Chapter 3

TECHNOLOGY AND INVESTIGATION BY LAW ENFORCEMENT IN CHILD PORNOGRAPHY CASES

This chapter explores the manner in which offenders possess and distribute child pornography and the technology that they utilize in the commission of their offenses. It also addresses law enforcement efforts to combat child pornography.

Federal child pornography prosecutions have increased dramatically over the past 18 years. In 1994 and 1995 combined, only 90 federal child pornography offenders were sentenced for possession offenses and receipt, trafficking, or distribution ("R/T/D") offenses.[1] By fiscal year 2011, the number of federal child pornography possession and R/T/D offenders had increased to 1,649.[2] Some of the growth can be attributed to increased resources dedicated to identifying and prosecuting child pornography offenders, but much of the growth is attributable to technological changes that have decreased the cost of production of child pornography and duplication of images and increased the accessibility of child pornography.[3]

Technology also appears to have affected the types of child pornography images that are in circulation and the extent and severity of revictimization that victims suffer through widespread ongoing distribution.[4] At one time it was theoretically possible for a child pornography image to be completely eradicated if all the hard copies were destroyed. In the Internet Age, that has become impossible for images in circulation, as they may spread to thousands of computers shortly after their initial distribution, and "[o]nce a picture has been copied and distributed over the Internet, its further distribution is wholly out of control . . . ."[5]

A. CHILD PORNOGRAPHY OFFENDERS' USE OF TECHNOLOGY TO COMMIT THE OFFENSE

Offenders can now produce, distribute, and access child pornography more easily than in the past. The vast majority of child pornography offenders today use the Internet or Internet-

---

[1] U.S. SENT'G COMM'N, SEX OFFENSES AGAINST CHILDREN: FINDINGS AND RECOMMENDATIONS REGARDING FEDERAL PENALTIES (June 1996) ("1996 Report to Congress") at 29 (citing USSG §§2G2.2 (Trafficking in Material Involving the Sexual Exploitation of a Minor; Receiving, Transporting, Shipping, Soliciting, or Advertising Material Involving the Sexual Exploitation of a Minor; Possessing Material Involving the Sexual Exploitation of a Minor with Intent to Traffic; Possessing Material Involving the Sexual Exploitation of a Minor) & 2G2.4 (Possession of Materials Depicting a Minor Engaged in Sexually Explicit Conduct)).

[2] U.S. SENT'G COMM'N, SOURCEBOOK OF FEDERAL SENTENCING STATISTICS 39 (2011) (Table 17).

[3] *See* PHILIP JENKINS, BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET 15 (2001) (arguing that criminal statistics alone cannot "tell us much about the scale or the geography of electronic trafficking" because they "measure official behavior and nothing more"); U.S. DEP'T OF JUSTICE, NAT'L STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION 11–12 (2010) ("NATIONAL STRATEGY").

[4] *See* Chapter 5 at 112–14 (discussing ongoing victimization).

[5] MAX TAYLOR & ETHEL QUAYLE, CHILD PORNOGRAPHY: AN INTERNET CRIME 9 (2003).

related technologies to access and distribute child pornography.[6] Until the late 1970s and early 1980s, child pornography was difficult to find, risky to produce, expensive to duplicate, and required a secure and private storage area. Advances in photography, computing, and communications technologies have reduced the barriers to child pornography offending.[7]

With respect to production of new child pornography, the "[e]ase of photographic developing, the ready availability of video cameras, and now digital imaging all have had an impact on the nature and availability of child pornography."[8] Indeed, digital technology now allows the average offender to manipulate photos in a variety of ways.[9]

Child pornography offenders can also view thousands of photos and videos from the privacy of their own homes.[10] Many in the law enforcement and research communities believe that the Internet's anonymity nurtures an environment for child pornography offending to

---

[6] The U.S. Department of Justice reports that between 2005 and 2009, U.S. Attorneys prosecuted 8,352 child pornography cases, most of which involved the offenders' use of "digital technologies and the Internet to produce, view, store, advertise, or distribute child pornography." NATIONAL STRATEGY, *supra* note 3, at 11.

[7] *Id.* ("[I]t is evident that technological advances have contributed significantly to the overall increase in the child pornography threat."); Jonathan Clough, *Now You See It, Now You Don't: Digital Images and the Meaning of "Possession,"* 19 CRIMINAL LAW FORUM 205, 206–07 (2008) (digital technology is "relatively cheap, easy to access and use, and portable."). *See also* TAYLOR & QUAYLE, *supra* note 5, at 9 ("Whilst the open commercial sale of child pornography is now no longer tolerated in any Western country, paradoxically the availability of child pornography is easier and in more plentiful supply than ever before. This is because of the Internet."); U.S. GENERAL ACCOUNTING OFFICE, FILE-SHARING PROGRAMS: PEER-TO-PEER NETWORKS PROVIDE READY ACCESS TO CHILD PORNOGRAPHY 2 (2003) ("2003 GAO Report") ("Child pornography is easily accessed and downloaded from peer-to-peer networks."); JENKINS, *supra* note 3, at 3 ("Just how easy it is to find these materials needs to be emphasized. . . . A month or so of free Web surfing could easily accumulate a child porn library of several thousand images."); IAN O'DONNELL & CLAIRE MILNER, CHILD PORNOGRAPHY: CRIME, COMPUTERS AND SOCIETY 36 (2007) ("The Internet brings with it accessibility, affordability and anonymity."); ROBERTA LYNN SINCLAIR & DANIEL SUGAR, INTERNET BASED SEXUAL EXPLOITATION OF CHILDREN AND YOUTH ENVIRONMENTAL SCAN 18 (2005) (same).

[8] TAYLOR & QUAYLE, *supra* note 5, at 43.

[9] Gray Mateo, *The New Face of Child Pornography: Digital Imaging Technology and the Law*, 2008 U. ILL. J.L. TECH. & POL'Y 175, 178 (2008); *cf.* NATIONAL STRATEGY, *supra* note 3, at 11–12 ("Prior to the mid-1990s, Internet access and the availability of digital home recording devices . . . were very limited, thereby confining the production and distribution of child pornography material to relatively few individuals."). The explosion of cheap child pornography can be at least partly attributed to the existence of basic production tools in nearly every Internet-connected household:

> Until recently, the child pornography producer, like any amateur photographer, required a darkroom, chemicals, film, paper, camera equipment, skill, time and privacy. . . . Contrast that with the situation today. For a modest investment, a home PC package contains a computer, scanner, photocopier and printer, often a Webcam and always an internal modem. Software packages for editing photographs and videos come as standard. Add the Internet and access to a child, and the average desktop computer becomes a pornography studio.

O'DONNELL & MILNER, *supra* note 7, at 36.

[10] TAYLOR & QUAYLE, *supra* note 5, at 9 ("The Internet enables the speedy, efficient and above all anonymous distribution of child pornography on a global scale.").

thrive.[11] The "perceived anonymity, the ease of developing social contacts and the capacity to create virtual social groups, [and] its essentially international character and the speed with which digital files can be transmitted creates an environment that challenges conventional notions of social organization and control."[12] Illegal images no longer have to be developed, printed, and shipped; instead, they are digitally recorded and made available for unlimited distribution at virtually no cost.[13]

Before discussing the specific technologies the offenders use, the next section will provide a brief overview of many of the underlying technologies related to the commission of child pornography offenses.

1. *Technology Primer*

The growth of child pornography offending has been facilitated by combined advantages of digital technology and networked computing.[14] Desktop and laptop personal computers, along with many other computerized devices such as smartphones, have several essential features relevant to the discussion of child pornography offending.

a. Internet Connectivity

Digital child pornography is easily shared through Internet-enabled devices.[15] Computer networks have existed (and have been exploited by child pornography offenders) for nearly three

---

[11] *See* NATIONAL STRATEGY, *supra* note 3, at 3 ("The anonymity afforded by the Internet makes the offenders more difficult to locate, and makes them bolder in their actions."); *see also* O'DONNELL & MILNER, *supra* note 7, at 45 ("The Internet . . . allows adults with a sexual interest in children instant access to others who share their proclivity, even if they are thousands of miles apart[,] . . . provides a level of inscrutability that is unattainable in the real world[, and] . . . encourages a culture of impunity.").

[12] Max Taylor & Ethel Quayle, *The Internet and Abuse Images of Children: Search, Precriminal Situations and Opportunity*, 19 CRIME PREVENTION STUDIES 169, 170 (2006); see also *id*. at 169 ("The easy availability of abuse images at low or no cost has both exposed and made possible a degree of sexual interest in children expressed through pornography production and possession that seems to be surprising in its extent.").

[13] JENKINS, *supra* note 3, at 4 ("Prices in the child porn world have not just fallen, they have all but been eliminated."). Unlike traditional photography, digital photography and videography permits costless creation of unlimited identical copies. TAYLOR & QUAYLE, *supra* note 5, at 9 ("The information passed over the Internet that constitutes a picture is a perfect copy of an original, which can be reproduced endlessly without loss of definition or any other qualities.").

[14] *See, e.g.*, YAMAN AKDENIZ, INTERNET CHILD PORNOGRAPHY & THE LAW: NATIONAL AND INTERNATIONAL RESPONSES 8 (2008) (citing "[e]ase of access, the partial anonymity provided by the Internet, developments in digital photography, issues surrounding the difficulty of policing international networks, and the limited risk of detection") (footnotes omitted); Clough, *supra* note 7, at 206–07 (concluding digital technology "allows for storage of large amounts of material which would be conspicuous if stored in hard copy[,] . . . may be produced cheaply and with no need for external processing[,] . . . may be copied with no diminution in quality and distributed easily, in large volumes, with minimal cost and relative anonymity.").

[15] *See* MONIQUE FERRARO & EOGHAN CASEY, INVESTIGATING CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, LAW & FORENSIC SCIENCE 9–10 (2004) (describing the adoption of Internet technologies by child pornography offenders to share and collect images).

decades.[16] An early iteration of networked computing called a bulletin board system (BBS) enabled users to connect to a host computer using a computer modem and ordinary telephone line.[17] Once connected, the user could post messages, interact with other BBS users, or download stories and images for viewing on the user's own computer. Some BBSs were public and free; others were private and charged a fee. They also allowed access to Internet newsgroups, and, eventually, to the World Wide Web ("web"). BBS and Internet newsgroups are still used by some technologically savvy child pornography offenders.[18]

The web (which most people think of when they refer to the "Internet") has in less than 20 years become common in American homes.[19] Today, the early online service providers like America Online that originally served as "web portals" have largely transformed into, or been supplanted by, a host of Internet Service Providers ("ISPs"). ISPs provide direct customer access to the Internet via dial-up telephone, digital subscriber line ("DSL"), broadband, or similar means.[20] ISPs include cable and telephone service providers such as Verizon, Comcast, DirectTV, TimeWarner, and AT&T. An individual home or business user connects to the ISP, which then provides the user with access to the Internet.[21] ISPs have the ability to monitor users' access to some kinds of web content, such as specific websites, where allowable by law.[22]

Once connected to the Internet, individuals often use electronic communication service providers to email, instant messaging, and store online content. Such providers include, among many others, Blogger, Yahoo!, Google, and Snapfish. As part of the Providing Resources,

---

[16] *See* 2003 GAO Report, *supra* note 7, at 6 ("[P]ornographers have traditionally exploited—and sometimes pioneered—emerging communication technologies—from the dial-in bulletin board systems of the 1970s to the World Wide Web—to access, trade, and distribute pornography, including child pornography."); *see* ATTORNEY GENERAL'S COMMISSION ON PORNOGRAPHY: FINAL REPORT 629–630 (1986) (describing child pornography BBS, newsgroups, and stating that "personal computers have instant communication capabilities and have afforded subscribers the opportunity to establish extensive networks."); JENKINS, *supra* note 3, at 41 ("Perhaps ten years before the Internet became known to the general public, computer databases and bulletin boards were becoming the favored tools of child pornographers, a strikingly precocious use of computer technologies."); *see* AKDENIZ, *supra* note 14, at 5 ("Paedophilia networks have been using computer networks [to disseminate digital child pornography] from as early as 1986."); O'DONNELL & MILNER, *supra* note 7, at 29 ("[T]here is evidence that paedophiles have been using computers to communicate since 1982 in the USA and 1985 in the UK.") (internal citations omitted).

[17] *See* NAT'L INST. JUSTICE, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS, SPECIAL REPORT, NCJ 210798 61 (2007) ("Investigations Involving the Internet") (available at https://www.ncjrs.gov/pdffiles1/nij/210798.pdf).

[18] *See, e.g.*, Prepared Presentation of James Fottrell, Child Exploitation and Obscenity Section, Criminal Division Department of Justice, to the Commission (Feb. 15, 2012) (on behalf of the U.S. Department of Justice) ("Fottrell Presentation") (depicting different types of distribution technologies in a three-part triangle of socialization) .

[19] U.S. Census, *Computer and Internet Use*, http://www.census.gov/hhes/computer/ (last visited Nov. 29, 2012) (number of Internet-connected households has climbed from 18% in 1997 to over 70% by 2010).

[20] *See* FERRARO AND CASEY, *supra* note 15, at 86–88.

[21] *Id*.

[22] For example, one UK ISP claimed it "blocked more than 20,000 attempts per day to access child pornography on the Internet" in July 2004. Ethel Quayle & Matthieu Latapy, *Current Situation Regarding Our Knowledge of Paedophile Activity in P2P Networks*, MAPAP — SAFER INTERNET PLUS 1 (2008), http://antipaedo.lip6.fr/Current_situation.pdf (last visited Nov. 29, 2012).

Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008,[23] any ISPs offering online storage of content are mandated to report child pornography that they find on their system to the CyberTipline of the National Center for Missing & Exploited Children ("NCMEC").[24]

b. Digital Storage

Digital storage capacity has grown so that much larger volumes of data can be stored on smaller and more easily transportable devices. Many offenders possess child pornography collections numbering in the hundreds of thousands or even millions of images and videos.[25] When child pornography trading moved online, the traditional physical limitations on the collection and distribution of images and videos were alleviated.[26] Every computer or computerized device includes some type of integrated, permanent storage such as an internal hard drive that digitally stores the operating system, programs, and files.[27] The computer may also come equipped or be compatible with one or more forms of removable storage, such as flash drives, zip drives, CD/DVD drives, secure digital cards, and external hard drives.[28]

Storage capacity is measured in units called "bytes" and multiples of bytes: kilobyte (1,000 bytes, known as a kB), megabyte (1,000,000 bytes, or MB), gigabyte (1,000,000,000 bytes, or GB), terabyte (1,000,000,000,000 bytes, or TB), and beyond. Advances in storage technology have driven the price of storage capacity down so that individuals routinely have access to digital storage libraries in the terabytes.[29] Huge volumes of information can now be

---

[23] Pub. L. No. 110–401, § 501(a); 122 Stat. 4229 (2008) (codified at 18 U.S.C. § 2258A).

[24] U.S. GENERAL ACCOUNTING OFFICE, COMBATING CHILD PORNOGRAPHY: STEPS ARE NEEDED TO ENSURE THAT TIPS TO LAW ENFORCEMENT ARE USEFUL & FORENSIC EXAMINATIONS EFFECTIVE 3 (2011) ("2011 GAO Report") (citing 18 U.S.C. § 2258A). NCMEC is a private, 501(c)(3) nonprofit organization created in 1984. The mission of the organization "is to help prevent child abduction and sexual exploitation; help find missing children; and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them." NCMEC, *National Mandate & Mission*, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1866 (last visited Nov. 29, 2012). NCMEC provides information and resources to law enforcement, parents, and children including child victims as well as other professionals. NCMEC's exploited children division has several programs that work with law enforcement to track child pornography images and identify and rescue child pornography victims where abuse is ongoing. For more information on NCMEC, *see* http://www.missingkids.com. As mentioned herein, NCMEC operates the CyberTipline and is authorized to receive reports of child pornography.

[25] *See e.g.*, Sentencing Memorandum, United States v. Burr, No. 09-cr-308, (D. Or. July 23, 2010), ECF No. 26 at 3–4 (more than one million images); Sentencing Memorandum, United States v. Worman, 07-cr-40 (E.D. Pa. July 30, 2009), ECF No. 208 at 1 (1.2 million images).

[26] *See* NATIONAL STRATEGY, *supra* note 3, at 12 ("Increased home computer storage capacity has enabled many child pornography offenders to store huge collections of images (some containing 1 million) and numerous video files (often 1 hour in length)" and citing example of a Philadelphia defendant in 2007 found with more than 15,000 videos).

[27] FERRARO & CASEY, *supra* note 15, at 81–83.

[28] *See* NATIONAL STRATEGY, *supra* note 3, at 76 (listing the types of media commonly seized during investigations).

[29] *See id*. at 130.

stored easily on small devices — thus one computer hard drive can contain what might otherwise have constituted vast archives of print photographs, magazines, or film negatives.[30]

Computers and computerized devices are able to display digital child pornography and, once downloaded, users may easily store and manipulate the images. Images can be displayed using free, pre-installed software such as Windows Picture Viewer, Windows Media Player, and Windows Movie Maker. The same programs can also perform basic image manipulation (like enhancing, rotating, or cropping images and trimming videos), while more advanced editing can be accomplished with widely available programs such as Picasa, ACDSee, and Adobe Photoshop.

"Cloud computing" is remote digital storage accessed through Internet connectivity. Files are stored "in the cloud" on remote servers maintained by third-party service providers and accessed by users through the Internet. The "cloud" refers to the ability of individuals or customers to access software, files, and storage, without downloading such files or software to their personal computers or data storage systems. [31] Many cloud services will keep a cache of recently accessed documents. Individuals store pictures, videos, and files in the cloud when they use media hosting web sites such as Flickr, Tumblr, or social networking sites to maintain digital photo libraries.[32] Cloud computing has been called "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[33] While cloud computing has been adopted for legitimate consumer and business purposes,[34] it is also relied upon by some child pornography offenders to store digital collections of child pornography remotely.[35] Remote storage "in the cloud" presents unique forensic challenges for law enforcement.

---

[30] *See* FERRARO AND CASEY, *supra* note 15, at 4 ("Computer storage capacity has increased to the point at which a small personal computer hard drive can hold as much information as the United States Library of Congress."); Clough, *supra* note 7, at 206–07; TAYLOR & QUAYLE, *supra* note 5, at 160 ("Unlike hard copies of photographs, images stored electronically . . . take up very little physical space . . . [and] can even be stored electronically at a location both anonymous and distant from the location of the collector's PC").

[31] Vivek Kundra, *Federal Cloud Computing Strategy*, THE WHITE HOUSE, at 4–5 (Feb. 8, 2011), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf (last visited Nov. 29, 2012).

[32] For more information on these services, *see* http://www.flickr.com/, https://www.tumblr.com/, and http://photobucket.com/.

[33] Wayne Jansen & Timothy Gance, *Guidelines on Security & Privacy in Public Cloud Computing (Special Publication 800-144)*, NAT'L INST. OF STANDARDS AND TECHNOLOGY, at vi (Dec. 2011) (available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494).

[34] *See, e.g.*, Vivek Kundra, *supra* note 31; Steve Lohr, *The Business Market Plays Cloud Computing Catch-Up*, N.Y. TIMES (Apr. 14, 2011) (available at http://www.nytimes.com/2011/04/15/business/15cloud.html?pagewanted=all).

[35] Audrey Rogers, *From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws* 22 (Feb 16, 2012) (available at http://ssrn.com/abstract=2006664).

c. Hash Values

The content of any digital file (including child pornography) can be summarized as a unique identifier through a process called "hashing."[36] The term "hash value" refers to the use of mathematical hash functions that return a value in the form of a relatively short, single number of about 38 hexadecimal (or base 16 numeral system) digits. These resulting hash values are easily managed by computers and investigators alike for verifying that two copies of a file are, in fact, the same, even if the filename or certain other attributes (such as the date it was last accessed) are changed.[37] This process is akin to the way a bookseller can compare a bar code on two different copies of a book to ensure that they are both the same version even if they have different covers.

NCMEC and law enforcement keep a record of the hash values of known child pornography images. These hash values of known child pornography images may be used to search and identify files on an offender's computer, or other digital storage devices, as child pornography without having to view the images themselves.[38] Hash values can easily be changed to avoid this forensic hashing function by slightly manipulating the digital images, but many child pornography offenders do not change the hash value of child pornography images,[39] in part because the hash value is important to programs that facilitate searches for, and distribution of, child pornography.

2. *Internet Technologies Used to Access Child Pornography*

Some child pornography offenders have been at the forefront of technological advancement in the Internet Age. Although child pornography today "is available through virtually every Internet technology,"[40] the rapidly evolving nature of the Internet renders impossible any definitive attempt to describe the technology used in current child pornography offenses. It is important to note that technologies associated with Internet child pornography continue to develop quickly. Any attempt to describe the current state of technology in child pornography offending may be dated in only a short period of time.[41]

---

[36] *See* FERRARO AND CASEY, *supra* note 15, at 197.

[37] *Id.*

[38] *See* Jaap Haitsma, Ton Kalker & Job Oostveen, *Robust Audio Hashing for Content Identification*, CONTENT-BASED MULTIMEDIA INDEXING 1 (2001); FERRARO & CASEY, *supra* note 15, at 197 (describing an algorithm used to conduct a hashing function). All digital files can have hash values.

[39] Robert J. Walls et al., *Effective Digital Forensics is Investigator-Centric*, PROC. USENIX WORKSHOP ON HOT TOPICS IN SECURITY (HotSec), at 4 (Aug. 2011).

[40] 2003 GAO Report, *supra* note 7, at 6–8 (discussing commercial or trading websites, e-mail, Usegroups/newsgroups, FTP, IRC/Chat, Gigatribe, and live streaming); *see* NATIONAL STRATEGY, *supra* note 3, at 11–12.

[41] For example, more child pornography offenders are using their smartphones to access and trade images such that "the tools of the trade are now pocket-sized and the search for child pornography can be carried out anywhere, any time." O'DONNELL & MILNER, *supra* note 7, at 63. Almost half of all Americans own a smartphone that features Internet connectivity. Aaron Smith, *46% of American Adults are Smartphone Owners*, PEW INTERNET PROJECT, at 2

a. Peer-to-Peer File Sharing

Peer-to-peer file sharing, commonly called "P2P," refers to a software program or application that enables computers to share files easily over the Internet. Computers connected through use of the same P2P software are deemed part of the same P2P network. Dozens of P2P networks exist and the software is widely available on the Internet via a simple search or at mainstream downloading websites.[42] P2P networks "allow. . . people across the world to connect directly to each other's machines without having to use a third-party."[43] In other words, rather than posting an image on a website for others to download, P2P file sharing lets two or more users swap files directly with one another. P2P networks came to prominence in the late 1990s with the software Napster, which at its peak allowed 80 million users to swap music files with one another. Napster which maintained centralized servers with lists of connected users and files to facilitate transfers, was enjoined in 2001 from engaging in conduct that would contributorily or vicariously infringe copyrights held by the plaintiff record companies.[44] Other P2P networks faced similar legal challenges and are now by legal decree defunct or have transformed themselves into legitimate business enterprises.[45]

Unlike Napster, today's P2P networks operate without the use of centralized servers to connect users, maintain lists of shared files, or monitor for copyrighted or illegal content. Therefore, no single entity is responsible for the content being shared at any given time.[46] P2P networks share all types of digital content, including software, text, movies, and pictures.[47] The

---

Mar. 1, 2012) (available at http://pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf). That is an 11% increase from May 2011 when 35% of Americans reported that they owned a smartphone. That number is even higher for those ages 18–29, of whom 66% own a smartphone. *Id.* Smartphones enable a child pornography user to capture new images, download existing images, and trade images as described below, all from his phone. Additional research suggests that at least among some populations, smartphones are being more frequently used for distribution of newly produced child pornography images. Janis Wolak, David Finkelhor, & Kimberly J. Mitchell, *Trends in Arrests for Child Pornography Production: The Third Nat'l Juv. Online Victimization Study (NJOV-3)*, http://www.unh.edu/ccrc/internet-crimes/papers.html, at 3 (2012) (last visited Nov. 30, 2012).

[42] O'DONNELL & MILNER, *supra* note 7, at 39–40.

[43] *Id*.

[44] *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1099 (9th Cir. 2001) (affirming district court's preliminary injunction and shutdown order).

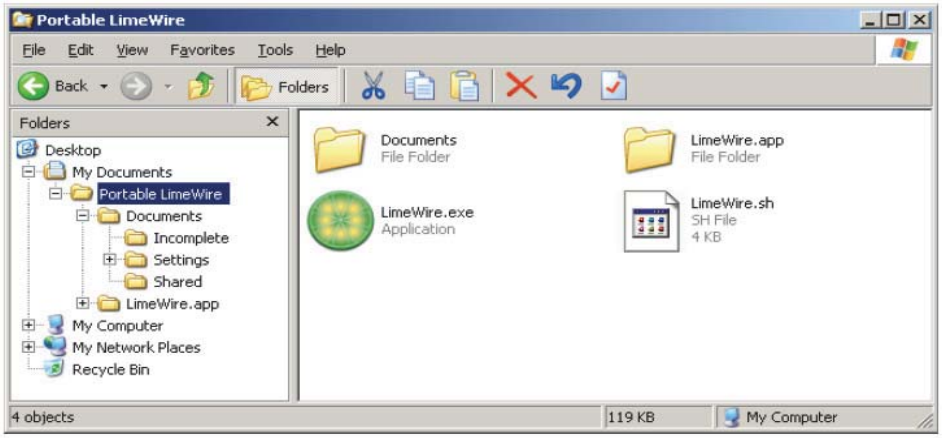
[45] LimeWire, one of the most popular P2P programs used by child pornography offenders in recent years, was ordered shut down in October 2010 pursuant to a stipulated consent order. *See* Arista Records LLC v. LimeWire LLC, No. 06-Civ-05936 (KMW) (S.D.N.Y. Oct. 27, 2010). And several other popular P2P clients like iMesh, BearShare, and KaZaA, have been transformed into legal subscription music sharing services. *See*, *e.g.*, http://www.bearshare.com/ (last visited Oct. 12, 2012); http://www.imesh.com/ (last visited Oct. 12, 2012) (offering "access to over 15 million songs and videos — All legal and free!"); http://www.kazaa.com/ (last visited Oct. 12, 2012) (permitting "download of 15 million songs and videos all legal and free!"). Nevertheless, versions of the LimeWire software remain in use and many individuals continue to share files on LimeWire-enabled networks.

[46] *See* Sgt. Josh Moulin, National District Attorneys Association, *What Every Prosecutor Should Know About Peer-to-Peer Investigations*, UPDATE: CHILD SEXUAL EXPLOITATION PROGRAM 1 (2010).

absence of a central authority and easy accessibility to images have attracted child pornography offenders to P2P networks.

P2P file sharing typically works as follows: initially, the user downloads a software program onto his own computer or Internet-enabled device that permits the individual to share and download files from the P2P network. Upon installation, the software typically creates two folders on the user's computer by default: an "incomplete" folder, which contains pending downloads, and a "shared" folder, which contains fully downloaded files. This is seen below in Figures 3-1 and 3-2, which are screenshots of LimeWire. As indicated by its name, any files downloaded to, or other files placed in, the shared folder are immediately made available for sharing with all other users on the P2P network.[48]

Figure 3-1[49]
Federal Defender Technology Presentation: Screenshot of LimeWire

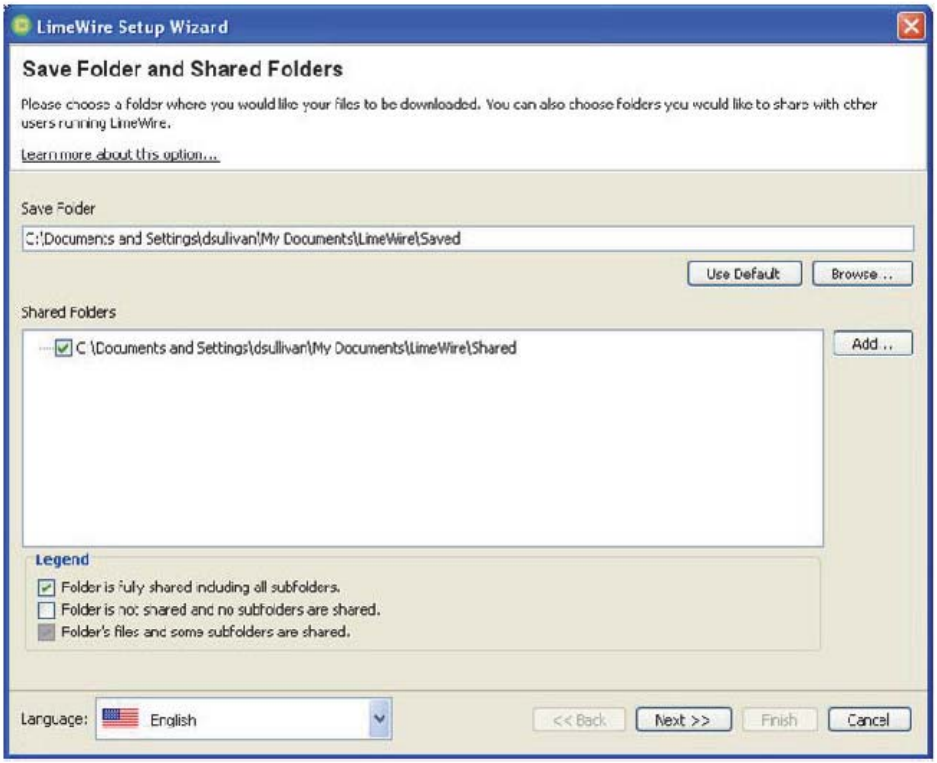


[47] *See* Terrence Berg, *The Changing Face of Cybercrime: New Internet Threats Create Challenges to Law Enforcement*, MICHIGAN BAR JOURNAL 18–19 (June 2007) ("The P2P networks . . . are tailor-made for sharing digital media of any kind; by downloading the P2P client software, each user's designated collection of digital files becomes accessible by every other user, in a privately created network.").

[48] Moulin, *supra* note 46, at 2.

[49] Prepared Presentation of Gerald R. Grant, Digital Forensics Investigator, Office of the Federal Public Defender, Western District of New York, to the Commission (Feb. 15, 2012) ("Grant Presentation").

Figure 3-2[50]
Federal Defender Technology Presentation: Screenshot of LimeWire Shared Folders



In addition to files manually placed in the shared folder, a user is usually asked upon installation to indicate whether he would like to share any files already present on the computer. If the answer is yes (*i.e.*, the user "opts in"), the software automatically scans the user's computer or any designated shared part thereof (often using a hashing function to identify and label files) and then compiles a list of files to share. Open file sharing is typically a default setting; however both downloading locations and sharing options may be changed by users to limit which, if any, files are available for sharing (*i.e.*, users may "opt out" of file-sharing).[51] After downloading and setting up P2P software, the user can begin searching for files shared on the connected network using search keywords associated with child pornography, in the same way one regularly uses a search engine such as Google.[52] In short, a user who downloads a P2P network application typically has an ability to control the extent to which that user's files are shared.

---

[50] *Id.*

[51] *See* Darren Gelber, *Cybercrimes: File-Sharing Programs Violating Copyright and Child Pornography Distribution Laws*, 255 N.J. LAWYER 66, 68 (Dec. 2008).

[52] *See* Giannina Marin, *Possession Of Child Pornography: Should You Be Convicted When The Computer Cache Does The Saving For You?*, 60 FLA. L. REV. 1205, 1210–11 (2008) ("Common child pornography-related Internet

P2P networks are common. In 2011, it was estimated that 57 percent of global Internet traffic was P2P traffic.[53] The very existence and purpose of P2P networks is to share digital content, and there is an active academic and community-level discourse criticizing P2P users who download but do not share.[54] Some P2P networks encourage sharing by offering faster download for sharers or even mandate sharing in some circumstances.[55]

Well known P2P networks include FrostWire, LimeWire, KaZaA, eDonkey, and isoHunt. Of P2P networks, LimeWire in particular was utilized in the recent past by a large percentage of federal child pornography offenders to access and distribute child pornography[56] but other research suggests that isoHunt and other networks are now more commonly used.[57] Although data on the number of users in each network is unavailable, many experts agree that P2P file sharing is widely used to download child pornography.[58] Two major enforcement investigations have revealed substantial illegal P2P trading activity in recent years.[59] Using special software, these two initiatives identified over 20 million unique IP addresses offering child pornography

---

search terms include 'illegal, preteen, underage, lolita, kiddy, child, and incest.' These terms specifically refer to child pornography and differ from terms associated with adult pornography.") (internal footnotes and quotations omitted and formatting modified).

[53] *See* Jeremy Prichard, Paul A. Watters, & Caroline Spiranovic, *Internet Subcultures & Pathways to the Use of Child Pornography*, 27 COMP. L. & SEC. REV. 585, 589 (2011).

[54] *See* Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, 5 FIRST MONDAY (2000), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/124 (last visited Nov. 30, 2012) (noting that individuals who download but do not share "free ride on the efforts of others" which "leads to degradation of the system performance and adds vulnerability to the system").

[55] *See* Bram Cohen, *Incentives Build Robustness in BitTorrent*, May 22, 2003 Workshop on Economics of Peer-to-Peer Systems (2003), http://www2.sims.berkeley.edu/research/conferences/p2pecon/papers/s4-cohen.pdf (last visited Nov. 30, 2012).

[56] *See* Chapter 6, at 154–55 (providing data from the Commission's 2010 coding project regarding use of P2P). Federal lawsuits brought by the recording industry have enjoined LimeWire from distributing software. *See* Arista Records, LLC v. Lime Wire, LLC, No. 06 Civ. 05936 (S.D.N.Y. Oct. 27, 2010). LimeWire settled these lawsuits in 2011 and 2012. *See* Ben Sisario, *Digital Notes: Indies Settle With LimeWire, and Kim Dotcom Speaks Up*, Media Decoder Blog, N.Y. TIMES (Mar. 1, 2012) (available at http://mediadecoder.blogs.nytimes.com/2012/03/01/digital-notes-indies-settle-with-limewire-and-kim-dotcom-speaks-up/); Ben Sisario, *Major Record Labels Settle Suit With LimeWire*, Media Decoder Blog, N.Y. TIMES (May 12, 2011) (available at http://mediadecoder.blogs.nytimes.com/2011/05/12/major-record-labels-settle-suit-with-limewire/). Nevertheless, "pirated" LimeWire software continues to exist and may be downloaded for free from many websites.

[57] Prichard et al., *supra* note 53, at 589.

[58] Ryan Hurley et al., *Measurement & Analysis of Child Pornography Trafficking on Gnutella & eMule*, TECH. REP. UM-CS-2012-016 13 (May 2012) (available at https://web.cs.umass.edu/publication/docs/2012/UM-CS-2012-016.pdf) ("CP trafficking over p2p networks is widespread"); Berg, *supra* note 47, at 19; Quayle & Latapy, *supra* note 22, at 2 ("Many studies show that a large amount of paedophile and harmful contents are distributed using P2P file exchange systems, and that volume of such exchanges is increasing.").

[59] Operation Fairplay was created in 2006 and supported by both the Wyoming Division of Criminal Investigations and the Palm Beach County (FL) State's Attorney's Office; Operation Roundup was developed in 2009 by the University of Massachusetts under a grant from the National Institute of Justice. *See* NATIONAL STRATEGY, *supra* note 3, at 12.

over P2P networks from 2006 to August 2010.[60] The typical offender may make dozens or hundreds of images available.[61]

Other research has largely confirmed the law enforcement findings. A 2011 study found that three terms associated with child pornography ("lolita," "PTHC,"[62] and "teen") were among the top searched terms on the isoHunt P2P network over a six month period in 2010.[63] A study from 2009 found that approximately one percent of queries on the Gnutella network were child-pornography-related, and that the most commonly searched-for term on the network, accounting for 0.2 percent of all searches, was "PTHC".[64] A 2006 study found that every day there were approximately 116,000 requests on the Gnutella P2P network for the term "child pornography."[65]

Traditional open P2P file sharing, as described above, permits "impersonal" sharing of files. Once an individual downloads the software and chooses to permit the network to share his files, he usually exercises no control over to whom the files are shared or how many times they are shared. He is, in effect, leaving a virtual door open on his computer and permitting individuals to copy any files they wish any time the software is running.[66] Impersonal distribution involves "offenders operating alone without direct contact with other[s]"[67] and not requiring specific directed action to share child pornography beyond installing the software, choosing to permit sharing of the user's files, and running the P2P network.[68]

---

[60] NATIONAL STRATEGY, *supra* note 3, at 12 (noting Operation Fairplay has 170,000 files on its "watch list" while Operation Roundup has 120,000).

[61] *See id.* at 13.

[62] PTHC stands for "pre-teen hardcore," a term associated with child pornography.

[63] Prichard et al., *supra* note 53, at 593.

[64] *See* Chad M.S. Steel, *Child Pornography in Peer-to-Peer Networks*, 33 CHILD ABUSE & NEGLECT 560, 560–61 (2009) (noting that 1.45% of search results on the network, or 2,770 uniquely named files, constituted child pornography; 7% of all sharing hosts, or 464 computers, shared child pornography; and 3% of all searching hosts, or 564 computers, sought child pornography). While these may seem like a small numbers, bear in mind that an individual could type *any* term into Gnutella based P2P networks searching for any song, software, celebrity image, movie, or television program.

[65] O'DONNELL & MILNER, *supra* note 7, at 40.

[66] The United States Court of Appeals for the Tenth Circuit has analogized such an "open" P2P network to a self-serve gas station, stating that a defendant who used an open P2P program:

> may not have actively pushed pornography on [P2P] users, but he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items. It is something akin to the owner of a self-serve gas station . . . . Just because the operation is self-serve, or in [the defendant's] parlance, passive, we do not doubt for a moment that the gas station owner is in the business of "distributing," "delivering," "transferring" or "dispersing" gasoline; the *raison d'etre* of owning a gas station is to do just that.

United States v. Shaffer, 472 F.3d 1219, 1223–24 (10th Cir. 2007).

[67] Testimony of James Fottrell, Child Exploitation and Obscenity Section, Criminal Division, Department of Justice, to the Commission, at 25 (Feb. 15, 2012) (on behalf of the U.S. Dep't of Justice) ("Fottrell Testimony").

[68] Testimony of Gerald R. Grant, Digital Forensics Investigator, Office of the Federal Public Defender Western District of New York, to the Commission, at 39–40 (Feb. 15, 2012) ("Grant Testimony"); Testimony of

P2P networks have continued to evolve and newer P2P networks incorporate more sophisticated features, some of which are described below such as "chat" and "social networks." These networks, such as Gigatribe or OneSwarm, can operate as "closed" P2Ps when compared to "open" P2P networks such as the early iterations of LimeWire.[69] Gigatribe and others allow individuals to create their own private networks to which the individual can invite or remove "friends" as well as decide which specific files to share and with whom.[70] As these networks are closed communities of individuals they are sometimes called "friend to friend" or "F2F" as opposed to P2P.[71] Invited users may browse, search for, and download files in their network and chat with other users, all while relying on encryption and relative anonymity to protect themselves from identification.[72] Gigatribe is rapidly growing in popularity and advertises itself as "private, secure, unlimited file sharing software."[73] Gigatribe and its progeny require more personal involvement of the offender who selects which files to distribute and to whom. "Personal" distribution involves some type of directed action — either direct communication (*e.g.*, "closed" P2P technologies Gigatribe, emailing or instant messaging) or sharing images in a specific Internet forum specifically devoted to child pornography (*e.g.*, a child pornography "chat-room").

b. Other Internet Technologies

Another Internet technology used by child pornography offenders are chat rooms, particularly those utilizing "internet relay chat" or IRC. Chat rooms are real-time chatting environments organized into channels — virtual "rooms" — based on specific interests.[74] Some channels may offer services other than text-chatting, such as live video.[75] Chat environments today are largely non-commercial. IRC is one popular example of a non-commercial chat room service that allows users to join one of hundreds of thousands of different group-chat channels.

Brian Levine, Ph.D. Professor of Computer Science, University of Massachusetts, Amherst, to the Commission, at 51 (Feb. 15, 2012).

[69] United States v. Sawyer, 786 F. Supp. 2d 1352, 1355–56 (N.D. Ohio 2011) (noting that Gigatribe is "a 'closed' peer-to-peer file sharing program . . . that is slightly different from . . . 'open' programs" such as LimeWire); United States v. Ladeau, No. 09-40021-FDS, 2010 WL 1427523, at *1 (D. Mass. Apr. 7, 2010) (describing the private nature of Gigatribe).

[70] *See* United States v. Sawyer, 786 F. Supp. 2d 1352, 1354 (N.D. Ohio 2011); United States v. Ladeau, No.09-40021-FDS, 2010 WL 1427523, at *1 (D. Mass. Apr. 7, 2010) (describing Gigatribe in context of denial of motion to suppress evidence seized based on search after investigator downloaded files from defendant's Gigatribe account).

[71] *See, e.g.*, *About OneSwarm*, http://www.oneswarm.org/about.html (last visited Nov. 30, 2012) (describing the benefits of a F2F system).

[72] *See Ladeau*, 2010 WL 1427523, at *1.

[73] *See* Gigatribe homepage, http://www.gigatribe.com/en/home (last visited Nov. 30, 2012).

[74] O'DONNELL & MILNER, *supra* note 7, at 38; TAYLOR & QUAYLE, *supra* note 5, at 122–23 (describing chat rooms).

[75] JENKINS, *supra* note 3, at 78 (describing the live stream activities of a pedophile group).

IRC channels are sometimes self-policed by moderators who control membership and monitor channel activity.[76] Channels may be open to anyone or private.

Newsgroups are another sharing modality.[77] Newsgroups allow non-real-time discussion groups that are "basically discussion forums" allowing people to post messages and read and respond to messages others have posted.[78] In addition to text messages, pictures and other files can be posted directly on newsgroups or shared via e-mail to other trusted newsgroup posters.[79] The largest and most prominent newsgroup system is Usenet, which carries thousands of groups.[80] A critical feature of Usenet is that it is not owned or run by any central authority; instead, "[a]lmost anyone can read the contents of a Usenet newsgroup, create new newsgroups or contribute to an existing one" and a new group joins Usenet "simply by finding any existing site that is willing to pass along a copy of the collection of messages it receives."[81] Web-based bulletin boards, often called Internet forums, serve a function similar to Usenet newsgroups but exist on web servers rather than on a Usenet.[82]

Note that newsgroups or bulletin boards dealing with child pornography may serve functions other than the simple sharing of illicit images and videos. For example, many may not themselves host child pornography but instead periodically post information about accessing private trading groups or provide links to anonymous caches of child pornography shared temporarily on free hosting websites.[83]

The social-networking websites Facebook, BlackPlanet, and FetLife, among others, are websites that combine many of the features of the aforementioned technologies by allowing users an opportunity to meet, chat in real-time or on bulletin boards, and sometimes share files.[84]

---

[76] TAYLOR & QUAYLE, *supra* note 5, at 122–23.

[77] Newsgroups at one time were probably the largest source of child pornography on the Internet and may still be, although new evidence suggests that online offenders have increasingly turned to chat and P2P. AKDENIZ, *supra* note 14, at 6 ("In terms of its availability and modes of distribution on the Internet, the problem of child pornography appears to be one that exists mainly within newsgroups . . . ."); Taylor & Quayle, *The Internet and Abuse Images of Children*, *supra* note 12, at 188 ("The Usenet newsgroup network is one of the major sources of abuse images of children on the Internet.").

[78] O'DONNELL & MILNER, *supra* note 7, at 37–38 ("Participants . . . contribute to discussions by posting messages to the group and returning later to see what, if any, response to their observations have been elicited."); *see* FERRARO & CASEY, *supra* note 15, at 31–33.

[79] O'DONNELL & MILNER, *supra* note 7, at 37–38; Taylor & Quayle, *The Internet and Abuse Images of Children*, *supra* note 12, at 188 ("Individuals post material to these newsgroups in the form of digital files, which are essentially like email attachments, and subscribers to that newsgroup can download these files.").

[80] TAYLOR & QUAYLE, *supra* note 5, at 122.

[81] *Id.* (noting that "[t]his in turn makes the Usenet a different social space from that which is possible in the offline world.").

[82] JENKINS, *supra* note 3, at 64.

[83] *See id.* at 67–69 (describing how "bulletin boards permit porn sites to exist and be used on a purely transient and anonymous basis."); *see also* United States v. McGarity, 669 F.3d 1218, 1230 (11th Cir. 2012) (discussing the method by which a closed child pornography trading group posted images for its members).

[84] *See* http://www.facebook.com/; http://www.blackplanet.com/; http://www.fetlife.com/.

Private social networks like ning.com and bigtent.com share most of the same features of their larger public counterparts but allow users to participate in private and by invitation-only to interact with one another and share files securely.[85] Child pornography offenders may utilize the infrastructure of such existing social networks to develop a community in which to distribute images.

Child pornography is also available via commercial Internet websites.[86] Although commercial child pornography websites exist, it is difficult to judge the number and proportion of commercial sites because of their transitory nature as well as the limited law enforcement resources dedicated to policing them.[87] Most of the commercial sites appear to be associated with either the United States or Russia.[88] In addition, there are websites which purport to offer "child model" images. These sites usually do not directly host illegal child pornography and instead typically feature sexualized images of children that straddle the standards for legality.[89] Nevertheless, as discussed in Chapter 4, some child pornography offenders, particularly pedophilic offenders, collect these sexualized child modeling images.[90]

---

[85] *See* Ning, http://www.ning.com; BigTent, http://www.bigtent.com.

[86] O'DONNELL & MILNER, *supra* note 7, at 36. Jenkins discusses the transitory manner that child pornography can be anonymously posted and then information about where one goes to get the images or the codes to unlock the images can be distributed within the online community. *See* JENKINS, *supra* note 3, at 67–69. An Internet user not associated with the online community would have little ability to find or stumble upon the child pornography because he would not know the URL; *see also* United States v. McGarity, 669 F.3d 1218, 1230 (11th Cir. 2012) (discussing the complicated security measures taken by a sophisticated child pornography group to ensure that no one outside the group would be able to access and view the child pornography postings).

[87] AKDENIZ, *supra* note 14, at 6 (noting that "the true nature [of child pornography] over the World Wide Web can only be speculated upon"). For example, the U.S. Immigration and Customs Enforcement estimates the number of *commercial* sites active at any given time at about 250, although many are short-lived and are available for less than 100 days. *See* NATIONAL STRATEGY, *supra* note 3, at 25–26. The UK-based Internet Watch Foundation reported that it received around 40,000 complaints to its Hotline in 2009, which led them to almost 9,000 child pornography URLs across 1,316 different domains. *See* INTERNET WATCH FOUNDATION, 2009 ANNUAL AND CHARITY REPORT 15, 17 (2009), http://www.iwf.org.uk/assets/media/annual-reports/IWF%202009%20Annual%20and%20Charity%20Report.pdf (last visited Nov. 30, 2012) ("This sort of detailed analysis is helpful in judging the scale of the problem, that is, 38,173 total reports processed; 8,844 confirmed child sexual abuse URLs; 461 identifiable brands being run as businesses to profit from the sexual abuse of children.").

[88] Quayle & Latapy, *supra* note 22, at 2 (citing Internet Watch Foundation statistics from 2007 showing 82.5% of websites linked to U.S. or Russia, up from 67.9% in 2005); *see also* International Watch Foundation, OPERATIONAL TRENDS 2011, http://www.iwf.org.uk/resources/trends (last visited Nov. 30, 2012).

[89] A large-scale prosecution for sexualized child modeling websites occurred in Alabama. Three co-conspirators and a corporation were convicted. One offender possessed child pornography on his computer in addition to his involvement with the child modeling site, another offender pleaded to money laundering, and the third was both a photographer of sexualized child images and hosted a child modeling website. *See* Sentencing Memorandum, United States v. Pierson, 05-cr-00429, ECF No. 22, at 1-2 (N.D. Ala. Feb. 7, 2011); *see also* Declan McCullagh, *Federal Case May Redefine Child Porn*, CNET, (Nov. 30, 2006), available at http://news.cnet.com/Federal-case-may-redefine-child-porn/2100-1030_3-6139524.html (last visited Nov. 30, 2012) (discussing the unusual nature of the prosecution).

[90] *See* Chapter 4 at 83–84.

Child pornography offenders also may trade images directly with one another through email, instant messenger services, webcasting, and videostreaming.[91] Webcasting and videostreaming are ways to watch content such as television programming without downloading the files directly.[92] Content may be webcast "live" or streamed as video after it occurs. Popular ways to stream legal video content include Hulu and Amazon Instant Video, both of which permit individuals to watch television shows and movies on Internet-enabled devices.[93] Webcasting has been associated with some adult pornography websites for years but research indicates that child pornography is now being streamed live as well, which allows users to witness and sometimes direct specific sex acts while leaving less evidence because files are not saved on the viewer's computer.[94] Webcasting enables child abusers to "provide a live broadcast of their abuses and have been known to take special orders as to what types of events offenders will pay to view."[95]

3. *Technology Child Pornography Offenders Use to Evade Detection and Prosecution*

Because of the illicit nature of the trade, child pornography offenders have learned to harness various technologies to evade law enforcement detection and to lessen the likelihood of successful prosecution if caught.[96] Most of the means of identity protection and safeguarding data as discussed below have legitimate uses; however, when used by child pornography offenders to avoid law enforcement investigation or prosecution, they present certain challenges.

a. Obscuring Identity or Location

An offender may attempt to prevent authorities from discovering his true identity by employing simple techniques like not downloading child pornography using a computer or account associated with his residence or workplace. In particular, he may make his identity untraceable by downloading from free or public wireless local area (Wi-Fi) networks at places like libraries, airports, and coffee shops, or by logging on to unsecured Wi-Fi networks in nearby private residences.[97] Because some commercial websites and Usenet providers require users to

---

[91] *See* FERRARO & CASEY, *supra* note 15, at 23–24, 33–37.

[92] Carol A. Lin, *Webcasting Adoption: Technology Fluidity, User Innovativeness, and Media Substitution*, 48 J. OF BROADCASTING & ELECTRONIC MEDIA 446, 446–47 (2004). Webcasting typically refers to a visual content that is being shown "live," however, webcasts may also be recorded and streamed as video.

[93] *See* Hulu, *More About Hulu*, http://www.hulu.com/about (last visited Nov. 30, 2012); Amazon, *Setting up and Watching Amazon Instant Video on Your TV*, www.amazon.com/gp/video/ontv/faq/ (last visited Nov. 30, 2012).

[94] NATIONAL STRATEGY, *supra* note 3, at 23–24 ("Offenders also increasingly access streaming web cam video to view victims in real time without actually producing or storing images or videos that could later be discovered by law enforcement.").

[95] SINCLAIR & SUGAR, *supra* note 7, at 20.

[96] O'DONNELL & MILNER, *supra* note 7, at 165 ("Even narrowly targeted surveillance is problematic on account of the easy availability of advanced encryption software and private communication channels. . . . A forensically aware offender will be difficult to catch and even a naïve one will take time to prosecute successfully.").

[97] NATIONAL STRATEGY, *supra* note 3, at 23. A study of child pornography offenders arrested in 2006 found that 77% mainly used computers at home, 3% mainly used work computers, and 19% used computers in other places,

pay for access (and thus risk law enforcement detection), many use alternative or anonymous payment methods such as digital currencies to disguise their identities.[98] Many digital currencies such as Bitcoin were created with privacy in mind and are virtually untraceable.[99] Other users may buy access to child pornography using stolen credit cards.[100]

Other offenders may access the Internet from home but attempt to mask their online identities. Every device connected to the Internet is assigned an "Internet Protocol" (IP) address that can theoretically be used by law enforcement to identify the computer and, by extension, the individual using the computer. Savvy offenders may use various techniques to disguise their IP addresses and avoid being identified.[101] For example, a proxy server is a website that acts as an intermediary between a user's computer and another computer, allowing an offender to search for or access child pornography material and, in so doing, display the other computer's proxy server's IP address rather than the offender's.[102] An investigator then has to go through an additional legal process to recover the true IP address from the proxy server, a task that is often impossible if the proxy server fails to keep accurate logging information, or, as is often the case, fails to keep identifying information at all.[103] Through a process of proxy relaying, web administrators can make their websites appear as though they are located in a foreign country, leading local investigators to focus on websites that appear to be hosted in their own jurisdictions.[104]

---

including laptops. Janis Wolak, David Finkelhor & Kimberley Mitchell, *Child Pornography Possessor: Trends in Offender and Case Characteristics*, 23 SEXUAL ABUSE 22, 32 (2011).

[98] NATIONAL STRATEGY, *supra* note 3, at 24 ("To further shield their identities, offenders occasionally will deviate from the common use of traditional credit cards and rely on digital currencies and prepaid credit cards to conceal transactions."); JENKINS, *supra* note 3, at 56–57.

[99] For more information on Bitcoin *see* http://www.weusecoins.com/questions.php.

[100] Wade Luders, *Child Pornography Web Sites: Techniques Used to Evade Law Enforcement*, FBI LAW ENFORCEMENT BULLETIN 17, 18 (July 2007).

[101] Brian Neil Levine & Clay Shields, *Hordes: A Multicast Based Protocol for Anonymity*, 10 J. OF COMPUTER SECURITY 3, 4 (2002).

[102] *See* NATIONAL STRATEGY, *supra* note 3, at 23, n.39 ("A proxy server is a computer system or an application program that acts as a go-between for requests from clients seeking resources from other servers."); Eric R. Diez, Comment, *"One Click, You're Guilty": A Troubling Precedent for Internet Child Pornography and the Fourth Amendment*, 55 CATH. U. L. REV. 759, 786 (2006) ("[C]hild pornographers routinely use protective measures such as anonymous proxy servers to eliminate 'digital fingerprints' in cyberspace."); Luders, *supra* note 100, at 18 (explaining that proxy servers are free and easy to use, require no identifying information, are often located in other countries, and keep no logs or other identifying information at all.).

[103] *See* NATIONAL STRATEGY, *supra* note 3, at 23, n.40 ("[T]here is no federal statute or regulation requiring providers to keep user IP information for any length of time, or at all.").

[104] Luders, *supra* note 100, at 20 (noting that because so-called redirect servers "have the outward appearance of being located in another country . . . law enforcement agencies often elect to use their investigative resources to find sites obviously hosted within their own jurisdiction to avoid the additional legal hurdles of pursuing an international legal process").

Along similar lines, an anonymizer is a software application that enables individuals to access the Internet while hiding the individual's identifying information.[105] Offenders sharing images via email may render their messages untraceable using re-mailers (which anonymously forwards email to a recipient), disposable email addresses (which may be used temporarily and anonymously and then discarded), or secure, encrypted free email addresses from services like hushmail.com.[106] An offender may also disguise his IP address through use of an "onion router." An onion router is a counter-surveillance tool that relies on a chain of proxies that "direct that Internet activity along complex circuitous routes in a network designed to completely obscure its origins."[107]

b. Safeguarding Child Pornography Collections

Beyond obscuring identity, many child pornographers make their child pornography collections more difficult to discover and analyze through various means. Some offenders rename their child pornography files so a casual observer will not recognize the illegal nature of the file. For example, an image or video file may be given an innocuous-sounding name, like "soccer.jpg." In addition, the file's extension — *i.e.*, the part of the filename generally comprised of a period followed by three letters (such as .jpg, .gif, or .tif for image files and .mov, .mpg, or .avi for video files) — may also be changed by the user in order to disguise the nature of the file. If the user changes "soccer.jpg" to "soccer.doc," the image is still accessible by an image-viewing program but appears from the file name to be a document. Other offenders use powerful password-protected encryption.[108] Encryption of data (in the form of images, videos, documents, etc.) can be used to secure the data so that it cannot be accessed without decryption software or a password. Some offenders have also been known to use steganography, which "make[s] it possible to hide an illegal image within an otherwise innocuous file."[109] Offenders may also use software to "partition" their computer or digital devices so that child pornography exists in a separate operating system and cannot be located during a cursory examination.[110]

---

[105] NATIONAL STRATEGY, *supra* note 3, at 23. Anonymizers have been criticized as "weak protection" as "users are placing all their trust in the Anonymizer's administrators." N. Boris Margolin, Matthew Wright & Brian Neil Levine, *Guardian: A Framework for Privacy Control in Untrusted Environments*, U. Mass Tech Report 04–37, at 2 (2004), available at http://prisms.cs.umass.edu/brian/pubs/margolin.wright.guardian.pdf (last visited Nov. 30, 2012).

[106] O'DONNELL & MILNER, *supra* note 7, at 161 ("A smart cybercriminal will never send a traceable message. It is easy to exchange messages using remailers that anonymise communications and then forward them to their destination."); SINCLAIR & SUGAR, *supra* note 7, at 20–21; *see also* Investigations Involving the Internet, *supra* note 17, at 51–52 (describing a complex scenario relaying on both P2P networks and proxy servers).

[107] NATIONAL STRATEGY, *supra* note 3, at 24, n.42.

[108] *See* HANDBOOK OF DIGITAL FORENSICS AND INVESTIGATION 39–40 (Eoghan Casey, ed., 2010) ("HANDBOOK") (describing common encryption techniques like PGP and BestCrypt); NATIONAL STRATEGY, *supra* note 3, at 23 ("Offenders also diminish the ability of law enforcement officials to investigate child pornography by storing images in encrypted files.").

[109] O'DONNELL & MILNER, *supra* note 3, at 161; *see also* HANDBOOK, *supra* note 108, at 40 (noting that examiners in child exploitation cases are advised to "be on the lookout for other forms of data concealment such as steganography," indicated by the presence of steganography software or unusually large files); SINCLAIR & SUGAR, *supra* note 7, at 23.

[110] For example, TrueCrypt is free encryption software that can partition storage devices, *see* http://www.truecrypt.org/ (last visited Oct. 12, 2012).

Offenders may also use software to "wipe" hard drives to prevent law enforcement from recovering previously deleted files.[111]

Knowledge about these methods is actively disseminated among the offending community.[112] According to one researcher, "[t]he constant emphasis on safety and self-defense is evident from the abundance of technical information, which constitutes a majority of postings on the [newsgroup] boards."[113] Child pornography offenders share things like encryption and proxy techniques, how to disguise the online identities of viewers as well as the offline identities of producers,[114] how to avoid tracking by law enforcement, and the importance of regularly cleaning their computers of evidence of illegal child pornography possession.[115] Offenders also engage "in specific counter-surveillance activities" like researching and sharing news of law-enforcement investigations and techniques as well as the screen names of suspected undercover agents.[116]

4. *Emerging Technology*

There appears to be a shift by some child pornography offenders toward even more secretive and sophisticated technologies. As briefly recounted above, some child pornography offenders utilize powerful multi-proxy anonymizing routers such as Tor and Freenet.[117] These anonymizers cloak an individual's online identity such that it is significantly more difficult to

---

[111] *See* HANDBOOK, *supra* note 108, at 43; NATIONAL STRATEGY, *supra* note 3, at 23.

[112] Fottrell Testimony, *supra* note 67, at 24–25; *but see* Grant Testimony, *supra* note 68, at 44–47 (cautioning that encryption and other privacy features are also used for legal purposes such as to protect against identity theft); *see also* Thomas J. Holt, Kristie R. Blevins & Natasha Burkert, *Considering the Pedophile Subculture Online*, 22 SEXUAL ABUSE 3, 15–22 (2010) (discussing how online pedophilic communities share security knowledge).

[113] JENKINS, *supra* note 3, at 110.

[114] United States v. McGarity, 669 F.3d 1218, 1230 (11th Cir. 2012) (describing the security measures shared in a sophisticated child pornography trading group which included distribution to new members of a document entitled "Security and Encryption FAQ"); NATIONAL STRATEGY, *supra* note 3, at 25 (describing how "producers of child pornography are increasingly taking precautions to hide their identities and the identities of their victims in images and videos," such as by removing location-tags or editing images and videos to "scrub" recognizable faces or identifiers).

[115] JENKINS, *supra* note 3, at 110–11.

[116] NATIONAL STRATEGY, *supra* note 3, at 24; *see also* JENKINS, *supra* note 3, at 151 ("Board participants are well aware of the various traps and investigations and regularly post news clippings and summaries of criminal cases as they arise, so other enthusiasts can learn about law enforcement techniques and be sure not to make the same mistakes themselves.").

[117] Tor explains that it is "free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis." Tor, *What is Tor?*, https://www.torproject.org/ (last visited Dec. 3, 2012). Freenet explains that it "is free software which lets you anonymously share files, browse and publish 'freesites' (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralised to make it less vulnerable to attack, and if used in 'darknet' mode, where users only connect to their friends, is very difficult to detect." Freenet, *What is Freenet?*, https://freenetproject.org/whatis.html (last visited Oct. 12, 2012).

trace it back to the individual.[118] Freenet acknowledges that some individuals exploit its anonymizing software to trade child pornography. While Freenet does not support child pornography or other illegal activity, it prioritizes freedom of speech and anonymity. Freenet discourages those who do not hold similar priorities from using Freenet by stating, "[i]f this is not acceptable to you, you should not run a Freenet node."[119]

Individuals using these anonymizers are able to access an otherwise invisible Internet through the use of hidden services.[120] In effect, the anonymizers function as magic glasses to access the invisible Internet; once the individual dons the glasses, the hidden services become visible. This invisible Internet is referred to alternately as "Deep Web," "Dark Net," "Darknet," and "Dark Web."[121] Here, for continuity, it will be referred to as Deep Web. Deep Web has been described as a "parallel" Internet that exists below the "surface" Internet.[122] Deep Web is simply not accessible without use of cloaking anonymizers.[123]

Within Deep Web, in addition to advertising other illegal material like weapons and drugs, individuals sometimes freely advertise child pornography.[124] Recent articles suggest that due to the high levels of protection afforded in Deep Web, law enforcement has minimal ability to identify child pornography offenders in Deep Web.[125]

---

[118] Some research has shown that even those offenders using powerful anonymizers may not always use such precautions and as such may be vulnerable to identification at times. *See* Ryan Hurley et al., *Measurement & Analysis of Child Pornography Trafficking on Gnutella & eMule*, TECH. REP. UM-CS-2012-016 (May 2012), (available at https://web.cs.umass.edu/publication/docs/2012/UM-CS-2012-016.pdf) (finding that "offenders use Tor inconsistently" with at least 60% of Tor users failing to use it at all times).

[119] See Freenet, *Freenet Frequently Asked Questions*, https://freenetproject.org/faq.html#childporn (last visited Dec. 3, 2012).

[120] Zhen Ling et al., *Protocol-Level Hidden Server Discovery*, http://www.cs.uml.edu/~xinwenfu/paper/HiddenServer.pdf (last visited Dec. 3, 2012) (discussing Tor's hidden services features) (last visited Oct. 12, 2012); *see also* Tor: Hidden Service Protocol, https://www.torproject.org/docs/hidden-services.html.en (last visited Dec. 3, 2012).

[121] While the term Dark Net/Darknet was used by Microsoft programmers in 2002 to describe any non-commercial online sharing of internet content, *see* Peter Biddle et al., *The Darknet and the Future of Content Distribution*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf (last visited Dec. 3, 2012), it has come to mean a sharing of digital content through onion routers or other sophisticated anonymizing technology. *See* BBC News, *File-Sharing 'Darknet' Unveiled* (Aug. 16, 2006), http://news.bbc.co.uk/2/hi/technology/4798059.stm (last visited Dec. 3, 2012).

[122] *See* Eileen Ormsby, *The New Underbelly*, THE AGE (June 1, 2012) (available at (http://www.theage.com.au/technology/technology-news/the-new-underbelly-20120531-1zktt.html); *see also* http://en.wikipedia.org/wiki/Deep_web (last visited Dec. 3, 2012).

[123] *See* Adrian Goldberg, *The Dark Web: Guns and Drugs for Sale on the Internet's Secret Black Market*, BBC NEWS, http://www.bbc.co.uk/news/business-16801382 (Feb. 3, 2012) (last visited Dec. 3, 2012); Eileen Ormsby, *supra* note 122.

[124] *See* Goldberg, *supra* note 123; Ormsby, *supra* note 122.

[125] *See* Adrian Chen, *'Dark Net' Kiddie Porn Website Stymies FBI Investigation*, GAWKER, (June 11, 2012), http://gawker.com/5916994/dark-net-kiddie-porn-website-stymies-fbi-investigation (last visited Dec. 3, 2012); Christopher Williams, *The Hidden Wiki: an Internet Underworld of Child Abuse*, TELEGRAPH (Oct. 27, 2011),

5. *Offender Culpability and Technology*

Offenders vary tremendously with respect to their technological sophistication and use of technology. Some federal offenders appear to be less technologically sophisticated than other offenders. A study conducted of local law-enforcement agencies about child pornography offenders arrested in 2006 found that just one in five child pornography possessors used a technical method to hide images.[126] Some have explained the phenomena of limited use of protective technology by arrested offenders by positing that "more technologically sophisticated [child pornography] possessors managed to avoid detection" and that law enforcement might be "nabbing the newest, least sophisticated, or most impulsive CP possessors."[127]

Some offenders claim to be technologically unsophisticated in that they only accidentally viewed child pornography or that, while they maintained possession of child pornography, they were not deliberately collecting it.[128] Although some individuals may accidentally access child pornography, the Commission's review of over 2,600 presentence reports from child pornography cases[129] indicates that the typical federal child pornography offender accessed child pornography on numerous occasions, across weeks, months or years, and deliberately collected hundreds or thousands of images. Intent to access child pornography is typically shown through a digital forensics examination of the offender's computer and other digital storage devices.[130]

Child pornography offenders claim that, even though they intentionally downloaded child pornography to their computers, they did not intentionally distribute child pornography on an "open" P2P network.[131] They typically explain that due to limited technological ability they did not understand that by installing a P2P program, they would end up sharing some files. Some courts have specifically rejected offenders' arguments that open P2P distribution should be distinguished from other types of distribution, noting that the offender "may not have actively pushed pornography on [P2P] users, but he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items."[132] Other

---

http://www.telegraph.co.uk/technology/internet/8851242/The-Hidden-Wiki-an-internet-underworld-of-child-abuse.html (last visited Dec. 3, 2012).

[126] Wolak et al., *Child Pornography Possessor: Trends*, *supra* note 97, at 32.

[127] Janis Wolak, David Finkelhor & Kimberley Mitchell, *Child-Pornography Possessors: Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, NAT'L CENTER FOR MISSING & EXPLOITED CHILDREN 10, 28 (2005).

[128] *See, e.g.* Belinda Winder & Brendan Gough, *"I Never Touched Anybody — That's my Defence": A Qualitative Analysis of Internet Sex Offender Accounts*, 16 J. SEXUAL AGGRESSION 125, 135 (2010) (a small study reporting that many child pornography offenders claimed their first exposure to child pornography was accidental).

[129] *See* Chapter 6 at 121–22 (discussing review of child pornography cases from fiscal years 1999, 2000, 2010, and 2012).

[130] *See infra* Sec. 3.b. *Proving Intent with Digital Forensics*.

[131] *See* Gelber, *supra* note 51, at 66, 68 (noting that because P2P programs put downloaded content automatically in a Shared folder, "by default it becomes available to other users of the P2P network, turning someone who thought he was *possessing* child pornography into someone who *distributes* child pornography—a much more serious offense.").

[132] United States v. Shaffer, 472 F.3d 1219, 1223 (10th Cir. 2007).

courts have focused on a fact-specific analysis of an individual's use of an open P2P network to determine whether the offender knowingly intended to share child pornography. In such cases, the court may reject an "automatic application of [the distribution enhancement under the guidelines] based solely on a defendant's use of a file-sharing program" but still find that "absent concrete *evidence* of ignorance . . . a fact-finder may reasonably infer that the defendant knowingly employed a file sharing program for its intended purpose."[133]

A subset of sophisticated child pornography offenders uses a variety of software applications to form or participate in child pornography communities dedicated to trading child pornography. The technological sophistication of some of these offenders enables members of their communities to evade detection and to exploit new victims.[134]

B. LAW ENFORCEMENT EFFORTS TO COMBAT CHILD PORNOGRAPHY

The rapid increase in the number of offenders and the sheer size of child pornography collections have challenged the ability of authorities to stem its rising tide.[135] Some in the law enforcement community view the "impact of these traders on law enforcement's ability to respond" as "catastrophic," as the scale of Internet trading "has caused the investigative and forensic infrastructure to be overwhelmed."[136] Various organizations are increasingly developing and utilizing technological tools such as "complex databases and software that scan for child-pornography images, increased ability to engage in undercover activity, and the ability to track electronic trails and evidence left by offenders as they communicate and surf online."[137] This section discusses some of these organizations, initiatives, and techniques.

---

[133] *See* United States v. Durham, 618 F.3d 921, 931 (8th Cir. 2010); *see also* United States v. Dodd, 598 F.3d 449, 452 (8th Cir. 2010).

[134] *See* Chapter 4 at 92–99 (discussing child pornography communities).

[135] For example, one Internet Crimes Against Children task force commander stated that the growth of child pornography "forces us into more of a reactive strategy, thereby we're responding to tips from the public, from the service providers, instead of being proactive and going out and combating this problem." Testimony of Captain Kirk Marlowe, Virginia State Police Bureau of Criminal Investigation, to the Commission, at 252–53 (Feb. 15, 2012) ("Marlowe Testimony").

[136] Statement of Flint Waters, Special Agent, Wyoming Attorney General Division of Criminal Investigation, *Child Sex Crimes on the Internet: Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 2 (2007) ("Waters Statement") at 2; *see* JENKINS, *supra* note 3, at 154 ("Even if they arrest hundreds or thousands of child porn users each year, the staggering mathematics of Internet usage imply that the traffic will continue."). One example, Operation Roundup, reports that over 100 search warrants have been completed from leads generated since its 2008 inception. *See* NATIONAL STRATEGY, *supra* note 3, at 13–14. But over that same time period, Operation Roundup has identified well over one million unique IP addresses trading in child pornography. *See id.*; *see also* Diez, *supra* note 102, at 786 ("[I]n an ever-evolving technological world, government bureaucracy and legislatures tend to be reactive to, and thus, two steps behind, net-savvy child pornographers.").

[137] Wolak et al., *Child Pornography Possessor: Trends*, *supra* note 97, at 29 ("[W]hile evolving technology may raise additional challenges in law enforcement's investigation of these cases, technological developments also have given new tools and advantages to law enforcement.").

1. *Organizational Overview*

Many government agencies and several private organizations participate in the investigation and forensic analysis of child pornography. The following discussion highlights some of the most prominent examples.

The largest United States law enforcement organization dedicated to stopping the creation and spread of child pornography is the group of task forces under the umbrella moniker Internet Crimes Against Children ("ICAC"). Founded in 1998, the ICAC Task Force Program is a national network of 61 separate task forces associated or affiliated with 2,500 federal, state, local, and tribal agencies located in all 50 states.[138] Through the use of federal grants, ICAC task forces assist in investigations, prosecutions, and training sessions related to child pornography and other forms of child exploitation. ICAC task forces also perform the bulk of computer forensic examinations related to child pornography.[139] In 2010, ICAC investigated 32,000 cases of child pornography and made 5,300 arrests.[140]

At the federal level, there are several agencies that investigate child pornography offenses and analyze evidence. The first is the Federal Bureau of Investigation ("FBI"), which administers several anti-child-pornography initiatives, conducts investigations, and analyzes forensic evidence. In 2010, the FBI investigated 6070 child pornography cases and made 1094 arrests.[141] In addition, the Immigration and Customs Enforcement ("ICE"), within the Department of Homeland Security ("DHS"), operates several programs to help combat child pornography.[142] Still other investigative and forensic work is performed elsewhere in the federal government, such as by U.S. Postal Service investigators and the Secret Service.[143] Federal child pornography cases are often prosecuted with assistance from the Child Exploitation and Obscenity Section of the Criminal Division ("CEOS") of the Department of Justice ("DOJ"). CEOS attorneys lead investigations and advise and train line prosecutors in U.S. Attorneys Offices across the country, as well as assist them in the prosecution of child pornography offenders.[144]

The National Center for Missing and Exploited Children ("NCMEC") is a public-private partnership created in 1984 pursuant to the Missing Children's Assistance Act of 1983[145] to help prevent child abduction and sexual exploitation and locate missing children, among other

---

[138] NATIONAL STRATEGY, *supra* note 3, at 58.

[139] *Id.* at 76.

[140] 2011 GAO Report, *supra* note 24, at 53.

[141] *Id*. at 51.

[142] *Id*. at 54–55.

[143] *Id*. at 55–57.

[144] *See* CEOS website at http://www.justice.gov/criminal/ceos/ (last visited Dec. 3, 2012).

[145] Pub. L. No. 98–473, 98 Stat. 1837 (1984), *see also* 42 U.S.C. § 5773 enumerating 19 specific tasks which NCMEC has been congressionally authorized to perform.

missions.[146] NCMEC was statutorily created, receives funding from federal sources, and has specific statutory responsibilities. Nevertheless, it is a private, nonprofit organization.[147] With regard to child pornography specifically, Congress has mandated that NCMEC operate both the CyberTipline and the Child Victim Identification Program ("CVIP"). The CyberTipline "serves as the national clearinghouse for online reporting of tips regarding child sexual exploitation including child pornography." Since its 1998 inception the CyberTipline has received over 1,300,000 reports,[148] including a 69-percent increase between 2005 and 2009.[149] Electronic communication service providers such as email systems and other websites that store online content are mandated to report child pornography that they find on their system to the CyberTipline.[150]

The CVIP program attempts to find identifiable children in child pornography images. CVIP relies on a variety of techniques including hash values to determine if the images they receive are known images of child pornography or if they are new images that have never before been encountered. CVIP had reviewed over 28.5 million child pornography images and videos by 2009, including a 432- percent increase in videos and images submitted for identification between 2005 and 2009.[151]

Child pornography is an international crime and there are international law enforcement efforts to combat it. INTERPOL is an international police organization with 190 member countries across the world, including the United States.[152] INTERPOL maintains a division dedicated to fighting Internet crimes against children.[153] INTERPOL works to identify victims, develop international strategies, and provide training to member countries.[154]

2. *Law Enforcement Investigations*

Investigations of child pornography offenders may take several forms. Some offenders are initially investigated for contact child sex offending and child pornography is found on their

---

[146] Nat'l Center for Missing & Exploited Children, *Mission and History*, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362 (last visited Dec. 3, 2012).

[147] *Id.*

[148] Nat'l Center for Missing & Exploited Children, *2011 Annual Report*, at 7 (2011).

[149] NATIONAL STRATEGY, *supra* note 3, at 11, 94.

[150] 2011 GAO Report, *supra* note 24, at 3; NATIONAL STRATEGY, *supra* note 3, at 11.

[151] NATIONAL STRATEGY, *supra* note 3, at 11. NCMEC reports that this number continues to increase; the CVIP program reviewed over 17.4 million images in 2011 alone. NCMEC, *2011 Annual Report*, *supra* note 148, at 7 (2011).

[152] *See* INTERPOL, *About INTERPOL*, http://www.interpol.int/About-INTERPOL/Overview (last visited Dec. 3, 2012).

[153] *See* INTERPOL, *Crimes Against Children*, http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children (last visited Dec. 3, 2012).

[154] *Id.*

computers during the investigation of the contact offense. Similarly, some offenders are initially arrested for "travel" or "enticement" offenses in which an offender travels to meet a real child (or an undercover law enforcement agent posing as a child) for sexual purposes and the offender also possesses child pornography. Other offenders are identified when an individual with access to the offender's computer finds the illegal material and reports the offender to the police. The reporting individual is commonly a family member, information technology support staff at the offender's workplace, or a computer technician hired by the offender to repair the computer.

Among federal offenders, many are identified through online investigations involving the recovery of IP addresses on P2P networks or Internet forums, or the recovery of incriminating payment authorizations at Usenet providers or commercial child pornography sites. A P2P investigation may involve trolling a certain network using specialized software to determine the IP addresses of those sharing child pornography images. By initiating a search, investigators can obtain a list of shared files involving child pornography that are then matched by hash values with known child pornography images or videos.

In such operations, investigators generally have two ways of identifying distributors: (1) identifying the IP address of the computer involved in the child pornography offense, and (2) a Globally Unique Identifier ("GUID"), which is the unique serial number assigned to each P2P program downloaded by a user.[155] The local investigator may then cross-check the IP address and GUID with past crimes or ongoing investigations and confirm that the computer is sharing illegal child pornography.[156] The IP address may reveal the general jurisdiction in which the computer is located and can be used to obtain the name and address of the user of the IP address through a subpoena for an ISP's records.[157] Unless the distributor has disabled the feature, the investigator is usually able to browse the distributor's computer directly to see a list of all files he is currently sharing. [158] If the IP address indicates the distributor is in a different jurisdiction, the investigator will share that information with the appropriate investigating jurisdiction. If the distributor is in the local jurisdiction, the investigator may subpoena the ISP to attempt to identify the distributor. If the distributor can be identified, the investigator will try to identify the occupants of the distributor's residence to determine if any children are present and whether any of the occupants have prior criminal history including child pornography offenses or other sexually dangerous behavior to prioritize the investigation. The investigator may then seek a search warrant to seize evidence for forensic examination, as well as interview the suspected offender during the execution of the warrant.[159]

Obtaining the IP address is typically only the first step in identifying a suspect. Several, sometimes challenging, steps must occur after obtaining the IP address. The law enforcement

---

[155] Moulin, *supra* note 46, at 2; 2003 GAO Report, *supra* note 7, at 25.

[156] Note that while GUIDs are globally unique, they are assigned to specific software programs rather than individuals and cannot be used to identify a particular user.

[157] *See* NATIONAL STRATEGY, *supra* note 36, at 23.

[158] Moulin, *supra* note 46, at 1–2. Increasingly, however, P2P applications have removed remote browsing as an option.

[159] Waters Statement, *supra* note 136, at 4.

agency must determine which ISP customer was using the IP address at a given time by subpoenaing information from the ISP. The ISP may simply not have a record of which customer was using that IP address at that time. 160 While in practice many ISPs do keep records as to which customer was using an IP address (at least for a short period of time), no federal statute requires the ISPs to retain sufficient information to associate an IP address with a particular customer.[161] Further, even those ISPs that express an intent to cooperate with law enforcement and retain excellent records may not respond promptly to all law enforcement requests due to insufficient resources dedicated to subpoena compliance. Finally, offenders who connect to the Internet after cloaking their identities with anonymizing proxy servers may be identified only by the additional step of subpoenaing the proxy server provider, many of which keep no records.[162] The same barriers stand in the way of locating those running child pornography websites. Law enforcement officials often lament the tedious and frustrating process because "by the time investigators have taken the legal steps to track administrators, the suspect sites have moved from one place to another on the Internet."[163]

Other offenders are identified via investigative sting techniques like website "honeypots" or through chatting with law enforcement agents posing as minors.[164] One example of an Internet sting operation involving a website "honeypot" was Operation Pin in 2003, in which the U.K. National Crime Squad (with help from INTERPOL, the FBI, and other international authorities) set up a series of fake websites offering child pornography and affording users the option of either proceeding to illegal content or leaving the website.[165] Once the user clicked through a sufficient number of pages he would receive a message from the authorities informing him that he had committed an offense and that his information had been submitted to the appropriate authorities.

---

[160] ISPs may assign users either a single fixed IP address, sometimes called "static," or one of many different rotating IP addressed sometimes called "dynamic." Only some individuals and businesses require a static IP address. For example, individuals or businesses that run email or Web servers, services that require external approval (such as approval for credit card purchases), or those who are using more sophisticated programs may require a static IP address. By contrast most home Internet users are assigned by their ISP a dynamic IP address that varies depending on when they access the Internet.

[161] *See* 2011 GAO Report, *supra* note 24, at 42–43; NATIONAL STRATEGY, *supra* note 3, at 23, n.40 (citing a 2009 survey showing that a majority of criminal investigators believed that the failure of ISPs to maintain user records detrimentally affects investigations).

[162] JENKINS, *supra* note 3, at 160–61 ("[C]ollecting IP addresses is rarely of much use since virtually all board participants use proxies, so only the individuals identified would be the inexperienced who were 'surfing naked'. . . . To be valuable, any information collected about IPs would require an additional step finding the real identities lying behind the proxies.").

[163] Luders, *supra* note 100, at 17.

[164] O'DONNELL & MILNER, *supra* note 7, at 155 (noting that as many as one in four arrests for Internet sex crimes against children involve investigators posting as minors); JENKINS, *supra* note 3, at 14 ("Both trading and chat lines are deadly because one is dealing with faceless individuals who often turn out to be police officers masquerading either as fellow enthusiasts or as underage girls; avoiding such chat facilities is a primary rule offered to novices in this underworld.").

[165] Taylor & Quayle, *The Internet and Abuse Images of Children*, *supra* note 12, at 189–90.

Finally, some sophisticated operations stem from infiltration of a closed Internet trading community by a law enforcement officer. As these private trading groups operate clandestinely, successful undercover infiltrations often require the arrest of a participating offender.[166] If the offender quickly cooperates by allowing his logon information to be used in the investigation, the subsequent infiltration can bring down an entire network of offenders.[167] Even in such cases it is often difficult to identify all members of a worldwide group due to the difficulty in coordination and cooperation across international jurisdictions.[168]

3. *Digital Forensics*

Once investigators seize computers or other property via an arrest or search warrant, they typically turn over the recovered evidence to digital forensic examiners. The goal of the forensic examiner is to identify the child pornography images and videos on the computer and preserve the evidence in a forensically sound manner.[169] Digital forensic examiners in child pornography investigations seek to identify the illegal child pornography images and uncover evidence of the user's identity and intent, as described below. Forensic examinations in child pornography cases are predominately conducted by state and local law enforcement agencies through one or several of the agencies that are members or affiliates of one of the ICAC task forces.[170] The number of such examinations has increased in recent years, from nearly 10,500 examinations in fiscal year 2007, to 14,339 in 2008, and 19,269 in 2009.[171] The amount of time each investigation takes may vary greatly depending on the type of device, size of the collection, and sophistication of the suspect.[172] A forensic examination typically requires making a duplicate image of a computer hard drive and then running an automated search for all the files with the same hash values as known child pornography images to identify the number of child pornography files in active space. While conducting such an automated search can be trivial in terms of time and resources, an exhaustive search of every part of a computer can be "enormously laborious," especially a search of parts of the computer that are inaccessible to the user and which may contain fragments

---

[166] NATIONAL STRATEGY, *supra* note 3, at 27 ("[T]hese criminal enterprises typically go to great lengths to evade law enforcement and, ultimately, are identified only when an individual member's computer is seized for unrelated conduct and law enforcement, posing as the member, observes the group activity on the computer and can infiltrate the group.").

[167] For example, several of the most prominent investigations, such as Operation Wonderland, were broken up only after low-level participants were arrested and subsequently cooperated with law enforcement officials in pursuing the wider ring. *See* JENKINS, *supra* note 3, at 152–53 (detailing publicly known information about the discovery, investigation, and prosecution of the Wonderland club); *cf.* United States v. Ladeau, No. 09-40021-FDS, 2010 WL 1427523, at *1 (D. Mass. Apr. 7, 2010) (noting that investigators used different arrested individuals' online identities to infiltrate Gigatribe network and engage with other potential suspects, including defendant).

[168] NATIONAL STRATEGY, *supra* note 3, at 27 ("While investigations into these groups can yield the arrest of multiple child molesters, identification of the members and cooperation with foreign law enforcement, which may be required, can frustrate efforts to identify specific suspects.").

[169] NATIONAL STRATEGY, *supra* note 3, at 76.

[170] 2011 GAO Report, *supra* note 24, at 33–34.

[171] NATIONAL STRATEGY, *supra* note 3, at 131.

[172] 2011 GAO Report, *supra* note 24, at 34; NATIONAL STRATEGY, *supra* note 3, at 30.

of deleted files.[173] In large part, however, forensics delays appear to be due to backlogs in forensics analysis rather than the complexity of performing forensics reviews.[174] For example, the FBI has reported that the volume of data processed at its labs increased by 3,000 percent between 2003 and 2009.[175]

a. Recovery of Child Pornography

One of the forensic examiner's main goals after forensically preserving the seized evidence is to search the computer or other media (such as external hard drives, DVDs, CDs, flash drives, or cell phones) for child pornography images.[176] This process may involve the search of file folders, browsing or communications programs, e-mails, and chat logs through automated search for files with relevant extensions (*e.g.*, .jpg, or .gif for images; .movor .mpeg for videos), or hash values indicating known child pornography images.[177] The files may be easily located by being stored in dedicated computer folders with names like "My Pictures" or "Shared," or that describe the type of child pornography stored in the folder.[178] At other times, the entire computer, or certain folders or files, have been hidden, renamed, encrypted, password protected, or deleted.

During a forensics examination it may be possible to determine when and how often an individual accessed child pornography files. This can be accomplished through a review of metadata that records when a file is created or changed and the last time the file was accessed.[179] Another basic forensics review technique examines the temporary files saved automatically by the computer and many programs. For example, web browsers keep a temporary Internet cache by default.[180] When browsing websites, the cache automatically downloads images and other files in order to speed up the browsing experience and, instead of re-downloading oft-visited pages, the browser can simply load the file from the cache. The forensic examiner may be able to recover individual child pornography images from the cache or load saved versions of the

[173] O'DONNELL & MILNER, *supra* note 7, at 165 ("The biggest obstacle facing any police force attempting to tackle child pornography is the huge commitment required in terms of time."); NATIONAL STRATEGY, *supra* note 3, at 30.

[174] 2011 GAO Report, *supra* note 24, at 35. This backlog was discussed by an ICAC commander at the Commission's recent hearing on child pornography. The commander stated "We do on-scene triage with regards to forensics to get information, but quite often those cases still need a full-blown forensics before they go to trial. So that backlogs the system for three to six months on any given case." Marlowe Testimony, *supra* note 135, at 252.

[175] 2011 GAO Report, *supra* note 24, at 35–36.

[176] NATIONAL STRATEGY, *supra* note 3, at 76 ("Investigators commonly seize multiple media in one investigation, including: internal and external hard drives, flash drives, DVDs and CDs, cells phones and other digital media devices containing terabytes of data in an effort to identify contraband files.").

[177] *Id.* at 76.

[178] *See* Fig. 3–2, Chapter 3 at 50.

[179] Nat'l Inst. of Justice, *Special Report: Forensic Examination of Digital Evidence: A Guide for Law Enforcement* 16 (Apr. 2004) (available at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf).

[180] *See* HANDBOOK, *supra* note 108, at 280–82 (describing mechanics of web cache).

websites themselves.[181] Many successful prosecutions for possession of child pornography have been based on the existence of such files found only in the temporary cache.[182]

Many offenders regularly delete their downloaded files and clear their temporary files.[183] In these cases, forensic examinations must rely on more sophisticated techniques to recover data that, although deleted by the user, still remains on the computer's storage device.[184] Using powerful data recovery or file carving software, examiners can often recover files that suspects believe they have deleted.[185] Even if a sophisticated offender has used software to "wipe" their unallocated space, an investigator may still be able to recover a list of all the deleted files.[186] Forensic examination may also decrypt hidden or encrypted files with the help of powerful software tools.[187]

b. Proving Intent with Digital Forensics

In addition to identifying the illegal child pornography possessed by the defendant, forensic examinations also play a role in offering evidence of the offender's intent. Because federal law prohibits the receipt, possession, or distribution of child pornography only if it is done knowingly,[188] the examination helps demonstrate the suspect's knowledge or intent in viewing, downloading, or distributing the illegal material. While not discussed here, a thorough digital forensics examination is equally important to an individual's defense. Such an

[181] JENKINS, *supra* note 3, at 111 ("Participants will instruct novices in the essential importance of cleaning the computer's cache regularly to erase images, which might otherwise constitute legal evidence of possession of child pornography.").

[182] *See* Marin, *supra* note 52, at 1213–14 (describing how temporary Internet files constituting illegal child pornography can be retained in a user's cache); *see, e.g.*, United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006) ("Here, we hold Romm exercised dominion and control over the images in his cache by enlarging them on his screen, and saving them there for five minutes before deleting them. . . . [and] this evidence of control was sufficient for the jury to find that Romm possessed and received the images in his cache.").

[183] Products used to clean and optimize computer drives, such as CCleaner, have legitimate uses but they are also sometimes used by child pornography offenders to avoid prosecution. *See* HANDBOOK, *supra* note 108, at 43; NATIONAL STRATEGY, *supra* note 3, at 23.

[184] In simplified terms, when a computer user saves a file, the operating system scans for enough free space to write the data and then sends the data there. Those newly written clusters become allocated space. When a user deletes a file, the operating system *does not* go back and change the previously written clusters; instead, it simply revises the map so that those clusters show up as unallocated space. *See* HANDBOOK, *supra* note 108, at 36–37 (noting that unallocated space "is important from an investigative standpoint because it often contains significant amounts of data from deleted files"); FERRARO AND CASEY, *supra* note 15, at 200–201.

[185] *See* HANDBOOK, *supra* note 108, at 36–37 (listing file carving tools like Foremost, Scalpel, DataLifter, and PhotoRec).

[186] *See id.* at 43; NATIONAL STRATEGY, *supra* note 3, at 23.

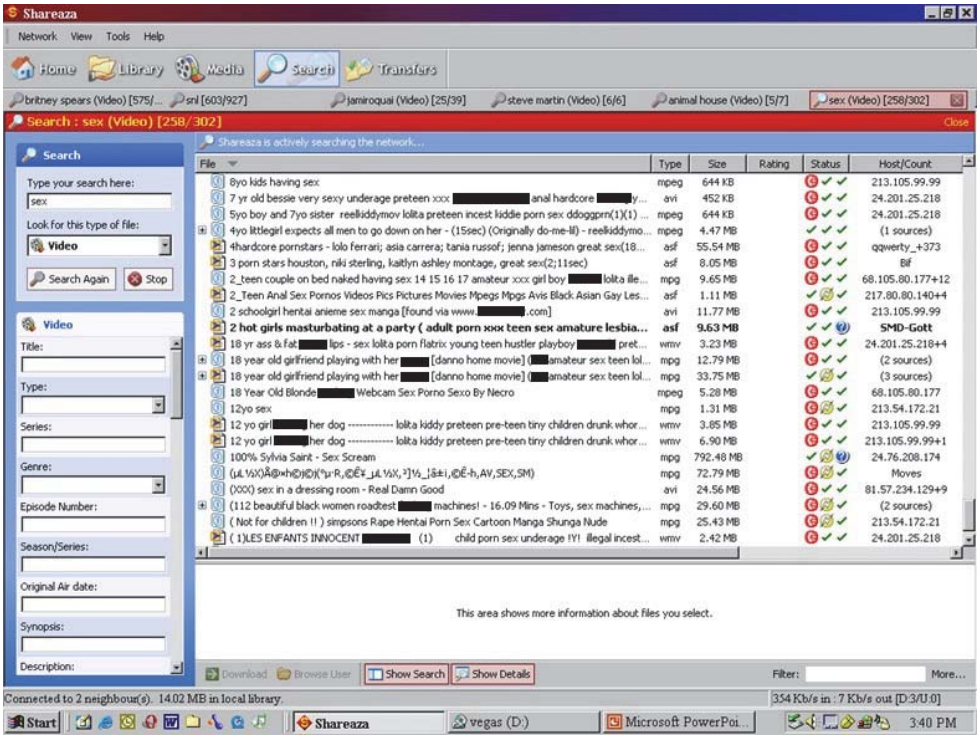
[187] *See* HANDBOOK, *supra* note 108, at 39.

[188] *See* 18 U.S.C. §§ 2252 & 2252A.

examination may negate claims regarding a defendant's intent to access or share images or it may otherwise limit sentencing exposure.[189]

Although some collections may be so vast or so organized that the question of knowledge is not an issue,[190] other times an offender may not have intentionally saved any images on the computer, as the offender instead only browsed web pages containing child pornography images.[191] Examinations may provide several ways to build a powerful evidentiary case against an offender who attempts to deny knowledge or intent. By collecting the right types of information, such as screenshots of an offender's sharing preferences as seen below in Figure 3-3, search terms, folder structure, and the like, forensics examinations can demonstrate that child pornography offenders intended to view or distribute child pornography.

Figure 3-3[192]
Federal Defender Technology Presentation: Screenshot of P2P Search Window



[189] *See* Grant Testimony, *supra* note 68, at 46–47 (discussing the importance of a full forensic examination to the defense team).

[190] *See* Chapter 4 at 80–85 (discussing offender collecting behavior).

[191] Marin, *supra* note 52, at 1211 (distinguishing between the Internet's "multiple avenues to access[ing] child pornography," including viewing files from an Internet server versus downloading an image to one's computer); *see also* Fottrell Testimony, *supra* note 67, at 22–23 ("[i]mages in particular folders sorted and organized . . . are not accidentally viewed; they are purposely sorted and organized in a particular manner").

[192] Grant Presentation, *supra* note 49.

Even when a file cannot be decrypted or has been deleted and cannot be recovered, the presence of powerful encryption, steganographic, or drive-erasing software may be used to buttress a showing of criminal intent.[193]

E. CONCLUSION

This chapter provided information regarding how child pornography offenders access and distribute child pornography.

- Until the late 1970s and early 1980s, child pornography was difficult to find, risky to produce, expensive to duplicate, and required a secure and private storage area. Technological advances since that time have made child pornography much more widely available and reduced the barriers to offending.

- Although it is possible that some individuals may accidentally access child pornography, the Commission's review of more than 2,600 non-production child pornography cases indicates that the typical federal child pornography offender intentionally accessed child pornography on numerous occasions, across weeks, months or years, and downloaded hundreds or thousands of images.

- Most child pornography offenders now rely on Internet or Internet-enabled technology to access and distribute child pornography.

- Many child pornography offenders rely on P2P networks, which enable people to connect directly to other individuals' computers without having to use a third-party. Some P2P networks are "open" in that they permit individuals to share with others in an anonymous or "impersonal" fashion. Other P2P networks operate in a "closed" fashion and combine elements of social networking. Closed P2P network users may select with whom they wish to share files in a "personal" fashion.

- Open P2P networks typically have default settings that permit sharing of a user's files; however, in most cases, both downloading locations and sharing options may be changed by users to limit whether files are available for sharing.

- Offenders use technology in a wide variety of ways to commit child pornography crimes. While some offenders utilize relatively non-sophisticated technology to view and save child pornography, others engage in sophisticated and elaborate tactics to communicate with other child pornography offenders and to evade detection.

- The extent of offenders' use of sophisticated techniques is unclear, given that most of what law enforcement and researchers know about child pornography

[193] NATIONAL STRATEGY, *supra* note 3, at 131; *see* HANDBOOK, *supra* note 108, at 33–34.

offenders is gleaned from those who are least likely to have used such techniques and are thus more likely to have been identified and arrested.

- Many federal law enforcement agencies and community resources are dedicated to fighting child pornography crimes, but these efforts face challenges from the sheer volume of online child pornography distribution, the technological sophistication of some offenders, delays in obtaining identifying information from ISPs regarding their customers suspected of distributing child pornography, and the logistics of completing timely forensics analysis.