Berkeley Technology Law Journal

Volume 19 | Issue 4 Article 3

September 2004

Don't Cache out Your Case: Prosecuting Child Pornograpy Possession Laws Based on Images Located in Temporary Internet Files

Ty E. Howard

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38R382

DON'T CACHE OUT YOUR CASE: PROSECUTING CHILD PORNOGRAPHY POSSESSION LAWS BASED ON IMAGES LOCATED IN TEMPORARY INTERNET FILES

By Ty E. Howard†

ABSTRACT

This Article explores issues surrounding the prosecution of child pornography possession laws based on images located in temporary Internet files. The Article begins with a technical background of both caches and the forensic examinations used by investigators. After reviewing the pertinent case law, the Article introduces the two conceptual approaches—the Present Possession approach and the Evidence Of approach—and discusses how conceptual choices affect the analysis of knowing possession. Using the two conceptual approaches as a guide, the Article then reevaluates the various factors courts have considered, and the various defenses defendants have forwarded, when faced with a possession case based upon cached images. For courts, that reevaluation suggests that the approach to which they have defaulted may not be the most technologically accurate. For prosecutors, the reevaluation suggests that their choice of conceptual approach could have serious effects on their case strategy as well as on how best to serve the punitive and penological goals of child pornography possession laws.

TABLE OF CONTENTS

---

† Assistant District Attorney, Chester County District Attorney's Office, West Chester, Pennsylvania. B.A., Pennsylvania State University (1994); M.G.A., University of Pennsylvania (1997); J.D., Georgetown University Law Center (2000). The views expressed in this Article are solely those of the author and do not reflect any position, policy, or opinion of the Chester County District Attorney's Office. I thank Trooper Jon Nelson of the Pennsylvania State Police Computer Crime Task Force for his helpful comments during the drafting of this Article and, most importantly, my wife Lin—for everything, for always.

I. INTRODUCTION

Child pornography has gone high technology, and there is no sign of the trend abating. For well over a decade, purveyors of child pornography have used the Internet as their principal means of communication and distribution. No longer are defendants collecting and trafficking in photographs, videotapes, and magazines—the media of choice are digital images. And no longer is the contraband traded and trafficked through adult bookstores and black market sales—the medium of choice is the Internet.

As child pornographers have become more tech savvy, however, so too has law enforcement. One major area of advancement is computer forensics, which is the study of computers and computer-related media for evidence of criminal activity. Unlike traditional forms of evidence, computer-based evidence is not easily destroyed without specialized knowledge. With the assistance of forensics software, a skilled investigator can recover large amounts of evidence from a computer that the user thought was deleted or never even knew existed. As a result, computers can be a veritable treasure trove of incriminating evidence for the prosecution. Un-

fortunately, finding the evidence is only part of law enforcement's job. The next task is for prosecutors and police officers to interpret and explain the evidence in a way that a fact finder can understand, and in a way that allows the court to apply the law correctly.

This Article examines one particular type of computer-based evidence—images found in a computer's browser cache—and the issues facing prosecutors and courts in properly analyzing that evidence in the context of a criminal prosecution for possession of child pornography. In exploring those issues, this Article focuses on the type of conceptual approach around which prosecutors should build and courts should analyze their cases.

Part II provides a technical background. First, it describes what a cache is, its purpose, and its functions. Then, the part explains the forensic process through which investigators can discover and analyze cached images. Part III outlines the general type of statute that criminalizes possession of computer child pornography, focusing particularly on the federal statute, 18 U.S.C. § 2252A (2000). Next, Part IV reviews the case law surrounding prosecutions for possession of child pornography based on images in a computer's cache. Part V then introduces two conceptual approaches—the Present Possession approach and the Evidence Of approach—that can be used by courts to analyze the cache-possession issue and how application of the different approaches may alter courts' legal analyses. Part VI describes likely defenses in Internet child pornography cases and suggested prosecution responses. Finally, Part VII concludes that the Evidence Of approach is the most technically and strategically sound conceptual approach, as well as the approach best designed to serve the punitive and penological goals of child pornography possession statutes.

II. TEMPORARY INTERNET FILES AND CACHES

A. Caches

A cache (pronounced "cash") is a storage mechanism designed to speed up the loading of Internet displays.[1] When a computer user views a

1. Except where otherwise noted, the terms "cache" or "computer's cache" as used in this Article specifically refer to a browser cache, which is one type of web cache. *See infra* notes 2-12 and accompanying text (discussing types of web caches and related topics). In distinction from web caches, the general term cache (sometimes referred to as "system cache") can refer to any type of storage area or reserved section of memory within a computer. *See* Paul Mazzucco, *The Fundamentals of Cache*, SLCENTRAL (Oct. 17, 2000), *at* http://www.systemlogic.net/articles/00/10/cache/print.php. Like web cache,

webpage, the web browser stores a copy of the page on the computer's hard drive in a folder or directory. That folder is known as the cache, and the individual files within the cache are known as temporary Internet files.[2] When the user later returns to a previously visited webpage, the browser retrieves the cached file to display the webpage instead of retrieving the file from the Internet.[3] By retrieving the page from the cache, instead of the Internet, the browser can display the page more quickly.[4]

The actual caching and retrieval processes will vary depending on several factors, some of which are controlled by the computer user and others which are controlled by the content provider. A user can customize her cache by increasing or decreasing the size of the cache, which allows a greater or lesser number of temporary Internet files to be saved.[5] Increasing the size of the cache allows a user to view more pages more quickly,

---

system cache is designed to increase the speed of the computer. *See* Charles M. Kozierok, *Layers of Cache*, PCGUIDE, *at* http://www.pcguide.com/ref/mbsys/cache/index-c.html (last visited Dec. 19, 2004).

2. *See, e.g.*, *Temporary Internet File*, WEBOPEDIA COMPUTER DICTIONARY, *at* http://www.webopedia.com/TERM/t/temporary_Internet_file.html (last modified Apr. 22, 2004). Many sources, and many courts, use terms like "cache," "cache files," "temporary Internet cache," and "temporary Internet files" interchangeably.

3. There are two subtypes of web caches that retrieve temporarily stored Internet files from different locations: browser caches and proxy caches. A browser cache is the typical type of web cache on a modern personal computer in which a portion of the hard disk is set aside to store files of recently visited websites. *See, e.g.*, Mark Nottingham, *Caching Tutorial for Web Authors and Webmasters: What's a Web Cache? Why Do People Use Them?*, WEB DEVELOPER'S VIRTUAL LIBRARY (June 21, 1999), *at* http://www.wdvl.com/Internet/Cache. A proxy cache works in a similar fashion, but on a much larger scale. Proxy caches are shared caches that are usually set up by corporations or Internet Server Providers (ISPs) that serve a large number of users. Users of a particular ISP or network request pages from a local server instead of directly from the Internet. The server obtains the webpage, saves it, and then forwards it to the user. Later requests from other users on that ISP or network get the saved copy. *See id.*; *see also Cache server*, WHATIS.COM, *at* http://whatis.techtarget.com/definition/0,,sid9_gci211731,00.html (last visited Dec. 19, 2004); Chuck Connell, *Proxies, reverse proxies, and passthrus*, SEARCHDOMINO.COM (Sept. 10, 2002), *at* http://searchdomino.techtarget.com/originalContent/0,289142,sid4_gci850152,00.html; *Proxy server*, SEARCHSECURITY.COM, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212840,00.html (last updated Sept. 14, 2004) (describing the caching functions of a proxy server).

4. Web caches improve speed and efficiency in two ways: (1) by satisfying a browser request with a cached file, the browser does not need to download the file a second time, thereby saving time; and (2) by only utilizing the server once to obtain a file, the cached file reduces the amount of bandwidth used. *See, e.g.*, Nottingham, *supra* note 3.

5. *See* Microsoft Knowledge Base Article - 155353, *How to Adjust Cache Size for Temporary Internet Files*, *at* http://support.microsoft.com/default.aspx?scid=kb;EN-US;155353 (last visited Dec. 19, 2004).

but also occupies greater space on the computer's hard drive. Decreasing the size of the cache frees up more hard drive space, but limits the number of cached files available for display. Because the size of the cache is capped, individual temporary Internet files are usually created and then discarded on a "first in, first out" basis.[6] Computer users can purchase software programs to increase the size and improve the performance of their browser cache.[7] In addition, users are able to delete the contents of the cache manually[8] or with the assistance of commercial software.[9]

While the user can customize her computer's cache, content providers such as website creators and ISPs can configure websites in ways that also will affect how certain images are cached. Those content providers can, among other things, affect how easily a requested page or image is cached,[10] whether and how often the cache will have to validate with the web server that the cached page is current,[11] and, significantly, whether certain requested pages can be cached at all.[12]

---

6. *See, e.g.*, Brian D. Davison, *A Web Caching Primer*, 5 IEEE INTERNET COMPUTING 38, 39 (2001), *at* http://www.cse.lehigh.edu/~brian/pubs/2001/Internetcomputing/davison01web.pdf.

7. *See, e.g.*, *Improving Browser Caches with Extensions and Personal Proxies*, WEB CACHING, *at* http://www.web-caching.com/personal-caches.html (last visited Dec. 19, 2004) (listing various software programs designed to increase cache size or improve cache performance).

8. *See* Microsoft Knowledge Base Article - 260897, *How to Delete the Contents of the Temporary Internet Files Folder*, *at* http://support.microsoft.com/default.aspx?scid=kb;en-us;260897 (last visited Dec. 19, 2004).

9. There are various software programs for purchase that will "clean" a computer's cache and remove other ambient or residual data on the computer. By design, these programs remove not only the cached files, but electronic remnants that would otherwise still be discoverable through forensic examination. *See, e.g.*, Evidence Eliminator v5.0, *at* http://www.deletecache.com (last visited Dec. 19, 2004).

10. *See, e.g.*, Davison, *supra* note 6, at 42-43; Mark Nottingham, *Tips for Building a Cache-Aware Site* (Feb. 15, 2004) (describing several technical points for webmasters to make sites more cache friendly), *at* http://www.mnot.net/cache_docs/#TIPS.

11. *See, e.g.*, Mark Nottingham, *How Web Caches Work* (Feb. 15, 2004), *at* http://www.mnot.net/cache_docs/#WORK (describing validation and freshness terms).

12. *See, e.g.*, Davison, *supra* note 6, at 42-43 (discussing certain web resources that are non-cacheable); Microsoft Knowledge Base Article - 234067, *How To: Prevent Caching in Internet Explorer*, *at* http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q234/0/67.ASP&NoWebContent=1 (last visited Dec. 19, 2004).

B. Computer Forensic Examinations

Computer forensic examinations involve three basic steps: acquisition, authentication, and recovery.[13] First, the investigator must acquire the electronic information contained on a computer or computer media. Once the original computer is seized,[14] the examiner makes an exact physical copy or "mirror image" of all the data from the hard drive to preserve the data exactly as it existed at the time of seizure.[15] To do so, the examiner

---

13. *See* Guidance Software, ENCASE LEGAL J., Dec. 2003, at 24-26, *at* http://www.guidancesoftware.com/corporate/whitepapers/downloads/LegalJournal.pdf.

14. In general, execution of a traditional search warrant will be the only means by which law enforcement can obtain the original computer and related media. The technical and legal requirements of search warrants for computers and electronic information are of vital importance. Courts have examined a number of issues related to search and seizure of computers and electronic media with differing results. *See also* COMPUTER CRIME & INTELL. PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.cybercrime.gov/S&Smanual2003.htm; U.S. DEP'T OF JUSTICE, FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS (1994), *available at* http://www.cybercrime.gov. *Compare* United States v. Carey, 172 F.3d 1268, 1272-76 (10th Cir. 1999) (finding no Fourth Amendment violation and upholding search), *and* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (same), *and* United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998) (same), *and* United States v. Lacey, 119 F.3d 742, 745 (9th Cir. 1997) (same), *and* Davis v. Gracey, 111 F.3d 1472, 1479-80 (10th Cir. 1997) (same), *and* United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir. 1995) (same), *and* United States v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (same), *and* United States v. Lamb, 945 F. Supp. 441, 457-58 (N.D.N.Y. 1996) (same), *with* United States v. Kow, 58 F.3d 423, 427-28 (9th Cir. 1995) (finding constitutional violation and suppressing evidence). *See generally* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2002) (discussing a wide variety of search and seizure issues with respect to computers), *available at* http://www.mttlr.org/voleight/Brenner.pdf; Donald Resseguie, *Computer Searches and Seizures*, 48 CLEV. ST. L. REV. 185, 203-10 (2000) (discussing cases regarding computer searches and seizures); Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides With the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 109-19 (2000) (discussing Fourth Amendment issues in computer-based child pornography cases).

15. In the forensics field, a "mirror image" of the hard drive generally refers to a bit stream backup. A bit stream backup copies all files and data on the hard drive, including ambient data, which is data stored in nontraditional, not readily accessible storage areas within a computer. *See, e.g.*, *Technical Definitions, Bit Stream Back Up Defined*, New Technologies Inc., *at* http://www.forensics-intl.com/def2.html (last visited Dec. 19, 2004); *Technical Definitions, Ambient Data Defined*, New Technologies Inc., *at* http://www.forensics-intl.com/def1.html (last visited Dec. 19, 2004). Outside of the forensics field, the term "mirror image," is sometimes used to refer to hard drive copies that are neither bit stream copies, nor evidence grade quality. *See, e.g.*, Wolfgang Wilke, *Bit-*

may use a commercially available software program such as EnCase.[16] The software alone, or in conjunction with some additional software, allows the examiner to keep the data constant. Once the acquisition is completed, the software allows the examiner to make a mirror image of all or part of the computer media. The examiner can then use the mirror image for purposes of his forensic examination without corrupting or altering the original hard drive.[17]

The second step of a forensic investigation involves authenticating the electronic information acquired through the imaged computer media. Authentication ensures that the forensic image and the original computer media are identical. Again, the forensic software plays the primary role. The software creates a mathematical validation figure called a message digest (version 5) hash or what is generally referred to as an "MD5 hash."[18] An MD5 hash is an algorithm that takes a large chunk of data and transforms it into a number known as a hash or hash value.[19] The hash value corre-

---

Stream Image vs. Mirror Image, Lawyers-Be Careful What You Ask For! (Nov. 2003), *at* http://www.cybercontrols.net/common/wp.asp (requires registration).

16. EnCase is a graphic-based forensic program sold by Guidance Software, Inc. and is primarily used by law enforcement. It is designed to allow an investigator to use it from the beginning to the end of a forensic investigation. *See Law Enforcement*, Guidance Software, Inc., http://www.encase.com/markets/LawEnforcement/index.shtm (last visited Dec. 19, 2004). Other similar programs exist, many of which perform more specific functions. *See, e.g.*, *Forensic Security Software*, New Technologies, Inc., *at* http://www.forensics-intl.com/tools.html (last visited Dec. 19, 2004) (selling software programs for a wide variety of forensic tasks); *The Coroner's Tool Kit*, #RootPrompt.org, http://rootprompt.org/article.php3?article=738 (last visited Dec. 19, 2004) (describing The Coroner's ToolKit, a forensic program for use with Linux operating systems).

17. *See, e.g.*, Anthony F. DeSante, Evidentiary Considerations for Collecting and Examining Hard-Drive Media, at 4-7 (Nov. 28, 2001) (describing forensic imaging process), *at* http://www.computerteacher.org/DeSante%201101.pdf; *see also* James R. Lyle, *NIST CFTT: Testing Disk Imaging Tools*, 1 INT'L J. DIGITAL EVIDENCE, Winter 2003, at 1-10 (discussing standards and requirements for forensic imaging software), *at* http://www.ijde.org/docs/02_winter_art1.pdf; *cf.* Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90, 119-21 (D. Colo. 1996) (discussing use of disk imaging software and criticizing the plaintiff's expert for failing to use appropriate software).

18. An MD5 hash is one particular type of hash value. In general, "hashing" refers to transforming a string of characters or data into a much shorter, fixed-length value that represents the original string. *See Hashing*, SEARCHDATABASE.COM, *at* http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212230,00.html (last visited Dec. 19, 2004) (defining hashing). MD refers to the type of value created by hashing, in this case a message digest value. Other types of hashes exist, such as a Secure Hash Algorithm (SHA). *See id.* (discussing types of hashes).

19. An MD hash is an algorithm specifically meant for digital signature applications. The numerical version (for example, MD2, MD4, MD5) refers to the different types of algorithms, each of which were designed for slightly different purposes and for

sponds to the precise content of the information contained in the imaged copy of the seized computer, acting as a type of "electronic fingerprint" that enables the investigator to verify that the data on the imaged computer media is, and remains, identical to the data on the original computer. If even one bit of data is altered—say, one space of text is added—the hash value would change.[20]

The third step in a forensic examination is the recovery process through which the forensic examiner actually views and analyzes the data. This process entails the recovery of not only the data that was immediately accessible to the suspect user, but also hidden files with renamed file extensions,[21] deleted files,[22] evidence from swap files,[23] evidence from file

---

different size computers. MD5, the latest and most widely used version, creates a 128-bit hash value. *See What are MD2, MD4, and MD5*, RSA Laboratories, *at* http://www.rsasecurity.com/rsalabs/faq/3-6-6.html (last visited Dec. 19, 2004); *see also* Ray Ingles, *How Ostiary Works*, *at* http://ingles.homeunix.org/software/ost/works.html (last visited Dec. 19, 2004).

20. The odds of two computer files having the same hash value with different contents has been estimated to be roughly 10^{38}. *See, e.g.*, Richard Hardy & Susan Kreston, *"Computers are like Filing Cabinets . . .": Using Analogy to Explain Computer Forensics*, 15 NCPCA UPDATE NEWSL. No. 9 (Am. Prosecutors Research Inst., Alexandria, Va.), 2002 ("The scientific possibility of two different objects having the same MD5 hash value is more than 1 in 340 undecillion[,] . . . a higher level of certainty than even DNA enjoys."), *available at* http://www.ndaa.org/publications/newsletters/update_volume_15_number_9_2002.html. Despite the seemingly impossible chances of duplicate hash values, some commentators have noted that such duplication is not theoretically impossible. *See* Brian Deering, *Data Validation Using the Md5 Hash*, New Technologies, Inc., *at* http://www.forensics-intl.com/art12.html (last visited Dec. 19, 2004).

21. Computer file names have an extension that normally identifies the file type. For example, a text file will usually have a ".txt" extension and a picture file will usually have a ".jpg" extension. Computer users will sometimes change the file extension of files to hide the actual contents of the file. Most files, however, have an electronic data signature particular to that file. The signature allows file viewer programs to recognize the file regardless of the file extension. Forensic programs utilize the same process as file viewers and, therefore, can identify files that have renamed file extensions. *See Data Formats and Their File Extensions*, WEBOPEDIA COMPUTER DICTIONARY, http://www.webopedia.com/quick_ref/fileextensionsfull.asp (last visited Dec. 19, 2004) (providing an enormous list of file extensions with descriptions).

22. When a computer user deletes a file, it is not simultaneously removed from her computer. The physical location on the hard disk where the deleted file resides is marked by the computer as unallocated file space, which allows it to be overwritten. The file is not actually removed from the computer until another file overwrites it. While the file is marked for deletion (but not yet overwritten), it exists in unallocated file space. Forensic software allows an investigator to search and view the contents of the unallocated file space. *See, e.g.*, Joan E. Feldman, *The Basics of Computer Forensics*, 12 PRACTICAL LITIG. 17, 19-20 (2001); Hardy & Kreston, *supra* note 20.

slack,[24] metadata from unallocated clusters,[25] and other data.[26] During the recovery process, forensic examiners generally can recover any temporary

---

23. A swap file (sometimes referred to as a "page file") is a file located on the computer hard disk that is used to temporarily store information. The swap files are created automatically each time the computer is started. *See, e.g.*, JOHN R. MALLERY, SECURE FILE DELETION, FACT OR FICTION? 2 (SANS Inst., July 17, 2001), *at* http://www.sans.org/rr/papers/27/631.pdf; *Swap file*, Computer Hope, *at* http://www.computerhope.com/jargon/s/swapfile.htm (last visited Dec. 19, 2004); *Windows Swap/Page File Defined*, New Technologies Inc., *at* http://www.forensics-intl.com/def7.html (last visited Dec. 19, 2004).

Any data that appears on the computer screen can be written to a swap file. As a result, a forensic examiner can, with the right software, find information in swap files that otherwise would not be discoverable. Like cache "cleaners," there are both free and commercial programs that "wipe" a computer's swap files. *See, e.g.*, Jetico, Inc., *at* http://www.jetico.com (last visited Dec. 19, 2004) (listing information on BCWipe, a commonly used swap file wiper).

24. Understanding file slack requires understanding a computer's units of measure for data. Data are represented by bits and bytes. The smallest data unit is a bit. Next smallest are bytes, which consist of eight bits. For efficiency, bytes are stored in fixed-length blocks of data called sectors, which are usually 512 bytes. Thus, sectors are the smallest units of storage of data (bits and bytes) in a computer. A computer groups sectors into clusters, which allocate the data storage areas on a hard disk. *See* Craig Ball, *Can Your Old Files Come Back to Life?*, LAW.COM (Jan. 15, 2004), *at* http://www.law.com/special/supplement/e_discovery/old_files.shtml; *Sector Defined*, New Technologies Inc., *at* http://www.secure-data.com/def15.html (last visited Dec. 19, 2004); *Cluster Defined*, *at* http://www.forensics-intl.com/def19.html (last visited Dec. 19, 2004).

The amount of information in a given file usually does not fill exactly one or more clusters. Consequently, there is left over physical space in the cluster. This space is called file slack. When file slack exists in a cluster, the operating system pads the remaining space in the cluster with the data that was in the cluster previously. That previous data is data that the user has marked for deletion, but that has not been overwritten yet. (If there is additional space left over in a sector, the computer also fills that space. Instead of using left over deleted material, though, the computer randomly selects data from the memory of the computer (known as RAM slack) to fill out the sector.) Because file slack contains potentially enormous amounts of unseen data on a computer, a forensic examiner can search file slack for various types of information that would not be otherwise available. *See, e.g.*, Ball, *supra*; Matthew Schwartz, *Shell Game*, Enterprise Systems (June 12, 2002), *at* http://www.esj.com/Columns/article.asp? EditorialsID=88.

25. A metafile is a file that contains information describing another file. *See, e.g.*, *Metafile*, WEBOPEDIA COMPUTER DICTIONARY, *at* http://www.webopedia.com/TERM/M/metafile.html (last visited Dec. 19, 2004). For example, when a user prints a file, the computer automatically makes a copy of that file and sends the copy to the printer. After the file goes to the printer, the copy is deleted. That copy is called a metafile. In general, a user is neither told of the creation of the metafile, nor is able to view it. *See generally id.* Most forensic software programs, however, are able to recover metafiles from a computer, thereby allowing the examiner to investigate the content of those metafiles.

26. Another significant area where forensic examiners can uncover hidden data in the context of child pornography investigations is the index.dat file. The index.dat file, a

Internet files from a computer's cache, along with detailed information about those files. In addition, examiners can learn extensive information about a suspect's browsing history, including the particular websites visited, the number of times visited, the degree of manipulation (such as enlarging, cutting, or pasting) of images, and any downloading activity.[27] Once the examination is complete and the information has been gathered, prosecutors must determine whether the results justify a criminal charge.

III. STATUTES

A. Federal

Most courts that have addressed whether the presence of images in a defendant's computer's cache constitutes knowing possession have done so in prosecutions charged under federal law. The federal child pornography statute is codified at 18 U.S.C. § 2252A.[28] Section 2252A prohibits, in

---

file in Microsoft's Internet Explorer web browser, records information about sites that a computer user has visited. Even if a user deletes the actual files in his computer's cache, the index.dat file will still keep a record of the visited sites, among other information. *See, e.g.*, John Marcovich, *All about index.dat files*, www.EXITS.ro (2003), *at* http://www.exits.ro/index-dat-files.html; WinGuides Software, *What is index.dat?*, *at* http://www.winguides.com/security/article.php/12 (last visited Dec. 19, 2004).

27. *See generally* Jeff Flax, Your Client's Computer Has Been Seized—Now What?, Presentation at National Seminar for Federal Defenders (June 5-7, 2000), *available at* http://www.dcfpd.org/2000seminar/flax.pdf (describing various types of recoverable evidence, where the computer stores it, and how investigators find it).

28. *See* Pub. L. No. 104-208, 110 Stat. 3009, 3009-26 (1996) (adding 18 U.S.C. § 2252A and amending §§ 2251, 2252, 2256). Congress added § 2252A as part of the Child Pornography Protection Act of 1996 ("CPPA"). Section 2252A was not the first effort by Congress to address the ills of child pornography. In 1977, Congress enacted the Protection of Children Against Sexual Exploitation Act of 1977 ("1977 Act"). *See* Pub. L. No. 95-225, 92 Stat. 7 (1978) (codifying the 1977 Act). The portion of the 1977 Act later codified at § 2252 focused on the use of real children in the production of child pornography. *See* 18 U.S.C. § 2252 (2000) (prohibiting knowing transportation, receiving, distributing, selling, or possessing of material produced using an actual minor engaging in sexually explicit conduct). Congress purposefully designed § 2252A to mirror the language and penalties of § 2252. *See* S. REP. NO. 104-358 (1996), 1996 WL 506545, at *9-*10 (describing the interplay between § 2252 and § 2252A). Several of the cases in this Article deal with possession or receiving charges brought under § 2252—not § 2252A. *See, e.g.*, United States v. Hall, 142 F.3d 988 (7th Cir. 1998); United States v. Mader, No. NMCM 99 01007, 2000 WL 1455260 (N-M. Ct. Crim. App. Sept. 18, 2000). In 2002, the Supreme Court struck down portions of the CPPA as unconstitutional. *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 258 (2002) (holding that portions of the CPPA banning virtual pornography violated the constitutional right to free speech). The particular portions were in the definitions section of the CPPA, which were codified at §§ 2256(8)(B) and 2256(8)(D). *Id.* Although beyond the scope of this Article, a spate of

pertinent part, knowingly possessing "any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer."[29] The term "child pornography" is further described in § 2256(8).[30]

B. States

Like the United States Congress, state legislatures have enacted statutes that prohibit the possession of child pornography. Although the statutes are organized in different ways and under different names, they are strikingly similar in effect. In each case, the statute requires some level of intent—usually "knowingly"—and defines the specific character of the prohibited images.[31] In addition, states have incorporated within their

---

commentators have analyzed the history and effect of the *Ashcroft* decision. *See, e.g.*, Sarah C. Marcy, *Banning Virtual Child Pornography: Is There Any Way Around* Ashcroft v. Free Speech Coalition?, 81 N.C. L. REV. 2136 (June 2003); Timothy Perla, Note, *Attempting to End the Cycle of Virtual Pornography Prohibitions*, 83 B.U. L. REV. 1209 (2003); Emanuel Shirazi, Note, *How to Constitutionally Protect Against Child Pornography*, 25 HASTINGS COMM. & ENT. L.J. 343 (2003). For a brief, related discussion of the *Ashcroft* decision's effect on potential defenses in child pornography possession cases, see *infra* Part VI.D.

29. 18 U.S.C. § 2252A(a)(5)(B).

30. Section 2256(8) defines "child pornography" as:

> any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. § 2256(8)(A)-(C) (Supp. II 2002).

31. *See, e.g.*, ALA. CODE § 13A-12-192(b) (2003) (entitled "Possession of obscene matter"); ALASKA STAT. § 11.61.127(a) (Michie 1998) (entitled "Possession of child pornography"); ARK. CODE ANN. § 5-27-304(a)(2) (Michie 1997) (entitled "Pandering or possessing visual or print medium depicting sexually explicit conduct involving a child"); CAL. PENAL CODE § 311.11(a) (West 1999) (entitled "Possession or control of matter depicting minor engaging or simulating sexual conduct"); CONN. GEN. STAT. § 53a-196d(a) (2001) (entitled "Possessing child pornography"); DEL. CODE ANN. tit. 11, § 1111 (2001) (entitled "Possession of child pornography"); FLA. STAT. ch. 827.071(5) (2001) (entitled "Sexual performance by a child"); HAW. REV. STAT. § 707-752(1) (2002) (entitled "Promoting child abuse in the third degree"); IND. CODE § 35-42-4-4(c) (2002) (entitled "Child exploitation; possession of child pornography"); IOWA CODE § 728.12.3 (Supp. 2003) (entitled "Sexual exploitation of a minor"); LA. REV. STAT. ANN. § 81.1(3)

child pornography statutes phrases and terms that explicitly address computer-generated and distributed images.[32]

C. Purposes of Statutes

Despite differing language, the purposes of the federal and state statutes that prohibit possession of child pornography are largely the same. The statutes focus on preventing pedophiles and sexual abusers from stimulating their appetites, protecting children, and encouraging the elimination of existing contraband.[33] The prohibition on possession attempts to reduce the demand for child pornography and to prevent criminal behavior that might be induced or encouraged by such contraband.[34] Put another way, the emphasis of the statutes is to address the potential negative externalities created by child pornography possession as well as the market for the actual child pornography.[35]

(West 2004) (entitled "Pornography involving juveniles"); MINN. STAT. ANN. § 617.247(4) (West 2003) (entitled "Possession of pornographic work involving minors"); MO. REV. STAT. § 573.037.1 (1999) (entitled "Possession of child pornography"); NEV. REV. STAT. 200.730 (2001) (entitled "Possession of visual presentation depicting sexual conduct of person under 16 years of age unlawful"); N.H. REV. STAT. ANN. § 649-A:3.I(e) (Supp. 2003) (entitled "Child Pornography: Offenses"); N.M. STAT. ANN. § 30-6A-3.A (Michie 2001) (entitled "Sexual exploitation of children"); N.Y. PENAL LAW § 263.11 (McKinney 1996) (entitled "Possessing an obscene sexual performance by a child"); OHIO REV. CODE ANN. § 2907.322(5) (West 2000) (entitled "Pandering sexually oriented matter involving a minor"); OKLA. STAT. tit. 21, § 1024.2 (2002) (entitled "Purchase, procurement or possession of child pornography"); 18 PA. CONS. STAT. ANN. § 6312(d) (West. Supp. 2003) (entitled "Sexual Abuse of Children"); S.D. CODIFIED LAWS § 22-22-24.2 (Michie 2002) (entitled "Possessing, manufacturing or distributing child pornography"); TEX. PENAL CODE ANN. § 43.26 (Vernon 2003) (entitled "Possession or Promotion of Child Pornography"); UTAH CODE ANN. § 76-5a-3(1)(a) (2003) (entitled "Sexual exploitation of a minor"); VT. STAT. ANN. tit. 13, § 2827 (1999) (entitled "Possession of child pornography"); VA. CODE ANN. § 18.2-374.1.1. (Michie 1992 & Supp. 2003) (entitled "Possession of child pornography"); WASH. REV. CODE § 9.68A.070 (2003) (entitled "Possession of depictions of minor engaged in sexually explicit conduct"); WIS. STAT. § 948.12 (2001) (entitled "Possession of child pornography").

32. *See supra* note 31 (listing state statutes).

33. *See, e.g.*, S. REP. NO. 104-358 (1996), 1996 WL 506545, at *2.

34. *See, e.g.*, 1991 Ark. Acts 607, § 2 (stating that the intent of the Act was to "protect victims of child pornography and to destroy a market for the exploitive use of children" and that the intent of penalizing child pornography possession was "to significantly decrease production of, and demand for, the material"); S. REP. NO. 104-358, 1996 WL 506545, at *3 (noting that prohibiting possession of child pornography will encourage possessors to destroy material, thereby "helping to protect the victims of child pornography and to eliminate the market for the sexual exploitive use of children");.

35. *See, e.g.*, Osborne v. Ohio, 495 U.S. 103, 109-11 (1990) (discussing Ohio and other states' interests in prohibiting child pornography possession generally and noting

Although the language and goals of the various child pornography possession statutes are similar, the manner in which courts have analyzed them is not. Turning to those analyses, the next Part surveys how various courts have construed child pornography possession laws with respect to images found in a defendant's computer's cache.

IV. CASE LAW REGARDING KNOWING POSSESSION AND CACHED FILES

Courts have treated cache-possession issues in different ways. While the majority of courts has determined that a cached image is sufficient to show knowing possession, others have rejected this view. Still more, other courts have simply noted the issue without providing any detailed explanation for the resolution of the issue.

A. Courts Holding that Images in a Cache Constitute Possession

The majority of courts have determined that images in a cache are sufficient to show possession. The type and degree of analysis of the different courts, however, have varied greatly.

1. United States v. Tucker

The leading case specifically holding that images located in a cache are sufficient to show knowing possession is *United States v. Tucker*.[36] In that case, parole officers discovered suspected child pornography on the defendant's computer.[37] The officers seized the computer and took it to the local police, who then performed a forensic examination.[38] The initial search and later examination of the hard drive revealed numerous images of child pornography located in the browser cache, recycle bin, and C-drive.[39]

During interviews with police, Tucker admitted to viewing several hundred images of children engaged in sexual acts.[40] He also admitted that he deleted his computer's cache after viewing pornographic pictures be-

---

specifically that one such purpose is to prevent pedophiles from using child pornography to seduce other children); New York v. Ferber, 458 U.S. 747, 756-58 (1982) (discussing legislative judgments in combating child pornography); *see also* 1 ATTORNEY GENERAL'S COMM'N ON PORNOGRAPHY, FINAL REPORT 649 (1986) (describing pedophiles' use of child pornography to lure other children).

36. 150 F. Supp. 2d 1263 (D. Utah 2001) [hereinafter *Tucker I*], *aff'd*, 305 F.3d 1193 (10th Cir. 2002) [hereinafter *Tucker II*].

37. *Tucker I*, 150 F. Supp. 2d at 1264-65.

38. *Id.* at 1265-66.

39. *Id.* at 1266.

40. *Id.* at 1265.

cause it was something "he always did."[41] Based on the evidence and Tucker's admissions, the government charged him with knowing possession of child pornography under 18 U.S.C. § 2252A(a)(5)(B).[42]

During the bench trial, prosecutors offered evidence establishing that Tucker participated in Internet newsgroups that provided child pornography to subscribers who paid a fee.[43] By subscribing to the newsgroups, Tucker received a password allowing access to several thousand images of child pornography, which he viewed often.[44] The trial court heard additional evidence that, when visiting these websites, Tucker would view "thumbnail"[45] pictures of child pornography, and then select certain thumbnails to enlarge and view further.[46]

Tucker stipulated that the images in question were placed in interstate commerce and depicted child pornography as defined by statute.[47] Tucker further conceded that he viewed those images.[48] He maintained, however, that he did not violate the statute for two reasons. First, Tucker argued that he never "possessed" the images because he never downloaded or copied them and because he affirmatively deleted the images in his computer's cache.[49] Second, Tucker claimed that, even if he possessed the images, his possession was not knowing because the computer automatically stored the images in its cache without any action on his part.[50]

Turning to Tucker's first argument, the district court began by reviewing the traditional and legal definitions of the term possession.[51] The court's analysis centered on Tucker's ability to manipulate the images as

---

41. *Id.*

42. *Id.* at 1266.

43. *Id.* at 1265.

44. *Id.*

45. A thumbnail is "a miniature display of a page to be printed," which allows the user "to view the layout of many pages on the screen at once." *Thumbnail*, WEBOPEDIA COMPUTER DICTIONARY, *at* http://www.webopedia.com/TERM/t/thumbnail.html (last visited Dec. 19, 2004).

46. *Tucker I*, 150 F. Supp. 2d at 1265.

47. *Id.* at 1266.

48. *Id.*

49. *Id.* at 1268

50. *Id.* at 1266, 1269.

51. *Id.* at 1266-67 (noting various definitions of "possession," including "to exercise authority, dominion or control over a given thing" (quoting EDWARD J. DEVITT ET AL., FEDERAL JURY & PRACTICE INSTRUCTIONS, CRIMINAL § 36.12 (4th ed. 1992); "the exercise of physical detention or control over a thing" (citing BLACK'S LAW DICTIONARY 1184 (7th ed. 1999); and "an appreciable ability to guide the destiny" of contraband (citing United States v. Massey, 687 F.2d 1348, 1354 (10th Cir. 1982)).

well as the actual manipulation of the images.[52] In particular, the court focused on Tucker's ability to control the images found in his computer's cache: "[Tucker] could control [the images] in many ways: he could copy them had he chosen; he could print them had he chosen; he could enlarge them and 'zoom-in' on the pictures as he chose; he could show them to other [sic] had he chosen;[53] and he could copy them to other directories . . . ."[54] The court found particularly significant Tucker's deletion of many of the recovered images, explaining that Tucker's possession "is not only evidenced by his showing and manipulation of the images, but also by the telling fact that he took the time to delete the image links from his computer cache file."[55] Indeed, the court concluded that "[l]ogically, one cannot destroy what one does not possess and control . . . . [T]he ability to destroy is definitive evidence of control."[56]

The court rejected Tucker's claim that his deletion of the files relieved him of criminal liability and that he could not possess that which he did not intentionally download or store.[57] With respect to the destruction argument, the court found Tucker's reliance on dicta in *United States v. Hall* misplaced.[58] Moreover, the court repeated its earlier statement that destruction of the files actually supported the conclusion that Tucker volitionally possessed the images.[59] Drawing an analogy to narcotics cases, the court remarked that "[j]ust as a possessor of illegal narcotics is not able to escape criminal liability for possession by throwing drugs out a

52. *Id.* at 1267-69.

53. Although the court did not cite this evidence in *Tucker I*, the *Tucker II* court recounted that the defendant showed a friend some images of child pornography on his computer. The friend reported this episode to another friend who, in turn, notified a contact in the United States Attorney's Office. That report eventually led to the search and seizure of the computer and the federal charges at issue in the instant cases. *See Tucker II*, 305 F.3d 1193, 1196-97 (10th Cir. 2002).

54. *Tucker I*, 150 F. Supp. 2d at 1267.

55. *Id.*

56. *Id.*

57. *Id.* at 1267-68.

58. 142 F.3d 988 (7th Cir. 1998). In *Hall*, the defendant affirmatively downloaded numerous computer images of child pornography onto his computer's hard drive. The defendant argued that he did not possess the child pornography, but rather just viewed it, analogizing his conduct to watching images on television. *Id.* at 997. The *Hall* court rejected the analogy, observing, in pertinent part, that "Hall had every opportunity to delete any computer files that he did not wish to retain." *Id.* Tucker maintained that this dicta stood for the proposition that deletion relieved him of liability. The *Tucker I* court, however, noted that the *Hall* court specifically "did not address what kinds of activity would constitute possession" because that issue was not before it. *Tucker I*, 150 F. Supp. 2d at 1267.

59. *Tucker I*, 150 F. Supp. 2d at 1268.

window, a person who possesses contraband such as child pornography cannot escape criminal liability by destroying it."[60]

The court similarly rejected Tucker's claim that he could not possess something without affirmatively downloading it. In particular, the court noted that contrary to Tucker's claims, the Internet neither put the images on his computer on its own, nor exercised any volition.[61] Rather, Tucker himself "purposefully visited Internet sites for the express purpose of viewing child pornography . . . . The images would not have been saved to his cache file had Tucker not volitionally reached out for them."[62]

Turning to Tucker's second argument—that he did not "knowingly" possess—the court again began by reviewing the traditional definitions of "knowingly" in the context of criminal possession.[63] Thereafter, the court concluded that Tucker knowingly possessed the images. In reaching its conclusion, the court largely reiterated its earlier point that it was Tucker who "volitionally reached out" for the images.[64] The court also noted that Tucker paid a user fee and had a specific password to provide entry to the pornographic websites.[65] Finally, the court found that Tucker further demonstrated his scienter by deleting the cached files after his Internet sessions.[66] Having determined that Tucker knowingly possessed the images in his computer's cache, the district court entered an order finding him guilty of the charges.[67]

Tucker appealed the district court's order to the United States Court of Appeals for the Tenth Circuit on several grounds, including that there was insufficient evidence to support a conviction for knowingly possessing child pornography.[68] On appeal, he argued that did not possess child por-

---

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.* at 1269 (stating that "knowingly" means that the defendant was "conscious and aware of his actions, realized what he was doing or what was happening around him, and did not act because of ignorance, mistake, or accident" (citing EDWARD J. DEVITT ET AL., FEDERAL JURY & PRACTICE INSTRUCTIONS § 17.04 (4th ed. 1992)).

64. *Id.*

65. *Id.*

66. *Id.* (noting that the "[defendant] would not know to delete the [pornographic images] if he did not know that he possessed them").

67. *Id.* at 1269-70.

68. *See Tucker II*, 305 F.3d 1193, 1204 (10th Cir. 2002). Tucker also argued on appeal that (1) the investigators lacked probable cause to search his home and (2) the investigators lacked probable cause to search and seize his computer. *Id.* at 1199-1201.

nography but rather merely viewed it on his computer.[69] In doing so, he made two related arguments.

First, Tucker argued that the images he viewed did not meet the definition of child pornography under § 2252 because they were not "stored" in his computer.[70] The Tenth Circuit summarily rejected this argument in a footnote, observing that Tucker simply misread the definitional section of the statute.[71]

Second, Tucker argued that, even though he knew that his computer saved copies of webpages he viewed in a cache, he did not desire the computer to do so and affirmatively deleted the cached files after each session.[72] The Tenth Circuit found this argument equally unpersuasive, noting that the defendant "intentionally sought out and viewed child pornography knowing that the images would be saved on his computer."[73] The court thereafter concluded that his conduct was voluntary[74] and affirmed the conviction.[75]

---

69. *Id.* at 1204.

70. *Id.* at 1204 n.15. Defendant's argument rested on his reading of several defined terms within Title 18. The charging statute, § 2252, criminalizes possession of child pornography. Section 2256(8) defines "child pornography" to include, in pertinent part, "any visual depiction, including . . . [a] computer or computer-generated image or picture . . . of sexually explicit conduct" performed by minors. 18 U.S.C. § 2256(8) (2000). The term "visual depiction" is further defined as including "data stored on computer disk . . . which is capable of conversion into a visual image." *Id.* § 2256(5).

71. *Tucker II*, 305 F.3d at 1204 n.15 ("Section 2256 does not require a visual depiction to be stored data. Rather the definition merely says that one type of visual depiction is data stored on computer.").

72. *Id.* at 1204.

73. *Id.* at 1205.

74. In doing so, the Tenth Circuit distinguished Tucker's analogy to *Martin v. State*, 17 So. 2d 427 (Ala. Ct. App. 1944). In *Martin*, an intoxicated bar patron was carried involuntarily from inside a tavern to a public place and thereafter charged with public drunkenness. 17 So. 2d at 427. The court held that voluntariness was a necessary element of the crime. Consequently, because the defendant did not appear in public voluntarily, the court dismissed the charge. *Id.* The Tenth Circuit distinguished *Martin* by observing that the defendant in Martin "did not drink with the understanding that he would be taken out in public," *Tucker II*, 305 F.3d at 1205, whereas Tucker clearly did understand that the images he viewed would be saved in his computer's cache file temporarily. *Id.*

75. The *Tucker II* court explicitly stated that it offered no opinion on "whether an individual could be found guilty of knowingly possessing child pornography if he viewed such images over the Internet but was ignorant of the fact that his Web browser cached such images." 305 F.3d at 1205 n.16.

2. *Other Cases*

Several other courts, both before and after *United States v. Tucker* (both district and appellate cases), have found that images located in a cache are sufficient to establish possession. Two such cases, *United States v. Mason*[76] and *United States v. Sanchez*,[77] were decided by the Air Force Court of Criminal Appeals.[78] In *Mason*, the defendant plead guilty to knowingly receiving child pornography under 18 U.S.C. § 2252A, as well as several violations of military law.[79] The defendant later appealed his convictions on several grounds, including that his guilty plea to AFI 33-129, paragraph 6.1.3[80] was improvident because he did not know that viewing an image on the Internet caused his computer to "store" the image in the cache folder.[81] Because he claimed the alleged storing was unintentional, Mason asked the appellate court to excise that term from his pleas[82] and to reconsider his sentence.[83] The court rejected Mason's argument. Specifically, the court noted that "[the defendant] admitted that he used his government computer to find and view the offensive or obscene materials, and that by opening the document it was stored—however temporarily—in a cache within the government computer."[84]

In *Sanchez*, the defendant was convicted of, among other charges, knowing possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(a).[85] When investigators performed a forensic examination on Sanchez's computer, they found twenty-three images of child pornography that were located on the computer hard drive or in a temporary Internet file.[86] Twelve of the images found were consistent with images

---

76. No. ACM34394, 2002 WL 1757175 (A.F. Ct. Crim. App. Jun. 11, 2002), *aff'd*, 60 M.J. 15 (C.A.A.F. 2004).

77. 59 M.J. 566 (A.F. Ct. Crim. App. 2003), *aff'd in part and rev'd in part*, United States v. Jenson, No. 04-0226, 60 M.J. 330 (C.A.A.F. Sept. 9, 2004), *review granted*, United States v. Sanchez, No. 04-0157, 60 M.J. 331 (C.A.A.F. Sept. 9, 2004).

78. The Air Force Court of Criminal Appeals is the intermediate appellate court for military matters.

79. *See Mason*, 2002 WL 1757175, at *1.

80. AFI 33-129, ¶ 6.1.3 prohibits "storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material."

81. *Mason*, 2002 WL 1757175, at *9.

82. *See id.* (noting the specification to which defendant pleaded guilty stated that he used his government computer "to process, store or otherwise transmit" obscene language and materials).

83. *Id.*

84. *Id.* at *10.

85. United States v. Sanchez, 59 M.J. 566, 566 (A.F. Ct. Crim. App. 2003).

86. *Id.* at 570; *see also supra* note 2 and accompanying text (discussing temporary Internet files).

that had been automatically saved to the computer by the web browser.[87] Sanchez argued that, because the computer automatically saved the images, he did not knowingly or meaningfully possess the files.[88] Like the *Mason* court, the *Sanchez* court found the defendant's claims meritless. The court reasoned that because Sanchez had subscribed to several "e-groups" described as nude teen sites, he could not claim ignorance of "remnant images on his computer hard drive."[89] In addition, the court noted that a witness testified to Sanchez's relative sophistication with computers, a factor that the court apparently found further rebutted the defendant's lack of knowledge argument.[90] Finally, the court pointed out that the forensic examination revealed that several of the images had been attached to an e-mail that Sanchez received at his own, password-protected e-mail address and that he attempted to manipulate and forward that e-mail.[91] Based on those findings, the court affirmed the lower court's decision.[92]

The most recent cases raising the cache-possession issue have occurred at the state level. In *State v. Knode*,[93] the Ohio Court of Appeals affirmed the defendant's conviction under Ohio's child pornography statute[94] based, in part, on his knowing possession of images in a temporary Internet file.[95] The court noted the explanation of temporary Internet files by the officers who performed the forensic examination on Knode's computer, as well as the forensic evidence showing that Knode had visited several child pornography sites and enlarged at least one thumbnail image from those websites.[96] The court engaged in little analysis of the cache-possession issue, but concluded that the jury acted reasonably and that "the data trail that led to [a trial exhibit] as a thumbnail image evidenced knowledge of the character of the material contained in the image as well as possession of the image."[97]

---

87. *Sanchez*, 59 M.J. at 570.
88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. No. 03CA014, 2003 WL 23094953 (Ohio App. Dec. 31, 2003).
94. OHIO REV. CODE § 2907.322(a)(5) (West 2000) (stating that no person shall knowingly "possess[] or control any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality").
95. *Knode*, 2003 WL 23094953, at *5-*6.
96. *Id.*
97. *Id.* at *6.

Shortly before the *Knode* decision, a Virginia Circuit Court held that images found in a defendant's cache file were sufficient to establish his knowing possession of child pornography.[98] In *Commonwealth v. Simone*, prosecutors charged the defendant with four counts of possessing child pornography under Va. Code § 18.2-374.1:1.[99] Of the four counts, three were based on images that were discovered in the Simone's computer cache.[100] Simone argued at trial that he could not be convicted of knowingly possessing the three cached images because they could appear as a result of "pop-up"[101] websites that he did not intentionally visit or manually download.[102]

The *Simone* court began its analysis by reviewing the reasoning in *Tucker II* and noting that, unlike the *Tucker* cases, prosecutors presented no evidence that Simone knew that the images he viewed were saved in his computer's cache.[103] The court also observed that the Virginia statute prohibited possession—not viewing.[104] From that foundation, the court ascertained that the critical inquiry to determine possession was whether Simone "reach[ed] out for and control[led] the images at issue."[105]

To aid in answering that question, the court drew an analogy between the images in the cache file and narcotics on a sidewalk.[106] The court reasoned that if a person walking down the street stopped, looked at the narcotics long enough to recognize what they were and then walked away, the person would not be guilty of possessing the narcotics.[107] The court then distinguished that person's conduct from someone who looked at the nar-

---

98. Commonwealth v. Simone, No. CRIM 03-0986, 2003 WL 22994245, at *7 (Va. Cir. Ct. Nov. 12, 2003).

99. *Id.* at *1. Section 18.2-374.1:1 provides that "[a]ny person who knowingly possesses any sexually explicit visual material utilizing or having as a subject a person less than eighteen years of age shall be guilty of a Class 1 misdemeanor." VA. CODE ANN. § 18.2-374.1.1 (Michie 1992 & Supp. 2003).

100. *Simone*, 2003 WL 22994245, at *2 (noting that three images were from "the computer's AOL 4.0 directory cache" and one image was from the "wallpaper" electronically placed on the computer screen).

101. *See infra* note 202 (citing sources explaining "pop-up" banners).

102. *Simone*, 2003 WL 22994245, at *3; *see also infra* Part VI.B (discussing "accidental viewing" defense).

103. *Id.* at *5-*6.

104. *Id.* at *6.

105. *Id.* The court further noted that asking whether the defendant reached out for and controlled the images promoted the purpose of the statute, which included "protection of the physical and psychological well being of juveniles . . . and destruction of the market for the exploitative use of children." *Id.* (citations omitted).

106. *Id.* at *7.

107. *Id.*

cotics long enough to recognize them and then reached out, picked them up, and carried them home.[108] In the latter case, according to the court, the person's conduct changed from "merely viewing" to "knowingly possessing" because the person reached out and controlled the narcotics.[109] Drawing on its analogy, the court concluded that Simone's conduct more closely resembled the latter situation than the former.[110] Specifically, the court noted that (1) Simone had performed various searches for child pornography using terms like "Lolita" and "pedophilia"; (2) police found print outs of graphic sexual stories involving children; and (3) Simone possessed a fourth image of child pornography found on his computer's wallpaper.[111] Based on those findings, the court concluded that there were no doubts about how the "three cached images found their way into the temporary Internet files on this computer" and that Simone's actions proved beyond a reasonable doubt "that he reached out for and controlled the three images contained in his computer's cache/temporary Internet file."[112]

B. Courts Holding that Images in a Cache Do Not Constitute Possession

The only court to hold that images in a cache do not constitute knowing possession is the United States Court of Appeals for the Eighth Circuit, which affirmed an unpublished ruling from a district court in Missouri. Unfortunately, the limited written record and relatively sparse analysis makes assessment of that holding somewhat difficult.

1. United States v. Stulock

In *United States v. Stulock* police searched the defendant's home following a sting operation during which the defendant ordered video tapes of child pornography.[113] Among the items seized was the defendant's computer.[114] A forensic examination of the computer revealed multiple files containing child pornography in several locations, including three images found in the browser cache.[115] Stulock was charged with know-

108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. 308 F.3d 922, 924 (8th Cir. 2002).
114. *Id.*
115. *Id.* at 924-25. The examination discovered thousands of deleted files recovered from the defendant's temp directory and on a secondary hard disk configured as the F-drive. Unlike most of the files recovered, the three images in the cache were not deleted.

ingly receiving and knowingly possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), respectively.[116] The possession charges were based solely on the three images in Stulock's computer's cache.[117] After a bench trial, the district court acquitted Stulock of the possession charges, but convicted him of knowingly receiving the videotape.[118] Thereafter, Stulock appealed.

In reviewing the history of the case, the Eighth Circuit summarized the proceedings, including the acquittal of the possession charges. The district court's reasoning for the acquittal, as recounted by the Eighth Circuit, was that "one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically saved in the browser's cache, without having purposely saved or downloaded the image."[119] Although the district court did not produce a written opinion, the transcript of the lower proceedings confirms the Eighth Circuit's summary. The district court further explained its views during sentencing: "the reason I acquitted the defendant on [the possession charge] was because the three images alleged in the indictment were on the cache files, and understanding the technical way the computer works, I did not believe that defendant actually possessed those three images."[120]

2. Other Cases

No other court has explicitly held that images within a computer's cache are insufficient to establish knowing possession. Several courts have highlighted the general issue without opinion,[121] while others have suggested that, even if cached images do constitute possession, it is less se-

---

In addition to the images themselves, investigators also were able to recover the defendant's web history, showing that the defendant had visited a number of child pornography sites. *Id.*

116. *Id.* at 925.

117. *Id.*

118. *Id.*

119. *Id.*

120. Brief of Appellee, United States v. Stulock, 308 F.3d 922 (8th Cir. 2002) (No. 02-1401) (quoting Sentencing Transcript at 15), 2002 WL 32139385, at *31 n.1 (on file with author).

121. *See, e.g.*, United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003).

vere conduct than traditional types of possession.[122] Scholarly comment on the issue has been similarly limited.[123]

C. Courts that Provided Unclear or Insufficient Analysis

Finally, several cases that dealt with images found in a cache are of questionable guidance due to the courts' limited discussion or inexact language. For example, in *United States v. Hall*, the government charged Hall with one count of knowingly possessing child pornography and three counts of knowingly receiving child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and § 2252(a)(2), respectively.[124] Following a bench trial, the court convicted Hall of two counts of knowingly receiving child pornography.[125] Thereafter, Hall appealed to the United States Court of Appeals for the Sixth Circuit.

Hall claimed on appeal, among other things, that there was insufficient evidence to support his conviction.[126] Significantly, several of the images at issue were located in his computer's cache.[127] Hall argued that he did not have knowing possession of child pornography. Yet, ironically, he premised that argument on his lack of knowledge that the images were *pornographic*—not on his lack of knowledge that the images were *located within his computer's cache.*[128] The Sixth Circuit rejected Hall's argument and affirmed the lower court's holding. Unfortunately, it is unclear from the court's opinion whether the convictions were based upon the images in the cache or other images.[129]

---

122. *See* United States v. Parish, 308 F.3d 1025 (9th Cir. 2002) (affirming district court's eight-level downward departure during sentencing of a child pornography defendant because, among other things, the defendant only had images in his cache file). For a further discussion of *Parish*, see *infra* notes 138-141 and accompanying text.

123. *Cf.* Matthew James Zappen, Comment, *How Well Do You Know Your Computer? The Level of Scienter in 18 U.S.C. § 1462*, 66 ALB. L. REV. 1161, 1165-76 (2003) (discussing various types of computer activity, including caching, and whether they can or should give rise to criminal liability).

124. No. 98-6421, 2000 WL 32010, at *1 (6th Cir. Jan. 4, 2000).

125. *Id.* at *1-*2.

126. *Id.* at *4.

127. *Id.* at *1. The other files were located in the active area of the defendant's computer's hard drive and in the "erase file," the inactive part of the defendant's computer's hard drive. *Id.*

128. *Id.* at *4-*5.

129. *See generally id.* A similar confusion arose recently in *State v. Lindgren*, 687 N.W.2d 60 (Wis. Ct. App. 2004). In *Lindgren*, the court affirmed the defendant's conviction for possession of child pornography. The images in question were, according to the court, "on the hard drive" of the defendant's computer. *Lingren*, 687 N.W.2d at 65, ¶ 21. In assessing the defendant's argument that he never possessed the images, the court quoted and adopted *Tucker II*'s reasoning. *Id.* at 67, ¶ 27. It remained unclear, however,

Later that same year, the Navy-Marines Court of Criminal Appeals addressed another child pornography case, but again provided little guidance. In *United States v. Mader*, Mader appealed from his guilty plea to charges which included possessing and receiving child pornography under 18 U.S.C. § 2252 and several military law violations.[130] On appeal, he argued, among other things, that certain charges were duplicative.[131] In rejecting Mader's argument, the court stated confusingly that the defendant "wrongfully received the graphic files when he downloaded the files over a period of time into the cache of his personal computer and viewed them."[132] The court then continued: "[t]he wrongful possession of the files occurred when [the defendant] saved the files to his hard drive and zip diskettes."[133]

The *Mader* court's dicta is troubling. First, it is unclear whether the court uses the term "cache" in its technical sense as a temporary Internet file or simply as another term for "storage." If the court intended the latter usage, then it appears to be suggesting that files within a computer's cache are sufficient to show receipt of an image, but that possession does not occur until the images are actively saved to a hard drive or diskette. Conversely, if the court intended the former usage, then it appears that the court used imprecise language in describing the conduct at issue. In either scenario, the court's analysis lacks clarity.

Other courts have addressed the cache-possession issue tangentially. In *United States v. Parish*, the defendant plead guilty to two counts of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).[134] The images of child pornography underlying the charges were found exclusively in the defendant's computer's temporary Internet files,[135] and there was no evidence that he "had actively downloaded and stored any of the images."[136] At the sentencing hearing, the district court departed downward from the sentencing guidelines eight levels, relying largely on testimony that the defendant's conduct was "out-

---

whether the images in *Lindgren* were at least in part cached images or all saved images accurately described as on the defendant's hard drive.

130. No. NMCM 99 01007, 2000 WL 1455260 (N-M. Ct. Crim. App. Sept. 18, 2000).

131. *Id.* at *2.

132. *Id.*

133. *Id.*

134. 308 F.3d 1025, 1028 (9th Cir. 2002).

135. *Id.* at 1027.

136. *Id.* at 1028.

side the heartland" of United States Sentencing Guideline § 2G2.4.[137] The government appealed.

On appeal, the United States Court of Appeals for the Ninth Circuit affirmed the decision of the district court to downward depart.[138] The court reviewed the testimony of a doctor who testified at the sentencing hearing that Parish's conduct was less severe than that of a typical offender under the same statute.[139] Specifically, the doctor noted that Parish neither downloaded any files, nor indexed or filed any of the images in an organized manner.[140] Based on that testimony, the Ninth Circuit concluded that "[the trial court] appropriately compared [the defendant's] possessory conduct with the possessory conduct of the typical child-pornography offender, and the record supports the court's conclusion that [the defendant's] conduct was comparatively minor."[141]

Two years earlier, the Ninth Circuit reviewed another case involving images of child pornography located in the defendant's computer's cache file. In *United States v. Hay*, police arrested the defendant for possessing and distributing child pornography.[142] The jury found Hay guilty at trial, after which Hay appealed on several grounds.[143] On appeal, Hay's argument turned in part on the admission of three exhibits of child pornography.[144] Hay argued that due to a prior stipulation that these images were child pornography, the district court improperly permitted the jury to view these exhibits during deliberations.[145] Hay claimed that these pictures were unduly prejudicial and that the jury's viewing of them merited a new trial.[146] Significantly, one of the exhibits the jury viewed was "a reconstruction of a page from [the defendant]'s web site based on the contents

137. *See id.* at 1028-29 & n.1 (explaining "heartland" term). For further discussion of the concept of "heartland," see UNITED STATES SENTENCING GUIDELINES MANUAL § 1A(4)(b) (2000).

138. *Parish*, 308 F.3d at 1033.

139. *Id.* at 1030.

140. *Id.* (noting, in addition, that the content of images found was "pretty minor" compared to images possessed by similar offenders).

141. *Id.* at 1030-31.

142. 231 F.3d 630, 632 (9th Cir. 2000).

143. *Id.* at 633.

144. *Id.* at 638.

145. *Id.* Pursuant to Fed. R. Evid. 403(b), Hay had moved *in limine* to preclude the numerous exhibits that contained child pornography. The district court ruled that the jury would not be permitted to view the exhibits, except upon the jury's specific request. Although none of the exhibits was published during the trial, the court did allow the jury to view three exhibits during their deliberations after the jury requested the three specific images. *Id.* at 638-39.

146. *Id.* at 639.

of his own web browser cache, which showed [him] using his browser to access his system."[147] The court rejected Hay's argument, finding that the images were not unduly prejudicial because there was evidence that Hay viewed them and the exhibits "reflected [his] personal involvement" with the child pornography.[148] The court, however, made no comment regarding the cache-possession issue, nor does it appear that either party raised it.[149]

The United States Court of Appeals for the Fifth Circuit also decided a child pornography case involving images found in the defendant's computer's cache, but again neither party raised the cache-possession issue.[150] In *United States v. Grimes*, the defendant was charged with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).[151] Of the thirteen images of child pornography that Grimes was charged with possessing, three were found in his computer's cache.[152] At trial, the jury found Grimes guilty, and he thereafter appealed on several grounds to the Fifth Circuit.[153] Grimes did not raise, nor did the court comment on, the possession issue with respect to the three images found in the cache file. The only potential, if quite vague, clue to the Fifth Circuit's view appeared in a footnote in the opinion where the court explained the nature of a temporary Internet file. The court stated: "[I]f the images were JPG files in the user's temporary Internet files ("TIF's"), they might be pictures from a

147. *Id.* The defendant in *Hay*, a student at the University of Washington, operated his own website and used the University of Washington as his ISP. Prior to the defendant's arrest, Ontario, Canada, police arrested a Canadian individual for trafficking in child pornography. The forensic examination of the Canadian defendant's computer revealed that he had recently transmitted multiple files via a File Transfer Protocol (FTP) to a numerical Internet address affiliated with the University of Washington. Investigators later determined that the numerical Internet address in question had been assigned to the defendant. *Id.* at 632; *see also File Transfer Protocol*, SEARCHNETWORKING.COM, *at* http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213976,00.html (last updated Feb. 10, 2003). The third exhibit at issue in *Hay* referred to an image on the defendant's own website. The defendant's access to that image was demonstrated by review of the browser cache. *See Hay*, 231 F.3d at 639. For a detailed explanation of FTP, see D.J. Burnstein, *FTP: File Transfer Protocol*, *at* http://cr.yp.to/ftp.html (last visited Dec. 19, 2004).

148. *Hay*, 231 F.3d at 639.

149. Unlike some other cases where cached images constituted the only alleged criminal possession, *see, e.g.*, *Tucker I*, 150 F. Supp. 2d 1263 (D. Utah 2001), Hay involved multiple other bases besides the cached image. *See Hay*, 231 F.3d at 632-33 (detailing pornographic files found on the defendant's hard drive).

150. *See* United States v. Grimes, 244 F.3d 375 (5th Cir. 2001).

151. *Id.* at 377.

152. *Id.* at 378-79.

153. *Id.* at 377.

public site that the user had visited. *As a technical point, only images that have appeared, at one time, on the computer screen become TIF's.*"[154] This seems to evoke the distinction between the images in the cache and the images of child pornography that were once viewed by the defendant; however, the court did not provide further analysis. The court later vacated and remanded the case on other grounds.[155]

V. TWO CONCEPTUAL APPROACHES: REEVALUATING THE FACTORS

As the cases demonstrate, courts have struggled with how to apply the legal definition of possession to digital images. In their attempt to do so, courts have examined several traditional indicia of contraband possession, including: (1) the defendant's knowledge of the contraband; (2) the defendant's destruction of the contraband; (3) the defendant's manipulation of and control over the contraband; (4) the defendant's actions to seek out and obtain the contraband; (5) the amount of contraband found; and (6) any other extraneous, relevant evidence. Those factors appropriately focus on whether the defendant had the requisite knowledge of and control over the contraband at issue to satisfy knowing possession. For purposes of tangible contraband—for example, drugs and firearms—evaluation of the above factors is sufficient to determine possession. However, unlike tangible contraband, digital images do not necessarily exist in a singular form. In the case of files stored in a cache, there are at least two temporally distinct versions of the image—the image on the computer screen[156] and a copy of the image automatically stored in the cache. Consequently, before courts consider the indicia of possession, they must decide conceptually which "version" of the image the prohibited possession focuses on and then build their analysis around it. That conceptual focus will determine the ultimate persuasiveness—indeed, the applicability—of the factors around which the court must build its analysis.

---

154. *Id.* at 378 n.3 (emphasis added).

155. *Id.* at 385.

156. The image that appears on a computer user's screen is the end result of several processes that define how the Internet, and web servers in particular, work. With that in mind, the term "image on the computer screen" used herein is intended to be illustrative, as opposed to a technical description. For an excellent introduction to the technical processes of the Internet and the underlying vocabulary, see Marshall Brain, *How Web Servers Work*, HowStuffWorks, Inc., *at* http://computer.howstuffworks.com/web-server.htm (last visited Dec. 19, 2004); Jeff Tyson, *How Internet Infrastructure Works*, HowStuffWorks, Inc., *at* http://computer.howstuffworks.com/internet-infrastructure1.htm (last visited Dec. 19, 2004).

There are two conceptual approaches to determining whether cached images constitute knowing possession. The first approach places legal significance on the images found in a cache, and it holds that the presence of those images within the cache constitutes actual knowing possession of child pornography at the time the images are found (hereinafter "the Present Possession approach"). The second, alternative approach places legal significance on the images that the computer user sought out and placed on his computer screen. This approach holds that the copies of images found in a cache constitute *evidence of some prior* (but no less real) knowing possession (hereinafter "the Evidence Of approach"). No court has discussed which conceptual approach it was following. To the contrary, it appears from the format and substance of the analyses that every court has defaulted to the Present Possession approach without even recognition of other conceptual models.

But the choice of approach matters—even if it is selected by default. The conceptual approach will not only affect the technical accuracy of courts' analyses, it will also affect the strategic choices prosecutors and defense lawyers must make. More broadly, different conceptual choices will influence how closely the enforcement of child pornography possession statutes aligns with the original purpose of those statutes. With those issues in mind, the next Section reevaluates the factors cited by courts, focusing on the factors' significance under the Present Possession and Evidence Of approaches. That reevaluation suggests that the courts that have addressed the cache-possession issue have engaged in faulty analyses by conflating the two conceptual approaches. Specifically, they have followed a Present Possession approach, but have justified their conclusions on reasoning that technically and logically can only apply under the Evidence Of approach.

A. General Principles

1. Present Possession Approach

According to the Present Possession approach, a defendant knowingly possesses the actual files or images located in his computer's cache. Under this approach, the computer is analogous to a file cabinet and the cache is a file drawer. The user has reached out to the Internet through use of a web browser and selected an image, after which the computer automatically "files" a copy of that image in its file drawer. Viewed this way, the possession of the image begins when the image is cached and ends when the

file is deleted and overwritten by other data.[157] Thus, the period of possession could be quite lengthy depending on the volume of browsing done by the user, the size of the cache, and other configurations of his computer.[158] Once the image is overwritten, it ceases to exist on the computer and is not forensically recoverable.[159]

2. Evidence Of Approach

The Evidence Of approach differs analytically from the Present Possession approach in the legal significance accorded the images in the cache. In the Present Possession approach, the cached images are the possessed items—they represent the contraband itself. In the Evidence Of approach, those cached images are evidence of previously possessed items—they represent a recording of the contraband. Thus, instead of the analogy to a file cabinet, the computer is now analogous to a video camera that records all of the activity of the computer user. The user has reached out to the Internet through his web browser and selected an item, all of which the video camera records. The possession begins when the user reaches out and selects the image from the Internet and ends when the user moves to another webpage or otherwise leaves the image.[160] In contrast to the Present Possession approach, the time period of possession is far shorter, represented only as that time that the user actually controls the image on his screen. The evidence of that possession, however, only ends when a cached file is overwritten by other data, thereby destroying the "videotape" of the illegal possession.

---

157. Significantly, the time period of possession does not end when a user deletes the image because the image is only marked for deletion—it still physically exists on the computer, albeit in a different format. *See supra* note 22.

158. *See supra* notes 5-12 and accompanying text (describing cache configuration issues).

159. Although once overwritten the actual data is not recoverable in the normal forensic fashion, examiners may be able to recover other information related to the actual data. *See supra* notes 21-27 and accompanying text.

160. This assumes, of course, that the user does not actively download the image. If the computer user downloaded or saved the image, the possession would not end until the downloaded image was deleted and overwritten. This presents a significantly different analytical situation than when only temporary Internet files are at issue. To date, there has been little controversy that downloaded or saved files constitute knowing possession. *See, e.g.*, United States v. Venson, No. 03-30159, 2003 WL 22348922, at *2 (5th Cir. Oct. 15, 2003); United States v. Raney, 342 F.3d 551, 555-56 (7th Cir. 2003); United States v. Richardson, 238 F.3d 837, 839 (7th Cir. 2001).

B. Analysis of the Factors

1. Knowledge

Perhaps the primary issue courts have considered in determining whether cached images constitute knowing possession is whether the defendant had knowledge of how the computer's cache operated.[161] Turning first to the Present Possession approach, knowledge of the cache is significant because the focus of the analysis is on the images actually in the cache. If a defendant does not even know that a cache exists he cannot knowingly possess a cached image.

For example, consider Peter Patron, a patron of adult bookstores. Peter enters an adult bookstore that has an (admittedly illegal) child pornography collection located behind a staffed counter. At this store, various books and films of child pornography are available upon request for customers to browse before purchasing. Store procedure requires patrons to request a title, which is then retrieved by the clerk and handed to the patron. Unbeknownst to patrons, the store has implemented a promotional program to attract more business. As part of the promotion, whenever a patron requests a magazine, the clerk automatically makes copies of several images found in that magazine. The clerk then goes to the customer coatroom, locates that specific, but unsuspecting, patron's coat and places the free images in his coat pocket as a token of the store's thanks for his business.

When Peter Patron enters the store, he requests a magazine containing child pornography. Peter receives the magazine from the clerk, sits down nearby, and browses the pages. Deciding that he does not wish to make a purchase, Peter then returns the magazine, retrieves his coat, and exits the store. As he walks down the street, he is approached by police officers who, acting on a tip, arrest him for possession of child pornography.

Based on the above facts, Peter would claim, quite rightly it seems, that he cannot be culpable for the child pornography images in his jacket because he had no knowledge of their existence, nor intent to possess them. However, if Peter were aware of the images in his coat—perhaps he had visited the store many times before and knew of the promotional program—he would be culpable. Courts following the Present Possession ap-

161. United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002); *Tucker II*, 305 F.3d 1193, 1205 (10th Cir. 2002); *Tucker I*, 150 F. Supp. 2d 1263, 1267-69 (D. Utah 2001); United States v. Sanchez, 59 M.J. 566, 570 (A.F. Ct. Crim. App. 2003); Commonwealth v. Simone, No. CRIM 03-0986, 2003 WL 22994245, at *5-*6 (Va. Cir. Ct. Nov. 12, 2003).

proach have reached that same conclusion: where defendants have admitted to knowledge of how images are cached, courts have found knowing possession.[162] Courts have also found knowing possession, even without a defendant's admission to specific knowledge of cache operation, when the prosecution presented evidence of the defendant's general computer expertise.[163]

The difficulty under the Present Possession approach arises in cases where the defendant—like Peter Patron in the original scenario—does not have knowledge of the cached image. Notwithstanding a defendant's lack of knowledge, several courts have still found that knowing possession existed based on other factors.[164] As detailed further in Parts V.B.2-.6, however, the presence of those other factors does not rebut the lack of knowledge defense because those factors focus on the defendant's possession and knowledge of the image on the screen, not the cached image.

By contrast, the lack of knowledge factor takes on a diminished role in the Evidence Of approach. Unlike in the Present Possession approach, knowledge of the cache operation is irrelevant because criminal liability arises not from the cached images themselves, but rather from the images that the user originally searched for, selected, and placed on his computer screen. Returning to the analogy, Peter Patron would not be criminally liable for the images in his coat pocket, but could be criminally liable for possession of the pornographic magazine he originally requested, obtained, and browsed in the store. Under the Evidence Of approach, the sole

---

162. *See, e.g.*, *Tucker II*, 305 F.3d at 1205 (rejecting argument that the defendant did not possess voluntarily, in part, because the defendant knew images saved in cache); *Tucker I*, 150 F. Supp. 2d at 1269 (noting that the defendant knew to delete cache files and that the case was not one "of ignorance, mistake, or accident"); United States v. Mason, No. ACM34394, 2002 WL 1757175, at *10 (A.F. Ct. Crim. App. June 11, 2002) (rejecting the argument that the defendant did not know a computer "stored" images when the defendant admitted otherwise in the guilty plea colloquy), *aff'd*, 60 M.J. 15 (C.A.A.F. June 10, 2004).

163. *See, e.g.*, *Sanchez*, 59 M.J. at 569-70 (rejecting the argument that the defendant did not possess because images automatically saved, in part, because of evidence of the defendant's knowledge of cached items and of the defendant's sophistication with computers).

164. Most courts have determined that the presence of other factors was sufficient to show knowing possession, even where lack of knowledge was claimed. *See, e.g.*, *Tucker II*, 305 F.3d at 1205 (rejecting the argument that the defendant did not possess voluntarily, in part, because the defendant knew images saved in the cache); *Tucker I*, 150 F. Supp. 2d at 1269 (noting that the defendant knew to delete cache files and that the case was not one "of ignorance, mistake or accident"); *Sanchez*, 59 M.J. at 570; *Simone*, 2003 WL 22994245, at *7. Much of the analyses offered by those courts, however, is inapposite when following a Present Possession approach. *See infra* Parts V.B.2-.6.

focus is on the original images; any automated processes initiated by the original images are irrelevant for determination of possession.

2. Deletion

A second factor courts have examined is whether a defendant deleted a cached image.[165] In doing so, at least one court has found a defendant's deletion of cached files legally significant to prove both possession and knowledge. Under the Present Possession approach, however, deletion does not provide a sound, much less sufficient, basis on which to find knowing possession.

With respect to possession, some courts have reasoned that a defendant, by deleting a cached image, has evidenced his possession of that image. For instance, the *Tucker I* court stated that "[l]ogically, one cannot destroy what one does not possess and control."[166] That logic falls short under extended analysis. Consider again Peter Patron. After he departs the bookstore, he gets in his car and begins traveling northbound along a highway. As he rounds a corner, he sees in the distance his arch enemy, Preston Policeman, traveling toward him southbound. Overcome by his violent thoughts, Peter increases his speed and, just as Preston is about to pass him in the other direction, Peter intentionally veers his car into Preston's car. The resulting crash completely destroys Preston's car. At no time in the above example did Peter ever control or possess Preston's car. Yet, clearly Peter destroyed Preston's car. The same result is obtained whenever someone attacks someone or something else with a weapon; the attacker can destroy (or at least injure) the person or property he is attacking, but certainly cannot be said to "possess" that person or property. Similarly, a defendant's ability to delete or deletion of a file cannot, standing alone, prove his possession of that file.

With respect to knowledge, the *Tucker I* court reasoned that a computer user, by deleting a cached file, has at the very least demonstrated her knowledge of that file and the cache generally.[167] Although such knowledge appears self-evident—except in the case of accidental deletion—it is not clear that that level of knowledge is sufficient to meet the knowingly standard required by most statutes. Consider again Peter Patron's situation with a slight twist. As Peter walks down the street unwittingly carrying images of child pornography, he suddenly recognizes something unfamiliar in his jacket pocket and, upon checking, realizes he has copies of child pornography in his pocket. He then immediately takes the copies out of his

165. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1267-69.
166. *Id.* at 1267.
167. *Id.* at 1269.

pocket and throws them into a trash can. Based on that scenario, it does not appear that Peter had knowing possession of the images. Indeed, the moment he obtained knowledge of the images, he discarded them, thereby evincing his intent *not* to possess. It follows that knowledge of the image is not enough. Rather, there must be knowledge, followed by some period of inaction, and then the deletion.

Still, deletion may be a factor worthy of consideration in certain cases, but the effect will be fact sensitive. For instance, deletion may be an indicator of accidental viewing where a user has a limited number of cached images, all of which were deleted.[168] Conversely, deletion could be strong evidence of knowing possession where a large number of cached images once existed but have been systematically deleted over an extended time period.[169] Finally, deletion could mean nothing at all, as in a case where a user deleted files as part of his routine maintenance based upon content neutral file attributes, such as the file's age or type.

Under the Evidence Of approach, deletion of a cached image is also irrelevant. Because the inquiry involves the images previously searched for and placed on the screen—not the copies of those images that were cached—the deletion of a temporary Internet file has no bearing on the legal analysis of knowing possession. Deletion, of course, does have significant bearing on the practical investigation of the crime. Deletion in this sense refers to the destruction of evidence, like a drug defendant flushing cocaine down the toilet when the police enter with a search warrant. Fortunately for investigators, mere manual deletion does not necessarily destroy the evidence, and it can often be recovered far more easily than cocaine flushed into a sewer system.[170]

---

168. *Cf.* VT. STAT. ANN. tit. 13, § 2827(c)(2) (1999) (creating affirmative defense to possession of child pornography where "defendant in good faith took reasonable steps, whether successful or not, to destroy or eliminate the depiction [of sexual conduct by a child or of a clearly lewd exhibition of a child's genitals or anus]"). Accidental viewing would be further supported if the images were visited only once and the defendant's searches were of the type that plausibly could have caused sites containing child pornography to appear inadvertently. *See infra* Part VI.B (discussing the accidental viewing defense).

169. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1265 (noting that the defendant admitted to deleting cached files because it was something "he always did").

170. *See supra* notes 22-25 and accompanying text (describing how manually deleted data can remain on a computer in various hidden forms).

3. *Manipulation and Control*

Courts have also focused on a defendant's manipulation of and control over temporary Internet files.[171] Like the deletion and knowledge factors, the manipulation factor proves problematic under the Present Possession approach. The nature of the conceptual difficulty, however, is different. When a computer user browses the Internet, he manipulates—and perceives to manipulate—only the image on the screen by actions such as printing, enlarging, cropping, copying, saving, and naming.[172] The cached image is simply a copy of the image that the user has reached out and placed on her computer screen. As a result, analysis that focuses on the image in the cache file cannot properly rely on manipulation of a *different* image as support for knowing possession.[173]

As further illustration, return again to the unsuspecting Peter Patron. After he has received his requested magazine containing child pornography, he retires to a nearby chair where he browses the magazine. During this time, he has the ability to turn the magazine any direction he wishes, to open the centerfold, to make a copy on the nearby copy machine, to attempt to steal it from the store, and so on. Manipulation of that magazine, however, provides no evidence of Peter's alleged possession of the copied

---

171. *See, e.g.*, United States v. Hay, 231 F.3d 630, 639 (9th Cir. 2000); *Tucker I*, 150 F. Supp 2d at 1267-69; United States v. Sanchez, 59 M.J. 566, 569-70 (A.F. Ct. Crim. App. 2003); Commonwealth v. Simone, No. CRIM 03-0986, 2003 WL 22994245, at *6-*7 (Va. Cir. Ct. Nov. 12, 2003).

172. The technical analysis may be different if it could be shown that the user was returning to a previously cached image, in which case the browser would actually call up the cached image. *See supra* notes 2-6 (discussing how cache works). The user's perception would, however, remain unchanged unless he had specific knowledge that the page he requested via the Internet was retrieved from his cache folder.

173. This result applies to findings of actual possession, as distinguished from constructive possession. *See* BLACK'S LAW DICTIONARY 1183 (7th ed. 1999) (discussing actual and constructive possession). Under the Present Possession approach, a court could properly rely on a defendant's *ability* to manipulate (that is, the ability to enlarge, shrink, crop, print, etc.) the actual image in the cache file as evidence of constructive possession. For example, in *Tucker I*, the court discussed the defendant's ability to exercise control over the images. *See* 150 F. Supp. 2d at 1267. This discussion could be applicable to a constructive possession case viewed under the Present Possession approach. However, the *Tucker I* court's discussion regarding the ability to exercise control focuses not on the cached image, but the image on the screen. *Id.* (noting that "[w]hile the images that Tucker received *were on his computer screen*, he could control them many ways . . .") (emphasis added). Once again, that discussion would be applicable under the Evidence Of approach. The analytic error in *Tucker I* is conflating the two approaches. *See id.* at 1267-69 (analyzing the manipulation of images on the screen but later analyzing the deletion of images in the cache file). Moreover, even if the analysis were consistent, it could not overcome a lack of knowledge defense in certain cases.

images placed in his coat. After all, Peter manipulated the images in the magazine—not those placed surreptitiously in his coat pocket. While he may later have had the ability to manipulate the images in his coat pocket, he could not have done so without knowing of their existence.

Conversely, under the Evidence Of approach, the manipulation factor does not suffer from the same conceptual difficulties. Peter's manipulation demonstrates his authority and control over the magazine and the actual images therein, thereby providing direct evidence of his possession. Consequently, under this approach, the courts' analysis of manipulation would be proper.[174]

4. Actions to Seek and Obtain

Courts also have considered whether a defendant took affirmative steps to seek out and obtain child pornography via the Internet. Courts have principally relied on two types of evidence to show those affirmative steps: a defendant's subscription to websites that charge a user fee for access or are password protected and a defendant's entry of search terms into a search engine to find child pornography.

Under the Present Possession approach, neither website subscriptions, nor search terms necessarily supports knowing possession. A subscription to a child pornography website may help prove knowledge of the content of the images,[175] but again it is inconsistent and irrelevant to proving knowledge of the cached images themselves.[176] Similarly, although search terms clearly demonstrate the user's intent to reach out for images of child pornography,[177] they demonstrate only the knowledge and intent of a user with respect to the image *on the computer screen*—not necessarily the images cached. This analysis holds even if the cached images are identical copies of the images called to the screen.

Take again the Peter Patron example with a few slight modifications. For a customer to browse the magazines, he must provide the sales clerk with a list of titles he is interested in and pay a fee. Peter Patron therefore pays his fee to view the magazine, but still does not purchase it. Instead,

---

174. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1267 (analyzing the defendant's manipulation of image).

175. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1265; *Sanchez*, 59 M.J. at 570.

176. *Cf.* United States v. Hall, No. 98-6421, 2000 WL 32010, at *4-*5 (6th Cir. Jan. 4, 2000) (rejecting the defendant's argument that he had no knowledge that the images in his computer's cache were of child pornography).

177. In this respect, search terms likely will be sufficient to overcome an accidental viewing defense. For further discussion of the accidental viewing defense, see *infra* Part VI.B.

he walks out the store empty-handed except for the free copied images he unwittingly has in his jacket. His payment to view the child pornography images in no way supports knowing possession of the images in his coat. Likewise, while providing a list of titles demonstrated his knowledge of what he was viewing,[178] his actions have not provided any independent evidence that he knowingly possessed the images later placed in his coat pocket.[179] As a result, search terms and a subscription fee will not necessarily rebut a lack of knowledge defense.[180]

Conversely, under the Evidence Of approach, the presence of search terms and subscription to child pornography sites are powerful evidence of knowing possession. A defendant's use of search terms and subscription to certain types of websites demonstrates his affirmative actions to obtain a certain image and place it on his computer screen.[181] In general, the search terms and subscription fees will also establish the defendant's knowledge of the content of that image.[182] In the bookstore example, Peter's request of certain titles and fee payment, coupled with those titles being brought to him in direct response to his request, shows his volitional act to obtain the magazines, as well as his knowledge of the content of those magazines. Similarly, because the focus of the Evidence Of approach is on the image that the defendant volitionally reached out for and brought to his computer

178. For a discussion of the "mere viewing" versus possessing issue, see *infra* Part VI.A.

179. Search terms may, of course, provide further support for knowing possession of the images in Peter's coat in a case in which knowledge is not an issue. If, for example, Peter knows that the images will be placed in his jacket—regardless of whether he requests a sports magazine or a child pornography magazine—and he still "searches for" or "requests" images of child pornography, those search terms provide additional evidence of his knowing possession.

180. For a discussion of the lack of knowledge defense, see *infra* Part VI.C.

181. After a computer user engages a search engine and types in certain terms, the affirmative acts do not necessarily cease. Thereafter, the user will have to select a website and then usually click on links or thumbnails before the actual image is displayed.

182. For example, if the terms include words indicating child pornography, like "lolita" or "prepubescent beauties," the substance of what the defendant was attempting to obtain is fairly clear. *See* United States v. Grimes, 244 F.3d 375, 379 n.7 (5th Cir. 2001) (defendant used search term "alt.japanese.neojapan.lolita."); United States v. Mader, No. NM CM 99 01007, 2000 WL 1455260, at *1 (N-M. Ct. Crim. App. Sept. 18, 2000) (defendant used search terms "pedophilia" and "child pornography"); Commonwealth v. Simone, No. CRIM 03-0986, 2003 WL 22994245, at *7 (Va. Cir. Ct. Nov. 12, 2003) (defendant used search terms "lolita," "pedophilia," and "pre-teen pictures"). Conceivably though, a defendant could use search terms that are vague with respect to the age of the persons depicted (for example, "hot young girls"), and therefore provide less direct evidence of his knowledge to obtain *child* pornography, as opposed to adult pornography.

screen—not the image automatically copied to the cache—knowledge of the cache operation is irrelevant.

5. Number of Images

The number of images found in a defendant's computer's cache has not been an explicit factor as to whether that defendant knowingly possessed the images. Courts have, however, intimated that the volume of Internet searching and number of cached images were anecdotal evidence of a defendant's intent and level of knowledge.[183] As a conceptual matter, the number of images is neutral with respect to the Present Possession and Evidence Of approach. Although the number of images may affect certain practical defense or prosecution strategies,[184] it does not affect the substance of the analysis regarding knowing possession.

6. Extraneous Evidence

Like the number of images factor, extraneous evidence neither directly affects the analysis of knowing possession, nor militates in favor of either conceptual approach. Courts have considered extraneous evidence when evaluating computer users' defenses, particularly lack of knowledge and accidental viewing.[185] Such evidence could include a variety of items, including but not limited to videotapes of child pornography,[186] stories involving child pornography,[187] other images of child pornography that have been saved or downloaded to a hard drive,[188] hard copies of child pornography, and witness testimony.

The problem with relying on extraneous evidence is that while it may show a defendant's interest in child pornography, it does not necessarily show knowing possession of the digital images at issue. For instance, a defendant with a large stockpile of photographs of child pornography may still not have the requisite intent to knowingly possess cached images.

---

183. *See, e.g.*, United States v. Parrish, 308 F.3d 1025, 1027 (9th Cir. 2002) (noting that 1,300 images of child pornography were found in the defendant's cache); *Tucker II*, 305 F.3d 1193, 1197 (10th Cir. 2002) (noting that the investigator recovered approximately 27,000 images of child pornography on the defendant's computer); United States v. Hay, 231 F.3d 630, 633 (9th Cir. 2000) noting that the defendant had "hundreds" of images on his hard drive).

184. *See infra* Part VI.B (discussing accidental viewing defense).

185. *See Simone*, 2003 WL 22994245, at *7 (finding that the defendant's possession of stories involving graphic juvenile sex supported his knowing possession of cached images of child pornography).

186. *See, e.g.*, United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (noting the defendant's conviction for possession of videotape in same case).

187. *See Simone*, 2003 WL 22994245, at *7.

188. *See Hay*, 231 F.3d at 632-33.

However, again like the number of images factor, extraneous evidence may have a practical effect on the prosecution's, and defense's trial strategy.[189]

As the foregoing Part demonstrates, many of the factors courts have considered cannot logically apply if the court proceeds under a Present Possession approach. In addition, the analyses are left vulnerable to a properly advanced lack of knowledge defense because its focus is still on technical knowledge of the cache. Finally, even where courts ultimately reached the correct decision, their reasoning reflects conceptual and technical misunderstandings that could lead to incorrect results in cases with slightly different facts.

The next Part outlines and provides responses to several common defenses to child pornography possession in cases in which the possession is based on images in a temporary Internet file. The defenses include strictly legal and conceptual arguments, such as whether viewing an image on a computer screen constitutes possession of that image. They also include defenses based upon factual scenarios that may provide reasonable doubt, such as images found on a computer that has multiple users.

VI. POTENTIAL DEFENSES

A. Viewing Does Not Equal Possession

Several courts have noted that possession—not mere viewing—is criminalized by statute.[190] Moreover, under traditional legal definitions of possession, mere viewing is not sufficient to demonstrate possession.[191] In addition, statutes criminalizing mere viewing of child pornography appear on their face to be nearly impossible to enforce.[192]

---

189. *See infra* Part VI (discussing defenses).

190. *See, e.g.*, United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003); *Simone*, 2003 WL 22994245, at *6.

191. *See, e.g.*, EDWARD J. DEVITT ET AL., FEDERAL JURY & PRACTICE INSTRUCTIONS § 36.12 (Crim.) (4th ed. 1992) (possession means "to exercise authority, dominion or control over a given thing"); BLACK'S LAW DICTIONARY 1183 (7th ed. 1999) (possession means "the exercise of dominion over property").

192. *But see* ARK. CODE ANN. § 5-27-304(a)(2) (Michie 1997) (prohibiting, *inter alia*, "view[ing] any visual or print medium depicting a child participating or engaging in sexually explicit conduct"); OHIO REV. CODE 2907.323(A)(3) (West 2000) (prohibiting "possess[ing] or view[ing] any material or performance that shows a minor who is not the person's child or ward in a state of nudity" unless certain exceptions apply); Clay Calvert & Kelly Lyon, *Reporting on Child Pornography: A First Amendment Defense for Viewing Illegal Images*, 89 KY. L.J. 13 (2000) (discussing First Amendment issues with re-

The computer, and particularly the Internet, has significantly changed the marketplace for child pornography.[193] In turn, the increased presence of computer images of child pornography has significantly changed the investigation and prosecution of child pornography laws.[194] As in other areas of the law, courts and practitioners are faced with the awkward task of applying traditional legal concepts—like "knowing possession"—to new technologies. A defense that claims that a defendant merely viewed, and therefore did not possess, child pornography attempts to capitalize on this awkward task.[195] While the mere viewing defense may be sound in a narrow class of cases, the defense is misplaced as a general bar to prosecution in most cache-possession cases.

The mere viewing defense is the principal challenge to the Evidence Of approach.[196] Indeed, the unchallenged assumption that a computer user who views an image on his computer screen does not possess it may explain courts' default application of the Present Possession approach. The Present Possession approach does have the advantage of intuitiveness; since the cached images are actually stored in the computer, they appear to satisfy the traditional criteria for knowing possession more naturally than the evanescent images on a computer monitor. In many cases, however, the analytical justification for finding knowing possession under the Present Possession approach falls short.[197]

The answer is to challenge the assumption that a computer user who views an image on his computer does not possess that image. Return yet again to the bookstore analogy. After Peter Patron has requested his maga-

---

spect to criminal defense of news reporter who viewed child pornography as part of story research).

193. *See, e.g.*, John C. Sheller, Note, *PC Peep Show: Computers, Privacy, and Child Pornography*, 27 J. MARSHALL L. REV. 989, 989-91 & nn.1-15 (1994) (discussing changing marketplace for child pornography with rise of computers and computer-transmitted images) (citing, *inter alia*, ATTORNEY GENERAL COMM'N ON PORNOGRAPHY, FINAL REPORT (1986)).

194. *See supra* Part III (discussing various federal and state statutes designed to combat child pornography, including computer-based images); *supra* Part II.B (discussing forensic examination procedures).

195. *See, e.g.*, Appellant Brief, United States v. Bass, 2004 WL 1252037, at *18-*19 (10th Cir. May 17, 2004) (No. 04-6049) (arguing that the defendant did "no more than view child pornography on the internet" because he did nothing "proactive with any image" and "did not change or modify images in any manner").

196. *See supra* Part V.A.2 (giving overview of the Evidence Of conceptual approach and distinguishing it from the more common Present Possession approach).

197. *See supra* Part V (discussing analytical factors and criticizing Present Possession approach). As discussed in Part IV, cases in which a defendant admits to knowledge of cache operation do not present the same analytical difficulty.

zines containing child pornography, he retires to a nearby chair and begins to browse through them. Meanwhile, the clerk places the copied images in Peter's coat pocket. The Evidence Of approach attaches legal significance to the images in the actual magazine that Peter holds in his hands—not the images in his coat pocket. The mere viewing defense maintains that Peter does not possess the images until he purchases the magazine because he is "just looking" at the contraband images.

But is Peter just looking at the images? Consider an addition to the analogy: after Peter sat down and began looking at the child pornography, police enter the store and immediately approach Peter. With the magazine still in his hand, open to pages with sexually explicit images of children, Peter is arrested for possession of child pornography. Later at trial, Peter's lawyer argues that Peter was merely viewing the images in the magazine and cannot be liable for possessing them. However, the prosecution offers evidence that Peter specifically requested the magazines that he knew contained child pornography and received those magazines. Upon receipt, the magazines were under Peter's dominion and control—he flipped through them, turned them at various angles, unfolded the centerfold, copied them on the bookstore's copy machine, showed them to other patrons, ripped pages from them, attempted to steal the entire magazine by secreting it in his backpack, and so on. Based on that evidence, there seems little doubt that, at the moment the police arrested Peter, Peter knowingly possessed the child pornography.

Of course, the police seldom have such good timing in the real world. As an evidentiary matter, it would do the police little good if they entered the bookstore two days after Peter left. Perhaps another patron could tell the police that he witnessed Peter's activity earlier that week, but that would be woefully insufficient evidence on which to base a criminal prosecution.[198]

Let us further assume now that the bookstore had a closed circuit video camera that was able to capture everything that occurred in the store at any given time. Now when the police arrive two days after Peter left, they ask the store manager for the video tape from the video camera. The images captured on the video tape are crystal clear. They show Peter in sufficient

198. Any criminal prosecution of child pornography possession requires the prosecution to prove that the images were, in fact, of children. Thus, the eyewitness account could be helpful if the actual magazine that Peter returned could be located and authenticated. The similar situation arises in drug cases: if a witness viewed Defendant possessing cocaine, Defendant could not be charged unless that actual cocaine were recovered and tested to prove that it was, indeed, cocaine. The practical difficulties of such an approach seem to exceed any theoretical potential of conviction.

detail to identify him beyond any doubt. Further, the tape records Peter's request to the clerk for the child pornography, his receipt of the requested item, and his complete and exclusive control over it. The tape also shows with great detail the precise images that Peter viewed in the magazine, when he viewed them, how many times, what he did with them, and how he manipulated them. Finally, the video tape documents the number of times during the past month that Peter visited the store and engaged in the same conduct. Because the contraband in any child pornography case is visual, the video tape would be sufficient to authenticate the images as child pornography.[199] That video tape is powerful evidence of Peter's guilt.

Just like the above videotape, a cached image is the most powerful evidence of a child pornography defendant's conduct. With the aid of a forensic examination, a cache can establish precisely when the defendant obtained the image, how he obtained it, how many times he viewed it, and what, if anything, he did with the image thereafter.[200]

Still, the defense could argue that the videotape captured mere viewing. Under the Evidence Of approach, however, the defense appears far less viable, especially if a number of factors weigh in favor of possession. Even in cases with minimal other evidence of possession, prosecutors should be able to distinguish mere viewing from knowing possession. Consider another example: Patrick Pedophile logs onto his computer and opens his web browser. He goes to a common search engine, like Google or Lycos, and types in several search terms including "lolita," "preteen nude pics," and "underage sex kittens." Upon receiving his search results, Patrick clicks on a particular website, which contains thumbnail images of child pornography. He then clicks on several of the thumbnail images to enlarge them and views them at his desk. As he is doing so, Patrick's coworker, Ian Innocent, happens to walk by Patrick's desk, where he stops to chat for a moment. When Ian arrives, he looks directly at Patrick's computer screen and views the precise same image that Patrick is viewing for several seconds.

---

199. Unlike, for instance, a video tape of a drug transaction that could not establish that the substance in fact was cocaine without additional evidence through witnesses, police officers, laboratory analysts, and the like.

200. For example, a defendant could enter his cache and locally view the images or move them to other portions of the hard drive. In the case of a sophisticated defendant who entered the cache to save, alter, or relocate the images, the type of analysis will change: the defendant has now focused his conduct on the actual cached image, thereby making a Present Possession approach appropriate, if not exclusive.

The distinction between Patrick and Ian's conduct is clear. Regardless of Ian's intent or knowledge about the images on Patrick's computer screen, Ian did not possess them. He had no control or dominion over them. He could not guide those images' destinies. He had no ability to move, alter, save, destroy, or choose the images. Ian merely viewed them. Contrast Ian's conduct with Patrick's conduct. Unlike Ian, Patrick sought the images out and affirmatively placed them on his computer screen. He had the ability—just as Peter Patron did with the magazine in the bookstore example—to move, alter, copy, save, destroy, and otherwise manipulate the image. Patrick had total ability to control and guide the image. In every sense, Patrick possessed the image at that time—and his possession was captured "on videotape" by his computer's cache file.[201]

The above discussion does not suggest, however, that someone actively using a computer could never be found to be merely viewing an image. The analysis will be fact-dependent and vary case-by-case. One potential situation that could arise is a so-called accidental viewing, which generally occurs through a pop-up screen. Subsection B addresses this scenario and the likely defense based upon it.

B. Accidental Viewing (a.k.a., Attack of the Dreaded "Pop-up")

A defendant may argue that a contraband image or website appeared automatically in the form of a "pop-up" banner while he was browsing legal sites.[202] The accidental viewing defense can be easily addressed by the prosecutor and the forensic examiner, preferably prior to charging. As discussed above, a forensic examination can identify, among other things, the number of times a defendant viewed an image, the number of different images, and the use of search terms.[203] Prosecutorial discretion dictates that a defendant who has a cache full of legal, adult pornographic websites, but one image of child pornography that he visited once (and perhaps even deleted from the cache), should not be charged. Conversely, a forensic examination that reveals thousands of images of child pornography, search terms obviously intended to obtain child pornography, or simi-

---

201. Patrick's knowledge of the cache operation, or even the presence of the cache, is irrelevant. Under the Evidence Of approach, a child pornography defendant's lack of knowledge about his computer's cache is no more relevant than a bank robber defendant's lack of knowledge about the bank's security video camera.

202. *See Pop-up*, *at* http://whatis.techtarget.com/definition/0,,sid9_gci212806,00.html (last visited Dec. 19, 2004) (describing characteristics and operation of pop-ups); *see also* Zappen, *supra* note 123, 1165-66 nn.27-28 (discussing and collecting sources defining pop-ups).

203. *See supra* Part II.B (discussing forensic examination capabilities).

larly incriminating evidence should largely, if not completely, defeat any claimed accidental viewing defense raised by the defendant.[204]

C. Lack of Knowledge

The lack of knowledge defense represents the chief impediment to following a Present Possession conceptual approach. As discussed at length in Part V.B.1, most of the factors courts have examined do not overcome a lack of knowledge defense under the Present Possession approach. By contrast, proceeding under an Evidence Of approach obviates the need to rebut a lack of knowledge defense because knowledge of the cache operation becomes irrelevant. For that reason, among others, the Evidence Of approach should be the approach followed by prosecutors.[205]

---

204. *See* United States v. Grimes, 244 F.3d 375, 379 n.7 (5th Cir. 2001) (acknowledging evidence that the defendant searched the Internet using term "alt.japanese.neojapan.lolita."); United States v. Mader, 2000 No. NMCM 99 01007, WL 1455260, at *1 (N-M. Ct. Crim. App. Sept. 18, 2000); (noting that the defendant obtained images by searching under "pedophilia" and "child pornography"); Commonwealth v. Simone, No. CRIM 03-0986, 2003 WL 22994245, at *7 (Va. Cir. Ct. Nov. 12, 2003) (reasoning that search terms "lolita," "pedophilia," and "pre-teen pictures" were indicia of knowing possession); *see also* United States v. Parrish, 308 F.3d 1025, 1027 (9th Cir. 2002) (noting that 1,300 images that appeared to be child pornography were found in the defendant's cache); *Tucker II*, 305 F.3d 1193, 1197 (10th Cir. 2002) (noting that investigator recovered approximately 27,000 images of child pornography on his computer); United States v. Hay, 231 F.3d 630, 633 (9th Cir. 2000) (noting that the defendant had "hundreds" of images on his hard drive).

205. It is not obvious, however, that lack of knowledge can or should be a complete defense even under the Present Possession approach. If a computer is thought of as a tool, the defense becomes essentially that the tool operator was ignorant of the tool's capabilities, and therefore, should be relieved of the result of his operation. The success of the defense turns on the level of knowledge required to meet the standard of knowingly. Different courts have defined knowingly in different ways. *See, e.g.*, United States v. Tracy, 36 F.3d 187, 194-95 (1st Cir. 1994) (acknowledging federal circuit split over definition of "knowingly"); *see also* United States v. Doyle, 130 F.3d 523, 540 (2d Cir. 1997) (stating that a defendant acts knowingly when "he acts intentionally and voluntarily" and when he "is aware of a high probability of [the fact's] existence, unless he actually believes that the fact does not exist"). *See generally* KEVIN F. O'MALLEY ET AL., FED. JURY PRACTICE AND INSTRUCTIONS CRIMINAL § 17.04 (5th ed. 2000) ("'Knowingly' Defined").

In a case in which a defendant claims a lack of knowledge regarding his computer's cache operation, the issue becomes whether the defendant knew, or was practically certain, the result (the contraband images saved as his temporary Internet files) of his conduct (searching for, clicking on, and viewing images with his web browser). Resolution of the issue turns partly on how the court applies the scienter. *See, e.g.*, United States v. X-Citement Video, Inc., 513 U.S. 64, 78 (1994) (applying scienter to all elements of 18 U.S.C. § 2252). It also turns on how the court addresses the gap between the user's perception and the actual operation of the computer. *See id.* at 69-71.

D. Other Defenses

Although not directly related to the cache-possession issue, there are several other defenses that often arise in computer child pornography cases. One factual defense that could arise, especially when images are found on a defendant's work computer, is that a user other than the defendant could have used the terminal. Overcoming a multiple users defense requires not only forensic investigation, but traditional law enforcement investigation as well.

A forensic examination usually should be able to determine if a user signed onto her computer with a unique password. While evidence of such a password is helpful, it is not dispositive for two reasons. First, there remains a viable argument that another user obtained the password and fraudulently logged on as someone else[206] or had the ability to override the password protection.[207] Second, even if the defendant did sign on with her password, another user could have surreptitiously used her computer in her absence while the defendant was still logged on. Traditional investigation can go a long way toward resolving these potential issues by determining, for example, the geographic configuration of the computer terminal(s), the working habits and responsibilities of the defendant and other possible users, the degree of supervision, the practice of home or office security measures, the time and dates of the access, and the content of eyewitness accounts. Secondary and tertiary forensic examinations can also lead to evidence establishing the true identity of the user.[208] Well-timed execution of search warrants can also reduce the likelihood of a multiple user defense.[209]

Another increasingly common defense is that the contraband images are not of real children but rather are virtual images. This defense stems from *Ashcroft v. Free Speech Coalition*, in which the Supreme Court held

---

206. This issue will be particularly problematic in a workplace where there is no strict policy for employees to lock their computer screens with passwords while away from their terminals. Similarly, computer terminals that are easily accessible to other parties, such as cubicle-style workspaces, will provide additional challenges for investigators to overcome.

207. Even where an employee has a terminal that is password protected, generally system administrators or other supervisory personnel will have the ability to access the employee's account by overriding the password.

208. For example, assume that at or near the same time as a user accessed images of child pornography, he also accessed a web-based e-mail account that itself was protected by a unique password. Under that scenario, the alleged interloper would have had to have known the additional password on the e-mail account as well as the network password.

209. For example, during a suspect's shift at work while he is at his computer or at a time when a suspect is most likely at home working on his computer.

that banning virtual pornography violated the constitutional right to free speech.[210] Consequently, it falls to the prosecution to demonstrate that the images are of actual children. There are two principal ways in which the prosecution can make that demonstration. First, certain organizations such as the National Center for Missing and Exploited Children ("NCMEC") have begun to compile databases of known child victims and the images in which they appear.[211] Use of that database at trial, through stipulation or testimony, can allow prosecutors to establish that certain images are indeed of real children. Unfortunately, the databases are limited and will never incorporate child victims who remain unknown. As a result, the database may only be helpful in a relatively small percentage of cases.

Secondly, prosecutors can consider using testimony by a computer animation expert to establish that certain images are of real children and are not computer-generated. Most courts have determined that whether an image is a virtual or real depiction of a minor is a jury question.[212] Although there are no reported cases involving expert testimony in this area, appropriately qualified experts should be able to describe the painstaking, expensive process of creating a virtual image and opine on whether the images at issue are of the quality and type that could be computer-generated.

VII. CONCLUSION

The Evidence Of approach offers two main advantages over the Present Possession approach: it reflects the technology at issue more accurately and it furthers the statutory purposes of the statutes more effectively.

The principal problem with the Present Possession approach is that it fails to account fully for how a browser cache operates. Most of the factors that courts have relied upon to show knowing possession of a cached file may support knowing possession of an image on a screen, but they do not support possession of the cached file itself. Moreover, none of those factors effectively counteracts a defendant's lack of knowledge defense. Conversely, under the Evidence Of approach, the typical indicia of possession properly apply. More importantly, under the Evidence Of approach, the most difficult and incongruous defense facing prosecutors—lack of

210. 535 U.S. 234, 258 (2002).

211. *See* Nat'l Ctr. for Missing & Exploited Children, http://www.missingkids.org (last visited Dec. 20, 2004).

212. *See, e.g.*, United States v. Kimler, 335 F.3d 1132, 1142 (10th Cir. 2003); United States v. Deaton, 328 F.3d 454, 455 (8th Cir. 2003).

knowledge—is rendered irrelevant. Thus, the focus of child pornography possession is no longer the cached files as contraband themselves, but rather their evidentiary value to prove the previous possession of contraband—the actual images on the user's screen.

Second, the Evidence Of approach furthers the appropriate punitive and penological goals. In general, the purpose of child pornography possession statutes is to address the demand for such contraband and to reduce the likelihood of such contraband from encouraging pedophiles to engage in criminal actions. Those purposes are fulfilled by prohibiting possession as viewed under the Evidence Of approach. The punitive and penological goals do not—and should not—depend on the technological accident of a browser cache. A technologically savvy defendant who disabled his browser cache (or took other evasive steps) is no less culpable than the novice computer user defendant who did not. The Evidence Of approach keeps the focus on the substance of the conduct—the exploitation of children—not the peripheral issue of how a defendant configured his computer.

There remains the issue of whether the choice of conceptual approach has any effect on the substantive result. After all, courts have largely reached the correct result—finding knowing possession—using their current analyses. Similarly, as a practical matter, the vast majority of child pornography cases will not center solely on temporary Internet files as the basis for conviction. Except in rare cases, police and prosecutors will likely only charge a possible defendant when a forensic examination uncovers more evidence beyond cached files.

Notwithstanding these issues, prosecutors and courts are wise to consider which conceptual approach they follow. While gaps in understanding may not have resulted in errors of law as of yet, the threat exists. It is not difficult to imagine cases where the wrong conceptual approach could result in over- or under-inclusiveness, especially as technology continues to evolve. In any area where parties attempt to apply traditional legal principles to new technology, but particularly in criminal law where individuals' liberties are at stake, courts and prosecutors should continually strive to improve their conceptual understanding of the issues.

Whatever the approach used, prosecutors will have to continue to exercise discretion in child pornography possession cases based on images in temporary Internet files. Few would disagree that, all other facts equal, a defendant with cached files—and only cached files—containing child pornography on his computer is less culpable than a defendant who has actively downloaded, saved, and indexed files of child pornography. Simi-

larly, there may be prudent practical or philosophical reasons not to charge an individual based on what he placed on his computer screen.

Regardless of extralegal concerns, prosecutors must still deal with statutes as written, and they should use these statutes to their maximum advantage. Legislators may ultimately make the policy decision that a person's control of images on a computer screen, despite meeting the technical legal requirements of possession, is not the target of child pornography possession statutes. Until they do, however, prosecutors should not shy from prosecutions based on temporary Internet files solely because of concerns about the legal viability.