS)
[REDACTED].onion)
)
)

Case No. [REDACTED]
UNDER SEAL

SEARCH AND SEIZURE WARRANT

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computer.

ATTACHMENT B

Information to be Seized

- The computer referred to herein as which will be located at the following WEBSITE by entering the following investigative technique:
- From any "activating" computer described in Attachment A:
1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
 3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
 4. information about whether the NIT has already been delivered to the "activating" computer;
 5. the "activating" computer's Host Name;
 6. the "activating" computer's active operating system username; and
 7. the "activating" computer's media access control ("MAC") address;

7. Tor-based Investigations

2012-present



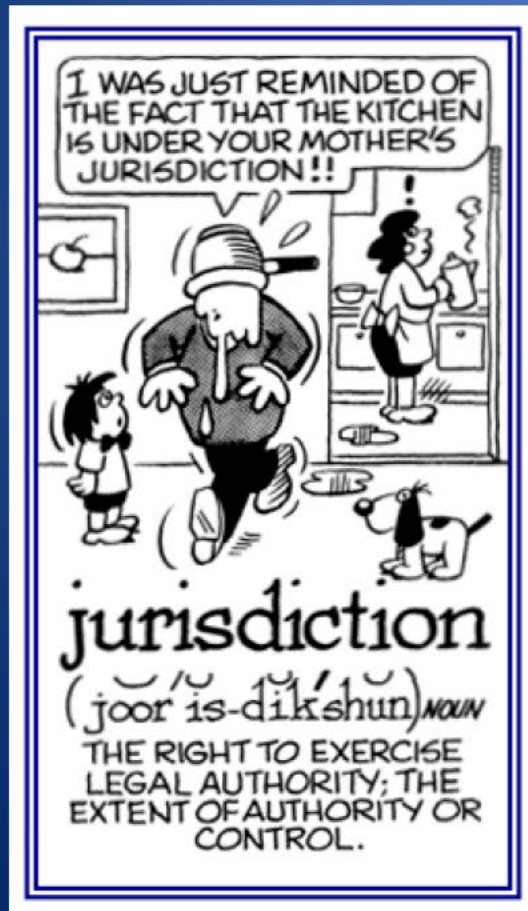
Operation Torpedo (2012 -)

- First-of-its-kind website takeover/NIT deployment
- 3 Tor CP websites seized
- 20 users prosecuted in DNE
- Model for future Tor investigations

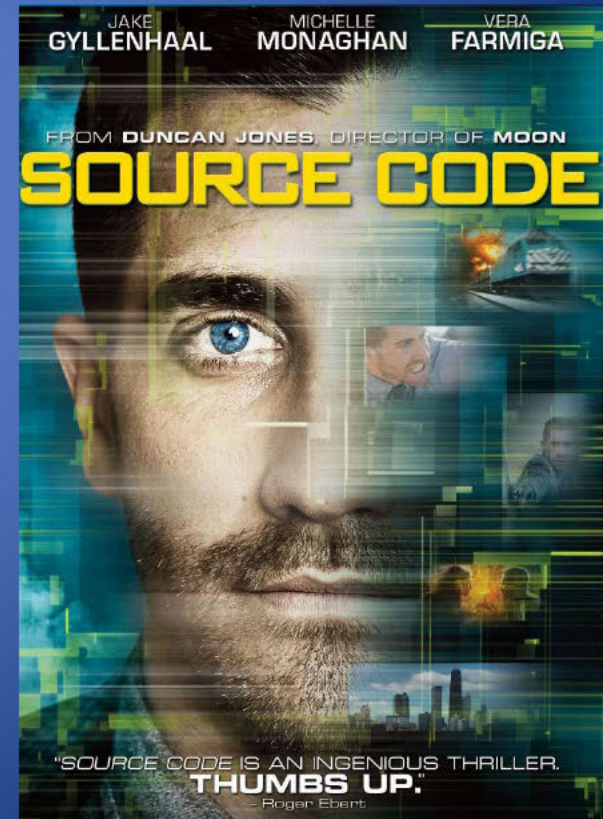


NIT Legal Challenges

- Suppression Issues
 - Rule 41(b) – Magistrate’s Jurisdiction to issue warrant



- Discovery Issues
 - “Source Code” – Materiality and Law Enforcement Privilege



Eleven courts have held that the EDVA magistrate was authorized to issue the warrant under the tracking device provision of Rule 41(b)(4)



Twenty courts have held that there was a technical violation of Rule 41 but suppression was unwarranted and/or the good faith exception applied



Four courts have held that there was a substantive violation of Rule 41, and that the good faith exception did not apply because the warrant was void *ab initio*; and granted suppression



Rule 41 Amendment

Rule

* * *

(b) V

enfo

* * *

(6) a

relat

warr

and

or o

(A) t

conc

(B) i

med

auth



aw

es

hin

en

t

Discovery Challenges: Source Code

- Defendants have sought discovery regarding the source code for the NIT
 - Possibility of compromise to computer's security settings (leaving computer open to someone else planting child pornography)
 - Need to confirm what information actually collected
 - Need to confirm that unique identifiers were unique

Discovery Challenges: Source Code

- Government has provided:
 - Source code for the NIT itself – instructions that ran on defendant computer
 - PCAP data stream – information back and forth between gov't and defendant computer
 - NIT information collected (IP, MAC address, host name, etc.)
 - Declarations stating that NIT did not compromise computer security settings and all unique identifiers were unique
 - Ex parte materials explaining sensitivity of further requested information
- Government has not provided:
 - Exploit and associated computer vulnerability
 - Code for generation of unique identifiers

THE HOTTEST TOPICS IN SEARCH AND SEIZURE

Advanced Online Child Exploitation Seminar
July 2018

Keith Becker, Deputy Chief
Child Exploitation and Obscenity Section, DOJ

(b) (6), (b) (7)(C) Senior Counsel
Child Exploitation and Obscenity Section, DOJ

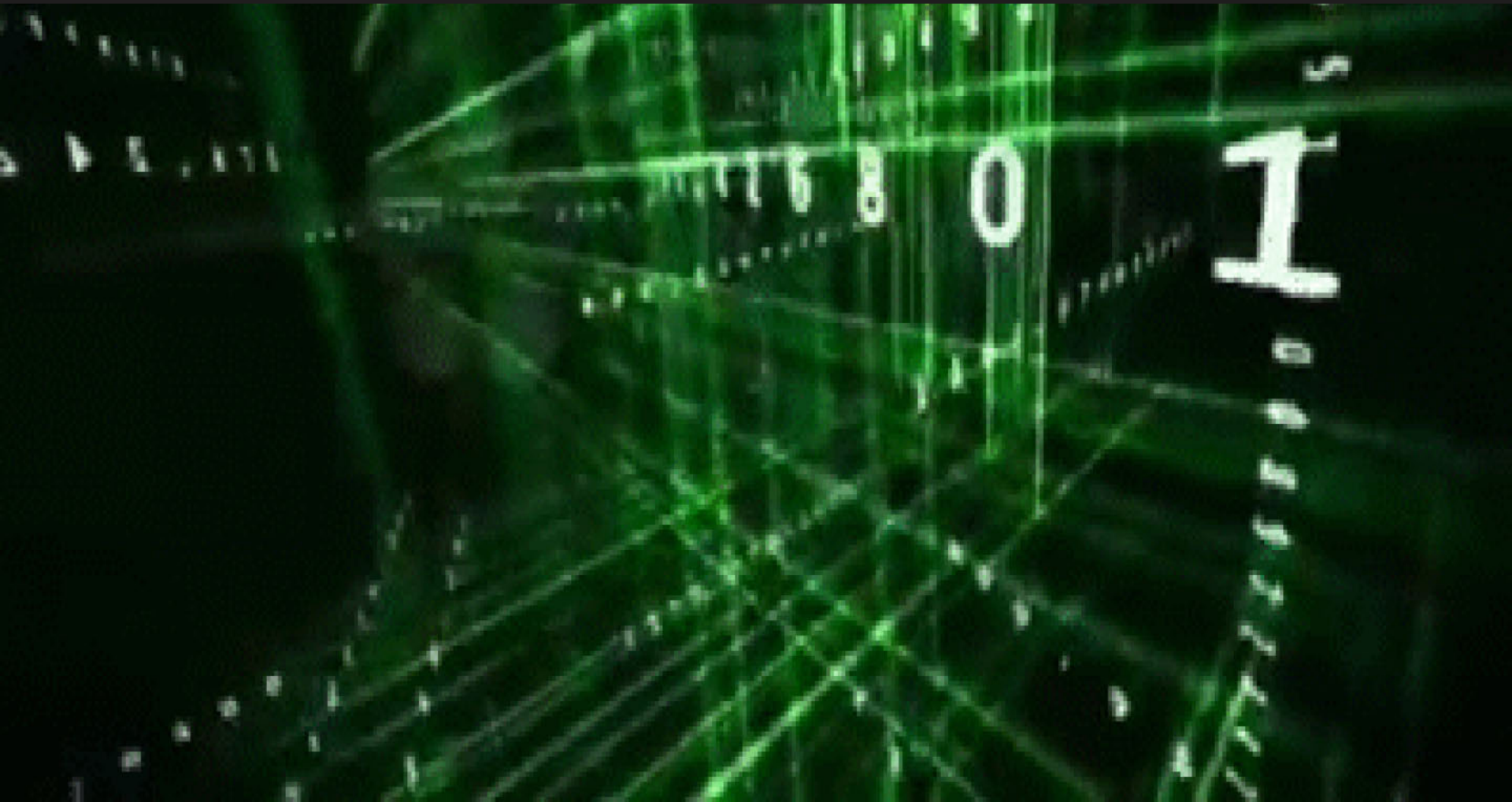




HOT TOPICS

- HSI Summonses
- Remote Search
- Private Search
- ECPA
- Border Searches
- Searching the Person
- SW Timing & Execution
- Encryption Workarounds

Remote Searches



Fed. R. Crim. Pro. 41(b)(6)

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means;

Operation Pacifier Update

- **Suppression of “NIT” Warrant**
- **Source Code Discovery**
- **“Outrageous Government Conduct”**
- **<https://dojnet.doj.gov/criminal/ceos/NationwideInvestigations/Pacifier.php>**

Limitations

- Deployment
- Operating System
 - Mac/Linux/Windows
- Browser
 - Firefox/Chrome/Safari/Opera
- Browser plugins/technology
 - Javascript
 - Flash
- Vulnerabilities/Patching



Necessary Legal Authorization

- Search warrant
 - Note: data collected is non-content, search authorization is for the technique
- Where to go for authorization if offender location unknown
 - Where will you install it (website location?)
 - Where will the user obtain it?

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

In the Matter of the Search of)
(*Briefly describe the property to be searched*))
(*or identify the person by name and address*))
OF COMPUTERS THAT ACCESS) Case No. 1:15-SW-89
upf45jv3bziuctml.onion)
) **UNDER SEAL**
)

SEARCH AND SEIZURE WARRANT

Tor-based Investigations 2012-present



COMING SOON TO
A THEATER NEAR YOU

Operation Torpedo (2012 -)

- First-of-its-kind website takeover/NIT deployment
- 3 Tor CP websites seized
- 20 users prosecuted in Nebraska
 - 6 convicted on conspiracy charges (12-25 years)
 - 12 convicted / awaiting plea on access/receiving CP (4-10 years)
- Model for future investigations



Operational Security Issues

Feds bust through huge Tor-hidden child porn site using questionable malware

FBI seized server, let site run for two weeks before shutting it down.

by Cyrus Farivar and Sean Gallagher - Jul 16, 2015 10:45am EDT

Share

Tweet

178



Teymur Madjderey

A newly unsealed FBI search warrant application illustrates yet another example of how the government deploys malware and uses **sophisticated exploits** in an attempt to bust up child pornography rings.

The **28-page FBI affidavit** (text-only, possibly NSFW) was unsealed in a federal court in Brooklyn, New York earlier this month. It describes a North Carolina server hosting a Tor hidden service site. The setup was seized in February

FURTHER READING



DEA, US ARMY BOUGHT \$1.2M WORTH OF HACKING TOOLS IN RECENT YEARS

Digital Forensics and Evidence: New Tools and Trends

Steve Grocki, Chief

Jim Fottrell, Director, HTIU

Child Exploitation and Obscenity
Section - DOJ

Overview

1. Tools for Mobile Devices
2. Top five computer artifacts
3. Into the Cloud - Internet Investigations
4. Anonymous Networks - Tor



Change to Rule 41

Google Says Proposed DoJ Warrant Tweaks Are “Monumental” Fourth Amendment Violation

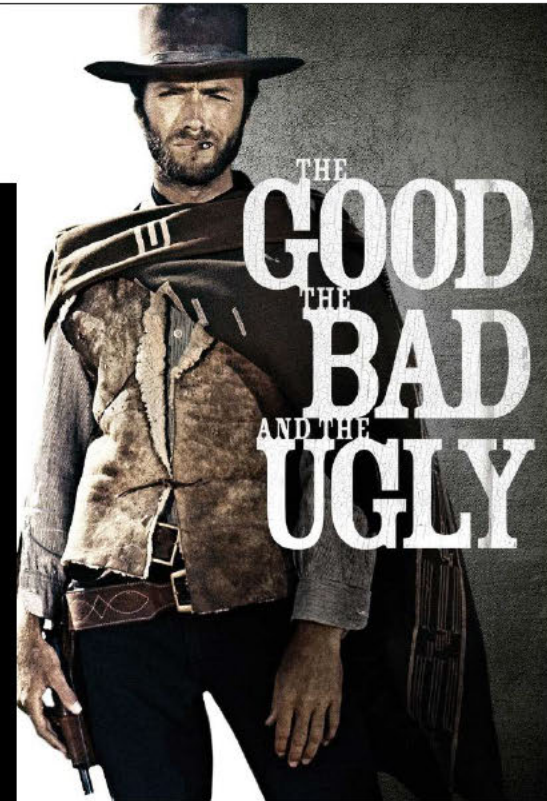
By Lily Hay Newman



Rule 41 -The Good, the Bad, and the Ugly

- Can go to a magistrate where activities related to crime occurred when tech used to conceal location.

(b) (5)





DEPARTMENT
OF JUSTICE

CHILD EXPLOITATION
& OBSCENITY SECTION

National Operations and Issues in CE Investigations

Steve Grocki, Deputy Chief
CEOS

What's wrong with a NIT?

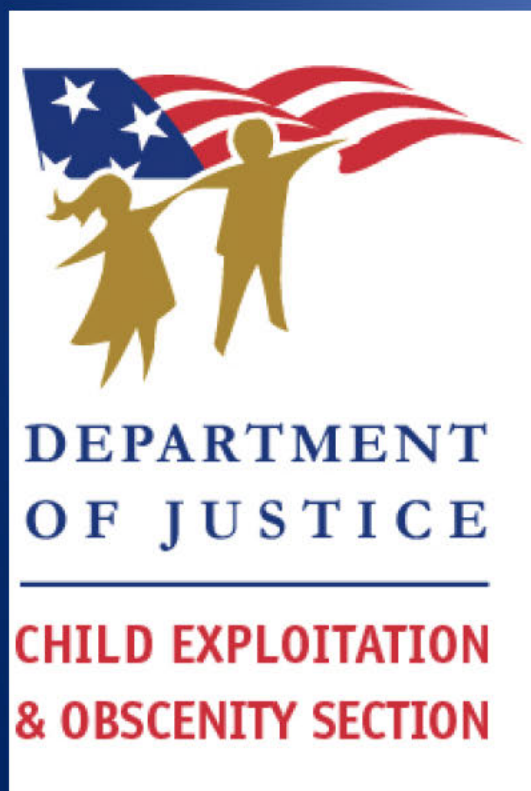
VISIT THE WRONG
WEBSITE, AND
THE FBI COULD
END UP IN YOUR
COMPUTER



What Authorization is Necessary to Implement a NIT?

- Search warrant
 - Note: data collected is non-content, search authorization is for the technique
- Where to go for authorization if offender location unknown
 - Where will you install it (website location?)
- Rule 41 Change allows judge to authorize anywhere in territorial US or if unknown

Current Trends and Challenges in Combating the Sexual Exploitation of Children



Keith A. Becker

Deputy Chief

U.S. Department of Justice, Criminal Division


Child Exploitation and Obscenity Section

Objectives

- Understand the purpose, operation and impact of organized child exploitation communities
- Review the technologies and platforms employed by offenders who participate in those communities
- Discuss investigative and prosecution strategies and challenges

Seize and Takeover – NIT deployment

(b)(6), (7)(C)



They're Watching...

05-21-2017, 02:29 PM

#1

After the Federal Bureau of Investigation arrested the administrator then took control of the child porn website PlayPen, investigators all over the world arrested about 900 users of the illicit site.

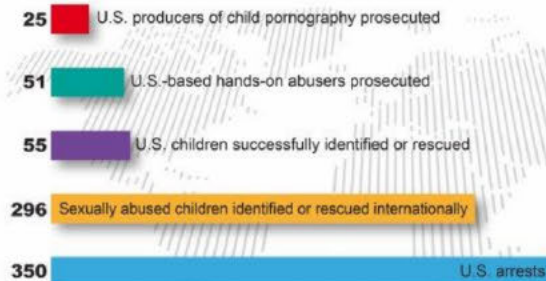
In December 2014, the FBI took control of the PlayPen child porn website for 13 days after arresting the administrator. While the Bureau was controlling the website, they uploaded malware, which they call NITs (Network Investigative Techniques), which provided them the IP address of the users who logged on in that 13 days. With the IP addresses acquired, the FBI had an easy job tracking down the criminals to their actual location. From 2015 to now, the federal agency managed to start investigations against hundreds of suspects, and law enforcement authorities all over the world arrested about 900 users of the child porn website.

Soon after the public was informed about Operation Pacifier (the law enforcement action led by the FBI and the US Department of Justice), the FBI received negative criticism from privacy advocates stating that the agency breached the civil liberties of the suspects. Additionally, some federal judges in the United States had ruled against the warrant the Federal Bureau of Investigation used in the course of the operation.

In connection with the PlayPen child porn website, 870 suspects were arrested worldwide with 368 of them located in Europe. According to the FBI's report, 296 child victims of sexual abuse were rescued of identified internationally, the Bureau added that the vast majority of the abused children are located outside of the US. The Federal Bureau of Investigation declared Operation Pacifier as the most successful law enforcement action against criminals who are located on the Tor network. One of the investigators said that Operation Pacifier was "one of the largest and most complex investigations ever undertaken in this field".

'Playpen' by the Numbers

The ongoing investigation of the Playpen child pornography website and its members led to its takedown in 2015 and has produced the following results through continued efforts by law enforcement agencies around the world:



Child's Play

(b) (6), (b) (7)(C)

Legal Challenges

- Suppression
- Discovery – Source Code
- “Outrageous Government Conduct”

National Litigation Results

- Suppression
- Discovery – Source Code
- “Outrageous Government Conduct”

Takeaways

- Organized, Online Child Exploitation Communities Pose a Unique and Significant Danger to Children
- Investigating Those Communities Requires a Multi-Faceted Approach, Involving Traditional and Technical Investigative Tools
- As Our Investigative Methods Evolve Alongside Our Offenders, (b) (5)