Common Defenses & Responses

Priscilla Grantham
Senior Research Counsel
National Center for Justice and the Rule of Law

Objectives:

After this presentation you will be able to:

• Describe some of the more common legal and technical defenses raises in technology-assisted crimes against children; and

• Recognize and explain the prime legal, investigative, technological, or forensic considerations surrounding such defenses

Special Thanks

Don Mason
Acting Director
National Center for Justice and the Rule of Law
...and also:

- Sgt. Josh Moulin, Commander, Southern Oregon High-Tech Crimes Task Force
- Martin Purselley, Chief, Computer Crimes Sec., Tarrant Co. D.A.'s Office, Fort Worth
- Howard Wise, Sr. Deputy D.A., Ventura, Calif.
- Justin Fitzsimmons, Sr. Attorney, NDAA/Nat'l Cntr for Pros. of Child Abuse
- Jeffrey Dort, Deputy D.A., San Diego
- Robert Morgester, Deputy Calif. A.G.
- Mary Graw Leary, Assoc. Prof., Columbus Sch. of Law, Catholic University
- Jill Trumbull-Harris, Ass't U.S. Attorney, N.D. Ind.
- Damon King, Deputy Chief, CEOS, U.S. DOJ

Dealt with Elsewhere

Entrapment:
“The gov’t made me do it.”

Impossibility:
“There was no real child involved in the conversation.”

Some common defenses:
1. Vigilante
2. Public authority
3. Official duties
4. 1st Amend. / Research
5. Internet addiction
6. Insufficient proof of age
7. Accident / Mistake
8. SODDI
9. Computer virus
10. Trojan horse
11. Spyware
12. Worm
13. Open wireless
14. Rootkit
15. Virtual images
1. Vigilante

- **Defense:**
  "I was doing my own undercover work to help law enforcement."

- **Response:**
  - No exception of privilege for non-law enforcement possession, receipt, etc.
  - No exception for police officer acting on own, outside official investigation.

2. Public Authority

- **Defense:**
  "I was authorized to have the images."
  (Allegedly as undercover informant or cooperating suspect)

- **Response:**
  - May NOT obtain or retain images outside clear scope of role
  - E.g., *U.S. v. Parker*, 267 F.3d 839 (8th Cir. 2001)

- **Considerations:**
  - Volume of evidence
  - How was it collected? When? Any distributed?

3. Official Duties

- **Defense:**
  "I was performing my official duties for which I'm immunized by law."
  As defense attorney, for example

- **Considerations**
  - Is atty accessing CP to advise potential client whether it's CP; or possessing it in course of representation, such as per discovery?
  - Even prosecutor may not possess outside official role.
4. First Amendment / Research

- **Defense:**
  “This is research for a book I’m writing.”
  (Writer, reporter, research, psychologist, Pete Townsend)

- **Response:**
  - No First Amendment right to possess
    U.S. v. Matthews, 209 F.3d 338 (4th Cir. 2000)
  - Also, First Amendment Privacy Protection Act (1980) excludes such contraband from protections against search and seizure by law enforcement

- **NOT an affirmative defense**

5. Internet Addiction

- Seems to be fading as a defense
- Not recognized in DSM
- Defense essentially forced to showcase the CP, so it can backfire w/ jury
- _Daubert_ or other hearing may be appropriate to address admissibility
- Argument may be relevant to sentencing

6. Insufficient Proof of Age

- **Defense:**
  “The gov’t failed to prove the models / subjects were minors.”
  “The gov’t did not present sufficient expert proof that the person depicted is a child.”
Proof of Age

- **Considerations:**
  - D’s own statements / admissions
    - To investigators
    - In chats, emails, other communications
  - Identification of the child
    - “local” victim?
  - NCMEC Known Images database

Proof of Age

- Pediatrician’s opinion
- Lay opinion as to age
- Description in file names
- The images themselves
  - Let the jury decide
  - Expert testimony not required

Technical Defenses

(Or mixed legal / technical)
Key Considerations

- Most technical defenses can be refuted by computer forensics
- Was D at computer when crime was committed?
- Is there evidence suggesting that D had knowledge and/or intent?
- Requires thorough time/date analysis of computer and real world events.

Knowledge and Intent Evidence

- Confession / statements of D.
  - Chats or web postings made by D.
  - Explanations given at time of search / arrest
  - Jail calls made by D.
- Efforts by D. to hide / destroy evidence
- D.’s prior admissible convictions or bad acts
- Notes, journals, passwords, CDs / DVDs
- Printouts or albums of CP
- D.’s fingerprints on physical evidence
- D.’s handwriting on physical evidence
- D.’s credit card transactions

Digital Knowledge & Intent Evidence

**Evidence that:**

I. CP files were purposely collected
II. CP was obtained via web browsing
III. CP was viewed by a user
I. Evidence that CP Files were Purposely Collected
   • Was CP found in computer’s allocated space?
   • Was CP located in folders assigned to particular “user” of the computer?
   • Were files organized, given relevant folder / file titles?
   • Default settings of computer software changed?

II. Evidence that CP Obtained via Web Browsing
   • Evidence in the index.dat files of web searches for CP?
   • CP found in temporary Internet files?
   • Any CP related Bookmarks / Favorites saved?

III. Evidence that CP was viewed by a user.
   • Any recent files / link files to the CP?
   • Windows Registry list other devices (scanners, thumb drives, etc.) recently connected to computer?
   • Any thumbs.db files containing CP?
   • Any CP videos listed in Windows Media Player / Real Player histories?
7. Accident / Mistake

• **Defense:**
  
  “I was looking for adult pornography, but child pornography came up.”

  “I did not intend to (did not knowingly) receive (or possess) the images.”

  “I did not intentionally possess the CP found in my cache or temporary Internet files. I didn’t know they were there.”

• “Pop-Up” defense (similar to others.)

---

**What’s on his hard drive?**

---

**Sorted File Names**
“Default” Directories

The “properties” tell all...
Stored Webpages

Keyword search terms used by D.
"lolita," "PTHC," "r@ygold," "incest"

Same images or search terms on multiple computers

Multiple thumbnails from one Web page on one date

Large amount of images and terms on computer

Websites visited on different dates / repeated visits

Stored Accounts

Rebutting Accident / Mistake

(helpful information)

- Keyword search terms used by D.
  "lolita," "PTHC," "r@ygold," "incest"
- Same images or search terms on multiple computers
- Multiple thumbnails from one Web page on one date
- Large amount of images and terms on computer
- Websites visited on different dates / repeated visits
**Rebutting accident / mistake**

- Enlarged images, not just thumbnails
- Images of type that would typically appear in pop-ups OR those that would appear after user clicked on "free trial," "site tour," etc.
- **External evidence**
  - Phone call to warn employer that pornography might be found on work computer

**Rebutting accident / mistake**

- Member in subscription-based (pay) CP sites
- Member of any free sites or newsgroups w/ CP name (found in registry, emails, chats, etc.)
  - Where is CP located on computer?
  - Has D moved or organized files on computer?
  - Did D take steps to delete or report the CP images

**Rebutting accident / mistake defense:**

_Showing knowledge / intent_

- D.'s statements to investigators
- D.'s knowledge:
  - How to delete files
  - How to empty Temporary Internet Files
- Hardcopy printouts of images
- Images on multiple external media
- Labels on media ("hot little girls")
- Handwritten notes, passwords, Usernames, etc.
Rebutting accident / mistake:
Computer forensic evidence

- User created folders (directory structure)
- Hidden folders
- LNK files
  - Shortcuts or pointers to files, folders, URLs, network locations
  - Show image, video, or folder has been opened
  - Documents and Settings\[username\]\Recent contains LNK files pointing to user's Recent files

Index.dat record — Can show Def had viewed downloaded images

Windows Registry artifacts:
Recent MRU (most recently used) — shows subject used certain application to view specific file

E.g., RecentFileList or MostRecentClips can show Windows Media Player or RealPlayer used to view movies downloaded from the Internet
Rebutting accident / mistake:
Computer forensic evidence

SPOOL files:
When user sends a file to printer, a graphics file (EMF) representing each page is created in:

Drive:\windows_directory\System32\Spool\Printers

Thumbs.db files:
- System-generated file snapshots of images, movies, and PowerPoints
- Used to view thumb-nail representations of files in a folder
- Only generated when user requests to see thumb-nail view (or folder is defaulted to that view)
- Stores file name

How Thumbs.db files are Created by Microsoft Windows
Rebutting accident / mistake:
Computer forensic evidence

- Browser download history
- Websited visited
- Chat logs
- Saved passwords
- Screen names
- Bookmarks

Pop-Up defense

- “The image of CP just popped-up on my computer screen.”
- Very common defense
- Easily defeated or verified
- Web activity should be examined
- Look at Search terms & registry info
- Pop-up images will only be in Temporary Internet Cache, not saved elsewhere

Knowledge in P2P cases

- **Defense:**
  - “I accidentally downloaded CP with P2P.”
  - or
  - “I downloaded CP via P2P but did not intend to distribute it.”
- **Considerations:**
  - Was D. the one who installed the software?
  - Did he accept all default settings, or adjust
  - Does he appear to be a sophisticated user who would understand how P2P works?
  - Were adult pornography or obscene files also downloaded? Shared?
8. SODDI

- **Defense:**
  
  “Some Other Dude Did It.”
  
  “It must have been downloaded by my son / father.”

- **Considerations:**
  
  What does a timeline of activity show?
  
  - Download dates/times
  
  - When was D. at computer, or when could he have been?
  
  - When were others on computer?

---

**SODDI**

- Put D. behind the computer at the relevant times

- Did anyone else have access?
  
  - To email, chat programs, P2P, or other key components
  
  - Were the other users computer savvy; did they actually use the accounts involved?
  
  - Did the others have work / school schedules or other commitments that took them away at relevant times?

---

**SODDI**

*How did D. use the computer?*

- Passwords and encryption keys

- Screen names

- Email addresses

- Internet service providers

- P2P programs

- IRC channels

- Remote storage devices used

- Directory and file naming structure
SODDI variation

• “The stuff was on my computer when I bought it.”

• Considerations:
  ♦ Relevant dates
  ♦ Did D. buy computer new?
  ♦ Did D. notice anything unusual on his computer
    ♦ When did he first notice it?
    ♦ Report to police or place of purchase?
  ♦ Did D. copy contents of another computer to the new computer?

9. Computer Virus

_Defense:_ “Something, or someone else is responsible.”

• Malicious code (malware) that can copy itself and infect a computer _without_ the user’s knowledge or permission.

• Can only spread from one computer to another when the host is taken to an uninfected computer

• If network files are infected, it can spread to any computer attached to the network.

_Virus_

• Primarily affect PC’s using Windows operating systems

• Rare on Apple computers or Linux-based computers, but not impossible

• Computers are most commonly infected with a virus when the malicious code is attached to a legitimate application.
Virus: Considerations

- Examine antivirus log files: was AV software regularly updated with new definitions?
- Examine Quarantine logs for evidence of viruses being located and quarantined.
- Detection of a virus but an AV engine does not tell whether the computer was infected or affected by the virus.

Virus: Other Considerations

- Virus can’t place CDs in drive tray
- Virus can’t insert a thumb drive
- Virus can’t plug in external hard drive
- Virus can’t make hand-written notes
- Virus can’t label a CD with a Sharpie

Virus — Forensic evidence:

Show Defendant’s use, knowledge, activities

- Location of stored images (desktop, My Pictures, etc.)
- Browser activity — sites, bookmarks, search terms, typed URLs
- Evidence of viewing / organizing files — LNK files, Thumbs.db
Virus —
Forensic evidence:

Virus analysis by forensic examiner —
• Are viruses present on computer?
• If so, are any of them active
• Are any of the viruses capable of having done the criminal activity?

Virus
Other Evidence:

• Evidence linked to D.’s identity
  Screen name, nickname, email address, Yahoo! ID, etc.
• Links between email, web-browsing, chat logs, images
• Windows Registry
• Evidence of attempts to conceal (e.g., Evidence Eliminator)

10. Trojan Horse Defense

• A trojan horse is a program that looks to be legit, but contains something malicious
• Unlike a virus, it must have user interaction (virus can self-replicate and self-execute)
• Does NOT affect the computer until activated by the user
Main types of Trojan horses:

1. Legitimate software that has been hijacked and code changed by a hacker
2. A program that’s designed to look interesting or useful but is actually malicious

Capabilities of Trojan horses:

- Destroy data
- Enable another to have remote access
- Keylogging
- Downloading
- Re-route Internet Traffic

Trojan horse — Steps in investigation:

- Computer scanned by 1 (or 2) anti-malware engines
- Research and report any Trojans
- Determine when Trojan was introduced to computer
- Research capabilities of Trojan
- Determine when illegal activity was done in relation to when Trojan was introduced
Trojan horses
Considerations / Questions:
• Where was evidence located on computer?
• Was anti-virus software installed on computer? Was it up to date?
• Any activity logs from anti-virus software?
• There have been instances of suspects intentionally installing malware on their computer to embed a defense.

Considerations re: Trojans continued...
• Is the Trojan responsible for the material on the subjects computer?
• Is it an “intentional Trojan horse?”
• Is there evidence that the computer was controlled?
• Is there functionality of the computer even w/ presence of Trojan horse?

11. Spyware:
What is it and what does it do?
• Any piece of software, installed or employed without a user’s knowledge that watches, logs, and reports on the User’s electronic movements
• Can track personal, demographic, and psychosocial information
Spyware:
• Generally designed for commercial gain by exploiting a computer
• Common tactics:
  • Delivery of unsolicited pop-up ads
  • Routing of http requests to advertising sites
  • Changing computer’s homepage
  • Theft of pwnl info
  • Monitoring web browsing activity for marketing
  • Reducing Internet connection speed

Spyware Forensic considerations:
• Most anti-malware tools will detect presence of spyware on a computer
• If spyware is detected, it should be investigated and reported
• Website activity of computer should be examined and compared to search terms, saved favorites, typed URLs, and other evidence

12. Remote Access Defense:
• Remote access accomplished when a person can control a computer via the Internet w/out having physical access to machine
• Several software tools allow this E.g., LogMeIn, GoToMyPC, ShowMyPC
• Some companies use such tools for tech support
• Trojan horses may also have a remote access capability, or a “backdoor.”
Remote Access

- Capabilities dependent on what the remote access software is designed for
- Many allow full control of computer just as if the computer was directly in front of the computer user

Remote access
Forensic Considerations:

- Remote access through a 3rd party tool (LogMeIn, ShowMyPC)
  - software and evidence of that should be found in forensic exam
  - log files and connection date / times also available
- Remote access via Trojan or other clandestine access
  - May or may not be evidence left on the computer
  - Should check Windows Events Logs, general file activity, and Anti-malware scans

13. Worm Defense

- Worm is self-replicating program
- Uses network to send copies of itself to other computers on same network
- Does not need to attach itself to existing program (like a virus)
- Always harms network instead of corrupting files on an individual computer
Worms
Forensic Considerations
• Anti-malware scan should be conducted to look for worms
• Any located worms should be researched and reported
• Worms generally won’t affect a single home computer, but should be looked at in business or network environment

13. Open Wireless Defense
• Wireless Internet allows users to broadcast their Internet connections
• Many wireless routers and access points do not have encryption and security settings turned on by default
• “War Driving” and other issues can result if users leave wireless Internet connections open

Open wireless
Forensic Considerations:
• Some WiFi routers and access points will log connections (generally not by default)
• Investigators should check for presence of wireless Internet devices
• SSID name and encryption settings should also be checked
Open Wireless
Forensic Considerations:
• Police WiFi devices should be disabled during consent searches or warrant executions
• War driving will lead investigators to IP address of the Internet connection, not the suspect's computer
• MAC (Media Access Control) address of suspect’s computer may be in logs of the wireless router
• If suspect computer is found, it may have SSID name of hotspots in the registry

Open Wireless
Considerations:
• Does user have a firewall? If so, was it in place?
• Are suspect images always placed on computer when person is at console?

14. Rootkit Defense
• Rootkit: Malware (including viruses, spyware and Trojans) that hide their presence from anti-malware engines and system management utilities
• Most rootkits are developed to provide a “back door” into the infected computer
Rootkit

- Rootkits can collect information and send it “home” or use the infected computer as a botnet
- Rootkits can also:
  - Capture any data passing through, stored on, or accessed from infected system
  - Log keystrokes
  - Send email on behalf of the attacker

Forensic Considerations

- Forensic examiner should check for malware
- Software such as Rootkit Revealer can be run on the system it’s powered off
- Forensic examiner can create a virtual machine of suspect’s computer and take snapshot of running processes

If suspect says rootkit attack is responsible for CP images on his computer...

- Shouldn’t be typed URLs
- Shouldn’t be a file sharing program in place
- Shouldn’t be emails or chat fragments concerning child exploitation
- Shouldn’t appear that processed occurred only when user/suspect was at the computer
15. Virtual Images – Not Real Child

- “The images were not of real children being abused. They are virtual reality images that I have a right to possess under Ashcroft”
- Similar to “The Government can’t prove it’s a minor” defense

Virtual Child Pornography

- VCP: Computer Generated Images (CGI) of children involved in lewd in lascivious behavior, including sex acts
- CGI means that 100% of the image is computer generated and no part is a real person

“Oh, I made this on my computer...”

Difficulties in creating image of a person:
- correct form, proportions of body
- facial expressions
- color, texture of skin
- interaction of light

Digital imaging experts: Current technology does not allow creation of computer generated images that are indistinguishable from real.
Virtual Child Pornography

Multiple images of same subject make it nearly impossible due to amount of time, skill, equipment and artistic ability it would take to make just one image

New language: “digital / computer image that is or is \textit{Indistinguishable} from a minor”

\begin{itemize}
\item "\textit{Indistinguishable}" – ordinary person would conclude depiction is of actual minor engaged in sexually explicit conduct.
\item Inapplicable to:
\begin{itemize}
\item drawings,
\item cartoons,
\item sculptures,
\item paintings
\end{itemize}
\end{itemize}

\textit{Affirmative defense for most crimes: Image is an adult or not an “actual minor.”}

Proving “real child”

\textit{Realistic CGI videos currently impossible to create:}

\begin{itemize}
\item Standard for US full motion picture is 30 frames per second
\item Each frame must be created by hand
\item All images must be consistent for details and smooth motion
\item Current technology not capable of automatically creating full range of motion
\end{itemize}
Proving “real child”

“Final Fantasy” – 2001 CGI film
- $115 million cost, 4 years to produce with 200 people
- 200 specialized computer workstations
- 93 minute film = 140,000 frames
- 200 people working 4 years = 800 work-years
- Cost of $20,500 per second of video
- Body movement captured by “motion capture” technology

Virtual Child Pornography
Forensic Considerations
- What software is installed on the suspect computer? Any capable of producing such CGI images?
- What format are the images in? JPEG is most common which has a tremendous amount of compression

Proving “real child”
- Identifying the child
- Expert opinion (e.g., pediatrician)
- “Known” image/series (e.g., NCMEC CVIP)
- Images pre-dated CGI technology
- Digital imaging expert
- Letting jury decide—Images speak for themselves
- Number of images
- EXIF data
EXIF Metadata

Easily obtainable by forensic software and some free software

• Extended Image File info embedded by some digital cameras / software
• May include:
  • Make/model/serial number of camera
  • Date/time image made (per camera’s clock)
  • Location where picture taken (if GPS-enabled)
  • Settings
  • Editing software, etc.
• Lack of such data does not mean the image is “virtual”

Proving “real child”

Expert not required: jury can determine

U.S. v. Rodríguez-Pacheco, 475 F.3d 434 (1st Cir. 2007)
U.S. v. Irving, 452 F.3d 110 (2nd Cir. 2006)
U.S. v. Stanina, 359 F.3d 356 (5th Cir. 2005)
U.S. v. Farrelly, 389 F.3d 649 (6th Cir. 2004)
U.S. v. Lacey, 569 F.3d 319 (7th Cir. 2009)
U.S. v. Becht, 403 F.3d 641 (8th Cir. 2005)
U.S. v. Salcido, 506 F.3d 729 (9th Cir. 2007)
U.S. v. Sams, 428 F.3d 945 (10th Cir. 2005)
U.S. v. Kimler, 335 F.3d 1132 (10th Cir. 2003)
U.S. v. Hall, 312 F.3d 1250 (11th Cir. 2002)
Proving “real” child
Expert not required jury can determine

People v. Phillips, 831 N.E. 2d 574 (Ill. 2005)
Peterson v. Commonwealth, 160 S.W. 3d 730 (Ky. 2005)

Review:
You should now be able to:
Describe some of the more common legal and technical defenses raises in technology-assisted crimes against children, such as:

1. Vigilante
2. Public authority
3. Official duties
4. 1st Amend. / Research
5. Internet addiction
6. Insufficient proof of age
7. Accident / Mistake
8. SODDI
9. Computer virus
10. Trojan horse
11. Spyware
12. Worm
13. Open wireless
14. Rootkit
15. Virtual images

and...
recognize and explain the prime legal, investigative, technological, or forensic considerations surrounding such defenses

Questions / Comments?

Priscilla Grantham
pgadams@olemiss.edu
662.915.6929