"But Your Honor, *I* Didn't Possess Those Pictures; My *Computer* Did."

Temporary Internet Files, Web Browser Cache Files, and Child Pornography

By

Priscilla M. Grantham

Gone are the days when a computer was a mammoth piece of equipment that occupied an entire room. Computers in the home are common-place. As of June 2008, the numbers of personal computers in use worldwide hit one billion, and as of 2005, 62 million households in the United States had an Internet connected computer. With the speed in which technology advances, these numbers will only increase. Digital technology is all around us. One can go to his local coffee shop or fast food restaurant and access the Internet on his smart phone, a task which would have seemed implausible just a few years ago. Digital devices have altered the way that we as a society work, study, and communicate – many would argue, for the better. Unfortunately, such technology is also responsible for the resurgence of child pornography.

Images of child sexual abuse are no longer traded in dark alleys; the images are not in the form of photographs that were developed in a home darkroom, or a copy of a picture reproduced so many times that the quality of the image has been degraded. One can produce child pornography utilizing readily available equipment: digital video recorders, digital cameras, phones. Once a scene is captured, it can be printed on a home printer, forwarded to "Buddy Lists," and uploaded to the Internet. Technological advances have made it possible to produce and distribute child pornography inexpensively and quickly, as well as enabling "collectors" with the means to acquire it. One only needs a credit card and Internet access to

subscribe to a website devoted to or featuring child pornography; with the click of a mouse, he will have images sent directly to him through cyber space. File sharing programs such as Kazaa, BearShare, and Limewire allow users to share files by downloading them from another user's computer.

Federal laws, as well the laws of every state and the District of Columbia, make it a crime to manufacture, possess, or distribute child pornography.[1] Possession of child pornography is banned by 18 U.S.S. § 2252 and 18. U.S.C. § 2252A. The language of the state statutes is similar to that of the federal statutes in that they proscribe the knowing possession of child pornography.

When contemplating the term "possession," most people would say that it involves the actual presence of a physical object – a weapon, for example that can be touched, held, locked in a gun safe. No one would assume that a person possesses a gun because they happened to see it behind glass at a gun shop. Mere viewing of this weapon does not constitute possession. But what does it mean to knowingly possess child pornography in this age of digital images? Can one be guilty of possessing child pornography when they "merely viewed" the image on their computer screen? In other words, are images that are viewed on the Internet and therefore automatically stored in a browser's temporary cache files "knowingly possessed," or must they be saved or downloaded to the hard drive in order to establish possession? Courts' have not been uniform in their approaches to determining what constitutes possession; some courts have held that images in cache are sufficient to show possession, while others have rejected this view. Furthermore, there is not a consistency in the ways that courts analyze this issue, with some courts focusing on the

[1] 18 U.S.C. §§ 2251-2260.

characteristics of the defendant, i.e., how knowledgeable was he about the way computers operate, and others looking to factors such as what actions did the defendant take that resulted in the placement of the images in his cache file?

One of the leading cases specifically holding that the presence of images in cache files constitutes possession is *United States v. Tucker*.[2] In *Tucker*, the forensic exam of defendant's computer revealed numerous images of child pornography in the browser cache. Tucker admitted to viewing several hundred images of children engaged in sexual acts. He also said that as a practice, he always deleted his browser's cache files after viewing these images. Tucker said that he did not violate the statute for two reasons (1) he didn't possess the images because he never downloaded or copied them and he deleted them from the cache files, and (2) even if he did possess the images, the possession was not knowing because the computer stored the images on his cache file without any action on has part. In rejecting these arguments, the court relied heavily on the fact that Tucker had control over the images while he was viewing them. The court noted that while these images were on his screen, he could do any number of things with them: he could print, copy, enlarge, place in other directories, etc., as a result, he possessed them. The court found no merit in Tucker's argument that the computer, not him, was responsible for placing the images in the cache files. The images were in the cache files, the court reasoned, solely because he sought out the images. Tucker was a member of an Internet newsgroup that in exchange for a fee, gave him a password that enabled him to visit websites where he could view child pornography.

[2] United States v. Tucker, 150 F. Supp 2d 1263 (D. Utah 2001), *aff'd,* 305 F.3d 1193, (10th Cir. 2002).

In *United States v. Romm*,[3] the defendant admitted to viewing child pornography on his computer but argued he was never in possession of it because he did not download any of the images. In rejecting this argument, the Ninth Circuit held that defendant's ability to control the images on the screen was sufficient to show possession.

Other courts finding that images in cache constitute possession focus on the fact that the defendant sought out the images of child pornography and placed them on his screen. This view eliminates the defense that the defendant did not know that images were saved to a cache file; 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. The copies of images placed in cache constitute evidence of prior knowing possession.

In the following cases, images located in cache files were also held to be sufficient to support convictions for the possession of child pornography:

- Based on images of child pornography found in his computer's cache files, Appellant was convicted under Ohio statute prohibiting the viewing or possession of child pornography. He claimed the images were automatically stored by the web browser in the computer's temporary cache files, and that there was no evidence that he accessed or viewed the material. The court concluded that the state presented sufficient evidence that Appellant sought out the images and exercised dominion and control over them; i.e., he typed in

[3] United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

search terms to search for child pornography websites and repeatedly accessed some of the pages.[4]

- Based on images of child pornography found in cache files, defendant was convicted under Pennsylvania statute for possession child pornography. He claimed that merely viewing the images (without downloading or saving them) did not constitute possession unless it could be proved he knew the images would be saved to the cache file.

  The court focused on the language of the statute that makes it a felony to possess or control "…any book, magazine…computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act…" . The court found that Appellant intentionally sought out and viewed child pornography. He took affirmative steps (operating the computer mouse, locating Web sites, opening the sites, displaying the images on his computer screen, closing the sites) which corroborated his interest and intent to exercise influence over, and thereby, control over the child pornography.[5] The court noted that a determination of whether a defendant sought and controlled pornographic images of children recognizes and promotes the purposes behind the statutes – the destruction of the market for the exploitative uses of children,[6] and the protection of the physical and psychological well-being of children.[7]

[4] State v. Hurst, 2009 WL 580 453 (Ohio App. 5 Dist.)

[5] Commonwealth v. Diodoro, 932 A.2d 172 (Pa. 2007).

[6] Osborne v. Ohio, 495 U.S. 103, 109 (1990).

[7] New York v. Ferber, 458 U.S. 747, 756 (1982).

- In *People v. Tecklenburg*,[8] the court addressed the issue of whether a defendant may be convicted of possessing child pornography stored in a computer's cache files absent some evidence that he knew those files existed. In other words, does a defendant knowingly possess child pornography on a computer when the computer automatically downloads, without the defendant's knowledge, those images into computer cache? The court held that knowledge of temporary Internet files or Web browser cache files is not necessary for a defendant's viewing of child pornography over the Internet using a Web browser to violate California's statute prohibiting possession or control of child pornography.

- Based on images found in his computer's cache files, Appellant was convicted under Texas statute that prohibits "knowingly or intentionally possessing" child pornography. The court stated that the crucial issue is whether the images were ***intentionally sought out***, or whether they appeared on the computer's hard drive by default. The fact that child pornography was stored in the same area as other pornography, and that child pornography images were downloaded from an Internet web site supports the finding that Appellant intentionally sought the images.[9]

Other courts, however, have held that statutes prohibiting the knowing possession of child pornography do *not* criminalize the mere viewing of these images on a computer. These courts reason that the presence of child pornography in cache files is evidence only of the fact that the images were at one time viewed on the computer screen.

[8] People v. Tecklenburg, 169 Cal. App. 4th 1402 (2009).

[9] Gant v. State, 278 S.W.3d 836 (Tex. App.-Hous. (14 Dist.) 2009).

- In *United States v. Kuchinski*,[10] the court held a defendant cannot be guilty of possession and control of child pornography located in a computer's cache files without evidence that he exercised dominion and control over the images.

- Likewise, the Eighth Circuit in *United States v. Stulock*,[11] held that one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing it to be automatically stored in the browser's cache, without having purposely saved or downloaded the image.

- In *Worden v. Alaska*,[12] the court found that even though images of child pornography were found in defendant's cache files, there was no indication that he intended to permanently store the images, rather, his intent was to view the images on his computer screen for the time that he was at the web site.

Possession of child pornography is not a new crime – it was in existence before the advent of computers; however, the Internet has become the dominant method from which to access these images. A review of the cases outlined above illustrates one of the many challenges posed by the advance of technology; how are existing laws to be applied to new situations? As it stands now, there is an inconsistency in case law regarding what constitutes possession of child pornography, and a determination of guilt in such a matter could very well turn on

[10] United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006).
[11] United States v. Stulock, 308 F.3d 922 (8th Cir. 2002).
[12] Worden v. State, 213 P.3d 144, 2009 WL 1424434 (Alaska App. 2009).

whether or not the defendant had an understanding of the technical aspects of computer processes.