Possession of Child Exploitation Material in Computer Temporary Internet Cache

Sungmi Park
*Legal Informatics and Forensic Science Institute, 2ricecake@naver.com*

Yunsik Jake Jang
*Legal Informatics and Forensic Science Institute, jakejang@hallym.ac.kr*

Joshua I. James
*Legal Informatics and Forensic Science Institute, Hallym University, joshua.i.james@pm.me*

Follow this and additional works at: [https://commons.erau.edu/jdfsl](https://commons.erau.edu/jdfsl)

Part of the Common Law Commons, Comparative and Foreign Law Commons, Computer Law Commons, Courts Commons, European Law Commons, Evidence Commons, Information Security Commons, Internet Law Commons, Law and Society Commons, and the Legislation Commons

**Recommended Citation**
DOI: [https://doi.org/10.15394/jdfsl.2017.1446](https://doi.org/10.15394/jdfsl.2017.1446)
Available at: [https://commons.erau.edu/jdfsl/vol12/iss3/3](https://commons.erau.edu/jdfsl/vol12/iss3/3)
POSESSION OF CHILD EXPLOITATION MATERIAL IN COMPUTER TEMPORARY INTERNET CACHE

Sungmi Park, Yunsik Jang and Joshua I. James
Legal Informatics and Forensic Science Institute
Hallym University
Chuncheon, South Korea 24252
2ricecake@naver.com, jakejang@hallym.ac.kr, joshua@cybersirmetech.com

ABSTRACT
When considering the possession of child exploitation material, the U.S. and German courts have the same focus, but slightly different interpretations. This slight difference in interpretation could mean that in one country a defendant will be found guilty of possession while in the other country he or she could be found not guilty. In this work, we examine the standards courts in Germany and the United States have used to combat child pornography, and analyze the approaches specifically related to viewing and possession of CEM. A uniform solution is suggested that criminalizes “knowing access with the intention to view” as a method to handle challenges related to the definition of possession.

Keywords: Child Exploitation Material, Computer Cache, Knowing Possession, Viewing Child Exploitation Material, Intention to View, Intention to Possess

1. INTRODUCTION
Many jurisdictions have established that Child Exploitation Material\(^1\) (CEM) is a severe matter that exploits and abuses the weakest members of society. Despite efforts by many countries to prevent child exploitation, the demand for such content remains. Like with all information sharing, the development of the Internet and related technologies has made access, production and distribution of CEM easier than ever before. In 2014 the National Center for Missing and Exploited Children (NCMEC) reported receiving more than 1.1 million reports related to CEM and child sexual exploitation on the CyberTipline.\(^2\) In this same period of time, they reviewed 132 million images through the Child Victim Identification Program.\(^3\) In 2012, the program showed that there was a 774% increase in the number of CEM images and videos identified.\(^4\) This staggering number of CEM images is a concerning to many countries who are implementing strict legislation against related acts, and also pushing for international cooperation on such matters. Both production and distribution are normally punished harshly, with the former receiving a greater punishment. However, the Supreme Court of United States has acknowledged that simply punishing production and distribution is not enough to solve the problem of child exploitation.\(^5\)

\(^1\) Also referred to as child pornography and child abuse material

\(^2\) National Center for Missing and Exploited Children (NCMEC) 2014 Annual Report

\(^3\) Id.

\(^4\) National Center for Missing and Exploited Children (NCMEC) 2012
exploitation. They concluded that severe consequences for the consumer market is also a state interest. Member States of the Council of Europe have agreed to the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, also called the “Lanzarote Convention” in 2007, and addressed the matter again in EU directives in 2011, stating that all kinds of sexual offences against children should be criminalized. European countries, as well as the United States, have agreed to penalize consumers of child exploitation material; however, we have found by comparing cases in the United States and Germany that inconsistent standards are used to punish an offender for “possession of child exploitation material.” One major challenge arises when it is shown that the defendants have viewed illicit images (CEM) on their computer using a browser without intentionally saving the image to their computer. In such case it is disputable if the defendant has possession of the illicit images, even if a copy of the image is saved on their computer in browser cache. This was a direct result of legislation that is vague and not up-to-date with today’s level of technology. The inconsistencies of decisive factors in court ruling are not to be neglected; an arguable case could be considered as a crime in one country, while the direct opposite could be true in another, even if similar legislation exists. Considering the fact that most illicit images and videos in question are being accessed through the Internet, it seems vital to analyze the reason for such differences, and to find a uniform solution.

In this work, we examine the standards that courts in Germany and the United States have used to combat child pornography, and analyze the approaches specifically related to viewing and possession of CEM. A uniform solution is suggested that criminalizes “knowing access with the intention to view,” following the example of a 2008 Amendment in the United States and directives of the EU, 2011.

2. THE PROBLEM OF DEFINING POSSESSION OF IMAGES IN CACHE

There are a number of challenges with defining possession based on jurisdiction. This is especially true with computer cache since a user may not be aware that such a cache exists and can be controlled.

2.1 What is the legal definition of “possession?”

While all countries mentioned in this paper have laws against possession of child exploitation material, none of them have an

---


6 Protection of Children against Sexual Exploitation and Sexual Abuse, Council of Europe (2012)


8 Protection of Children against Sexual Exploitation and Sexual Abuse, Council of Europe (2012), p. 9(Preamble)

9 18 U.S. Code §2252 Notes 2008 Amendment: “Subsec. (a)(4)(B). Pub. L. 110-358, §§103(a)(3)(D), (b), 203(a)(2), inserted “, or knowingly accesses with intent to view,” after “possesses” and “using any means or facility of interstate or foreign commerce or” after “has been shipped or transported” and substituted “in or affecting interstate” for “in interstate”.

---
explicit explanation as what constitutes “possession.” Possession, in a colloquial sense, is “the state of having, owning, or controlling something.”

In Anglo-American law, possession is acknowledged in two forms: actual custody, and de facto custody. The former applies when the defendant has control or physical custody of the item in question. This is the most obvious and literal form of possession. Before the Internet, possession was mostly understood as “present manual custody” as the item was presumed to be physical. However, according to a 2011 study, 95% of all criminals in the United States convicted of possessing child exploitation material had CEM stored on computer hard drives or similar storage devices. This change of storage method – from physical to digital – emphasizes the importance of control of the item rather than literal physical custody. If the defendant holds a storage device that contains the relevant data, and if the data is under his or her physical control, it can be considered as actual custody.

De facto custody is understood when the item is stored in a place the defendant would not be deterred physically from obtaining manual possession. This concept expands the form of actual custody in that it also includes cases where the defendant does not have physical custody or control, but the ‘exclusive right or power’ to have manual custody if he or she desires. For example, a defendant is able to manipulate images remotely because he or she maintains the website in which the relevant files are published. There are also theories that extend the concept to include ‘accessing or attempting to access material on a website.’ The reasoning is that although the defendant does not have physical control to delete the original file, he or she is able to save, copy or view the file, therefore also exercising control.

In the German Criminal Law, it is important to understand that intention is analyzed in two elements, knowledge (Wissen) and desire (Wollen). In the case of digital files, it is generally understood as possession if the relevant data is stored in a non-volatile storage device of which the defendant exercises actual control. However, there have been court decisions that have accepted possession of child pornography before the saving process into a permanent storage device. This inconsistency occurs because the court not only considered the technical aspects (whether the file has been stored on a non-volatile device or not) but also the knowledge (if the defendant knew of the child exploitative material that was stored) and the ‘willingness to possess (Besitzwillen)’ of the defendant in each case. This will be more thoroughly discussed below.

2.2 The Characteristics of Cache

http://www.oxforddictionaries.com/definition/english/possession


Clough, id.


Clough, id.

Clough, p. 310

Clough, id.

Clough, id.

Fischer, “Strafgesetzbuch und Nebengesetze(58.Auflage)”, §184b

Leipold, Tsambikakis, Zöller, “Anwalt Kommentar StGB(2.Auflage), §184b
As mentioned above, discussing simple possession of data stored on a hard drive is relatively clear if not by law, then by practice; if the defendant has knowledge and control over the files, he or she is in possession of said files. The controversy in possession occurs in cases that involve unknown downloads, such as the cache memory and a defendant who was—proven by evidence or admission—viewing child exploitation material.

Before we analyze what makes cases about illicit images in cache memory different from cases in which evidence was stored in other devices, we will first give a brief explanation of what cache is.

When visiting a website, the Internet browser (Internet Explorer, Google Chrome, Safari, Firefox, etc.) automatically saves copies of images on that page to the hard drive to speed up the loading process should the site be revisited. The area used for to store temporary data is called “cache” also known as “browser-cache.” If a user revisits a website, the browser will first look through cache to find the necessary files, which shortens the download time of resources on the page such as texts or images.

With the exception of “a pop-up or the existence of malicious software,” an image will not be saved in the cache if the user did not access the web site on which the original image is published. However, generally the browser-cache uses a hidden or difficult to find folder (storage location on the disk). A person who uses a browser to access the Internet does not need to know the location, size or function of this cache. The process of copying and downloading data is fully automated.

The cache can be deleted automatically or manually, depending on the settings of the browser. For most browsers, the information, if not manually removed, can be stored for months.

Since the images were downloaded are saved on the hard drive, cache files are accessible offline. If the storage is not emptied out, the user technically has free access to the images stored in cache.

2.3 The Discrepancy in Definition of Possession: In Case of Images in Cache

With the development of digital technologies, the traditional definition of possession, that was meant to determine possession of physical items, cannot by itself apply to Internet-based crimes without creating loopholes. While the concept of possession has been amended by shifting the focus from the location of the item to the actual control of the defendant, items stored in cache has another factor to consider. As stated above, files stored in browser-cache are distinguished from files actively downloaded by the defendant by the fact that the downloading process is automatic, and possibly not known. This is an issue when attempting to prove the intention to possess the item, as it can be disputed that the defendant had knowledge of the images stored in the hard drive in the first place. This argument likely progresses to the debate whether “possession of child exploitation material” is deducible by the “mere viewing.”


United States v. Kuchinski, 469 F.3d 853 (9th Cir. 2006)
On one side, it can be argued that simply the act of knowingly accessing websites that contain child exploitation material and therefore causing copies to be downloaded to cache already constitutes criminal possession. On the other hand, it can be claimed that the act of viewing should not be equated with active downloading.

As most pertinent laws require knowing possession of child exploitation material, it all comes back to proving knowledge and intention of the defendant; knowledge of that the item was within the defendant’s actual control and, in some countries, intention to exercise that control.

For a uniform solution, it is first necessary to understand why there were inconsistencies in the interpretation of “possession.” Therefore, we will identify the criteria that has been used to deduce possession until now, and analyze each. We have separated the relevant cases by country and factors courts have used in their approach. While a number of other circumstantial evidence have to be considered, such as number of images or other extraneous evidence, we have chosen the criteria that have played a decisive role on determining knowledge and intention in particular.

3. CASE STUDY: COURT DECISIONS IN THE UNITED STATES

Since this paper compares court decisions of two countries, we will start with a comprehensive overview of the pertinent law in each country.

3.1 The Law

In the United States, the federal law that penalizes knowing possession of child pornography is codified at 18 U.S.C. § 2252(4). The purpose of Congress by adding this law as part of the Child Pornography Protection Act of 1996 was to address the ills of child exploitation material and prevent children becoming victims of sexual exploitation.

It is significant that in 2008, Congress decided to criminalize knowing access with intent to view by adding it next to knowing possession in § 2252(4)(B). Through this amendment, a defendant may be guilty by simply viewing even a single image of child pornography, as long as the defendant knows that the images are of child and explicit in nature and is accessing the website knowingly. Intention to view the images, without actually seeing them, may also suffice if the defendant purposely accessed the website. This seems to be the response to clarify the imprecisions of § 2252’s wordings and neutralize the defense’s potential argument of “mere viewing not possessing.”

However, for a more accurate point-by-point comparison between U.S. Court approaches and German Court’s decisions on “possession of child exploitation material,” the case study in this section will primarily focus on cases before the 2008 Amendment.

3.2 The Three Court Approaches to Deduce Possession

Although united under the same law and goal, the court approaches and the factors that were considered decisive in the 2000s lacked uniformity and consistency, some courts even

---

24 Clough, p.311
25 Ty E. Howard, Id.
26 Id.
making decisions without providing sufficient explanations. The majority of courts acknowledged illicit images in cache as enough evidence for possession of child exploitation material, but in instances such as United States v. Stulock, the court noted “one cannot be guilty of possession for simply having viewed an image on a web site” since the images are automatically stored without the intention of the defendant. This shows that courts have used different factors as criteria in each case resulting in various analysis and sometimes, result.

3.2.1 Control of Image and Knowledge Cache

An important element to consider when analyzing the court approaches is how inference is used to deduce intention of possession (or how the logical deduction steps progressed to ultimately conclude knowing possession).

In United States v. Tucker, the Tenth Circuit found the defendant guilty of knowing possession of child exploitation material. Tucker was a member of an Internet newsgroup labeled “alt.sex.preteen” that provided CEM in exchange for a fee. Tucker admitted that he had access to several thousand images of CEM. He also admitted to viewing them, clicking on the thumbnails, selecting some of them to enlarge and deleting his computer’s cache afterwards. While Tucker conceded that the images were CEM as defined by statute and the fact that he viewed them, he argued he did not possess the images as he never downloaded them or copied them and because he emptied the cache storage.

The district court focused on Tucker’s ability to control the images reviewing the legal definition of possession (stated above). It came to the conclusion that “[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 others had he chosen; and he could copy them to other directories...” According to the court, the fact that Tucker deleted the files in cache spoke to the high level of control Tucker possessed over the files. Since Tucker “could control [the images] in many ways,” the court considered the evidence of control was sufficient to convict him of possession of CEM. Knowing possession was inferred from Tucker’s actual control over the images.

In United States v. Romm, the defendant Stuart Romm was convicted for both possession and receipt of CEM, the Ninth Circuit looking to the Tucker analysis for guidance. Similar to Tucker, Romm had admitted in viewing child exploitation images before deleting them from his cache. Romm told the agents that he had purposely emptied his cache because he knew they were going to find child exploitation material on his computer. The court decided based on the knowledge Romm possessed about cache (“know that the unlawful images are stored on a disk”), his admittance of repeatedly seeking out CEM and the control he had over the files.

30 Ty E Howard, id., at p. 1249
31 United States v. Stulock, 308 F.3d 922 (8th Cir. 2002).
32 Thumbnails are snapshots of small images in a single place. http://techterms.com/definition/thumbnail
34 Id.
35 United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006)
36 Romm, 455 F.3d at 1000.
(Romm had intentionally found and deleted the illicit images from his cache) that Romm was guilty of possession of CEM.

However, in the same year, 2006, the Ninth Circuit used the same reasoning in United States v. Kuchinski; this time to a different result.

In Romm, the court found that “the government must prove a sufficient connection between the defendant and the contraband to support the inference that the defendant exercised dominion and control over it.” This means, knowledge of the contraband enables the defendant to have control (in forms of deletion, saving to another directory, print, etc.) from which possession can be inferred. Because Romm knew how to access his cache, he could control them. Because he could control them, he possessed them, as it would not be possible to gain actual control without possessing the item first.

Conversely, in the case of Kuchinski, the result was the opposite because of the emphasis that was made on knowledge and control. The fact that John Kuchinski viewed child exploitation images was indisputable as the FBI discovered around 15,000 images on his computer. However, the court found no evidence that suggested Kuchinski had tried to access the cache files, no evidence that he was sophisticated enough to know about the existence of the cache files. The court stated, “the lack of knowledge about the cache files” leads to the assumption that the defendant lacks “access to and control over those files.” Thus, without “other indication of dominion and control,” the defendant cannot be found guilty of the images found in cache. Kuchinski was only found guilty for the 16 images he had downloaded on his hard drive and 94 deleted files he had put in the “bin.”

3.2.2 Deletion of Image in Cache

Another factor that played a significant role in the Tenth Circuit’s ruling in United States v. Tucker was the fact the defendant had intentionally deleted the images in his cache storage. While Tucker claimed that the deletion should be considered as evidence of his innocence, or non-possession, the court rejected the claim. It gave an analogy of narcotics cases, explaining that possessor of illegal narcotics is not relieved of criminal liability if he or she throws the drugs out of the window.

The deletion of image approach is also used by the Tenth Circuit in United States v. Bass. Brian Bass was a member of an e-group labeled “Candyman.” Once the police investigation started, Bass admitted he had viewed CEM. He also admitted that he had sought out a way to remove information from his computer out of fear of his mother finding the illegal files. He used software called “Window Washer” and “History Kill,” both programs that are used to effectively remove the files from computer and Internet history and any other traces by overwriting the data multiple times. This is a factor that differentiates the case from Tucker, who deleted the files manually by directly accessing the place the cache files were stored. It is also a factor that differentiates this case from Kuchinski; despite Bass’ claim that he did not

37 Id.
38 Kuchinski, 469 F.3d at 863; Romm, 455 F.3d at 998.
39 Id. At 863.

http://www.toptenreviews.com/software/privacy/b est-privacy-software/historykill-review/
know about the automated saving process of the browser, the Tenth Circuit found Bass guilty of possession. To comprehend how the Tenth Circuit reached its verdict, another step of logical deduction is needed. Although Bass insisted he did not knowingly possess the images, as he was ignorant about the cache function, the court found it reasonable that a jury could infer knowledge from the purchase and usage of “History Kill.” Unlike Tucker who clearly had knowledge about the automatic saving process (directly deleted files saved in cache), knowledge in Bass’ case was inferred from the broader act of deletion of the files (bought and used software to wipe images from hard drive).

3.2.3 Active Search for Child Pornographic Images

As the law requires specifically “knowing” possession, the court takes various factors under consideration to infer knowledge. The act of actively searching for the images is one. When Tucker claimed that he had no criminal liability, he had claimed that 1) he had no possession as he did not copy or download the files and because he had deleted them 2) even if he had possession, it could not be knowing possession as the downloading process was not influenced on his action. For the second argument, the court noted “each time [Tucker] intentionally sought out and viewed” images of child pornography over the Internet, he “knowingly acquired and possessed the images.” The court inferred active, knowing possession from the fact that Tucker had intentionally visited websites on which the images in question were available. The court further explained that it was ultimately Tucker’s own volition of actively searching for the websites and clicking on the images that started the download process of the illicit images. In context of criminal possession, as Tucker “volitionally reached out” for the files, paid a subscription fee to obtain a password to the pornographic websites, and considering other factors mentioned in previous sections, the court logically deduced that Tucker knowingly possessed the images.

Another case in which the court takes the active search approach is Commonwealth v. Simone. In its ruling, the court considered the fact that the defendant had specifically searched for child pornography using terms like “Lolita” and “pedophilia” so he had a series of images saved in cache, was in possession of prints outs depicting graphic sexual stories of children, had saved an illicit image as his computer’s wallpaper. Because of those reasons, the court noted “the defendant reached out for these images with the intent to control and have dominion over them.” The emphasis was set on Simone’s action to seek out child exploitation images. This, the court explained with an analogy between the images in the cache and narcotics on a sidewalk. If a person walks down the street and sees narcotics, recognizes them, and walked past, the person is not accountable for illegal possession of narcotics. However, if the person recognizes the narcotics and reaches out to carry them home, the narcotics can be considered to be in the person’s possession. The court saw the case of Simone similar to the latter, as Simone had recognized the images as child exploitative in nature and had reached out by actively searching for them. According to the court, “merely viewing” changed to “knowing possessing” when the person reaches out and gains control over the item. Combined with other evidence, the court

44 Bass, id., at 1201-02.
45 Id.
46 Tucker, 150 F. Supp. 2d 1263

47 Id.
inferred knowing possession from Simone's conduct of active search.

It is in this last approach in which we can assume the core of the issue; the courts are expanding the term of “possession” to include “active search” as a factor, accepting knowledge if there is a possibility of control over the item and taking intention if the defendant was viewing or looking for specifically child exploitation material.

### 4. CASE STUDY: COURT DECISIONS IN GERMANY

To compare to the United States, we will examine cases in Germany.

#### 4.1 The Law

In Germany, possession of child exploitation material is penalized at §184b IV StGB (German Criminal Code). The regulation criminalizing CEM has been amended several times. In January 1, 1991, the law was added to §184 StGb (Distribution of pornography), in 2004 it was separated to stand alone as §184b.

The law as it is stated today was enacted in 2008, integrating guidelines of EU legislation, especially broadening the definition of pornography to widen the possibility of interpretation and strengthen the punishment. The purpose of this law is the eradication of the market that offers child exploitation materials, as the existence of such market indirectly encourages the sexual abuse of children.\(^{48}\)

#### 4.2 The Three Court Approaches to Deduce Possession

The German Law generally accepts possession (Dauerhaftigkeit) and stability (Festigkeit) of actual control over the item (tatsächliche Sachherrschaft) is given as well as the willingness to possess (Besitzwillen)\(^{49}\). However, different from saving the data on external storage devices or downloading data to the hard drive, defining possession of data in cache under German law is disputable; first, the saving process is automated and second, the actual control is not necessarily permanent. In the following years, there have been verdicts and analysis that contradicted each other. While U.S. courts were more focused on proving knowledge, German courts reasoned the evidence to prove intention of the defendant.

Similar to the previous section, the cases of this case study will also be categorized according to criteria or decisive factors.

#### 4.2.1 Active Search of Clicking on Links for Child Exploitation Images

On February 23, 2009, a defendant was found not guilty by the district court Hamburg-Harburg. He had been charged with possession of CEM; in the investigation, it was discovered that he had viewed at least 18 images and one video file depicting children between 4 to 11 years of age performing sexual acts with or to adults, or their own genitalia.

The defendant had searched actively for such material and received e-mails with "links" to websites with CEM and was tempted to view the images by offers of "free tours." He regularly clicked on previews, which were automatically stored in browser cache. However, the defendant had no prior knowledge about such caching functions. The defendant had no manually saved images and claimed he didn't have any intention to save them in the first place.

---

\(^{48}\) Leipold, Tsambikakis, Zöller, “Anwalt Kommentar StGB(2.Auflage), §184b

\(^{49}\) Id.
The district court did not find the evidence proved sufficient for possession. The objective element of possession was fulfilled, as the defendant had the files on his computer; however, intention to obtain control over the files could not be proved. There was no evidence that the defendant’s desire to merely view the images could be equated with the willingness to possess those images.

However, on February 15, 2010, the Higher Regional Court (Oberlandesgericht, OLG) Hamburg rejected the ruling, explaining the goal-oriented search of child exploitation images with the intention to view and the download of the file caused by that desire was enough to satisfy the requirements of §184b IV StGB. In its decision, the OLG does not see indicia of possession at the level of browser-cache but already in the loading data on RAM\(^{50}\) succeeding to penalize active search as acquisition to possess.\(^{51}\)

The OLG stipulated a computer user already had a high level of control over the data, if he or she downloaded the image knowingly and willingly to RAM with the intention to view. Once the image is downloaded into RAM, the user has the ability to manipulate the file, for example to enlarge it, but also to save it or print it to obtain the file permanently. The OLG conceded to the point that images loaded on the RAM does not fulfill the element of permanence. The images cannot be considered as being stably in possession as it is understood by tangible items, as the possession status would end the moment the user leaves the browser or turns the computer off. This could lead to the argument that the data is not fully in the user’s disposal.

However, the OLG also notes that possession should have a different definition, specifically for digital data, as it shows certain characteristics essentially different from tangible items; because images on the Internet can be copied and multiplied to be exactly the same as the original, it can be assumed that the data are as much as in the user’s or the viewer’s disposal as it is to the provider.

The argument that another step is needed to “save” the file and gain actual control, is not found to be effective for the following reason: as the download to the cache file is automatic, a second step is also needed if the user decides to configure the browser not to save the data. According to OLG Hamburg, loading the data on the screen with the intention to view is not only a possible opportunity to obtain control over the data, but should already be considered to be in complete material control of the user. In this case, as loading the images into RAM is considered possession, the intention of possession can already be inferred from actively seeking out child pornographic images.

In the same year, following the OLG’s reasoning, the district court in Kiel determined that hyperlinks could fulfill the requirements of the criminal code as well.\(^{52}\) According to its ruling, it could be understood as possession if the defendant activates a link to gain access of image, the image is downloaded to RAM or cache of the defendant’s computer or even if he just tries it.\(^{53}\) However, this decision was met with heavy critique; an attempted activation of a link to be considered evidence of possession of the file was considered to excessively broaden the terms of the penal code that could easily be a slippery slope.

---

\(^{50}\) Random Access Memory, also known as RAM, is a volatile memory that loses its data when the computer is turned off. When browsing through the internet, images are loaded in ROM to be executed.


\(^{52}\) LG Kiel, 6. September 2010 -8 Kls 2/10

\(^{53}\) Id.
4.2.2 Deletion of Image in Cache

In year 2008, OLG Hamburg stated in a ruling that a defendant’s lack of intention can be proved if he deletes the images from the browser-cache immediately after viewing or can show evidence that he had planned to do so.\(^{54}\) Willingness to possess cannot exist if the user decided from the beginning to get rid of the loaded images promptly and irreversibly by emptying the Internet-cache immediately. In this case, the defendant had searched for child pornographic material, viewed them on his computer, thereby causing the files to be automatically saved into a hard drive he had in his house cellar. Out of fear of being discovered by his wife or the police, he had deleted the files on the same day manually. According to the OLG, the district court had overlooked this fact. While there was a Federal Supreme Court (Bundesgerichtshof, BGH) decision that data saved in cache could constitute as possession as it was possible to retrieve the data and view the files; the OLG emphasizes that the necessary willingness to possess was not explained in the former ruling. In this case, it was established that the defendant had “promptly deleted” the data of the browser-cache “shortly after their creation.” The court distinguishes this case from the one BGH concluded possession\(^{55}\) with the fact that in the latter the user had kept the cache files for days. Following this note, the deletion of images in cache is a factor that proves the lack of intention to possess, if the deletion was planned from the beginning and executed promptly, and not after a few days have already passed.\(^{56}\)

\(^{54}\) Hanseatisches Oberlandesgericht Hamburg, Beschluss vom 11.11.2008 – 1 – 53/08

\(^{55}\) BGH(NSStZ 2007, 95)


4.2.3 The Ability to Retrieve the Images in Cache

In 2012, the BGH stated in a ruling that possession is established if the user knows that the images are stored in cache, as that knowledge can be used to retrieve the images and exercise actual control.\(^{57}\) In this case, the two defendants had created an Internet platform for pedophiles, and encouraged potential members to post hardcore CEM in a chat room. After interviewing the candidates about their interests and desires, the two defendants rated the child pornographic video. If they deemed the age of the child and the sexual content as acceptable, they invited the new member to their platform. The members were encouraged to post and share more videos or pictures to be ranked higher and gain access to more material. In this case the Federal Supreme Court notes the term possession in context of §184b II StGB, obtaining possession of CEM for another. Because the links the defendants sent to their members were purposely created to provide the receiver with CEM, and the receiver was able to gain control over the file by simply clicking on the link, the court regarded it as possession. The BGH makes it clear that it is discussing browser-cache and not the cache on the CPU, as it was vaguely distinguished in the ruling of OLG Hamburg 2010 (above). The court also states the necessity of intention; the viewing of child exploitation material on the Internet is regarded as possession, if the user is able to retrieve the data from his or her local computer and the data is not deleted immediately from cache. The knowledge of cache implies the user is able to re-access the kinderpornographischer Schriften im Internet“, StV 2009, at 471-472

\(^{57}\) BGH, Urt. v. 18. January 2012 -2 StR 151/11
data for later use, which can be considered an element of actual possession.

5. COMPARISON AND ANALYSIS OF COURT APPROACHES

Overall, it can be assumed that while the U.S. courts concentrate on what constitutes as prior knowledge of the cache function, the German courts are adamant about determining the "desire" (Wollen) component of intention.

This is evident in the German court's approach of deletion of images in cache; in Germany, it cannot be considered possession if the suspect erased the cache files immediately after he/she saw the problematic images on the screen, as this is evidence that the suspect had no desire to save or possess the files. In the U.S., deletion of images, regardless directly from cache or by use of a program, was considered knowledge and evidence to support possession.

Also, while the BGH ruling in 2012 seems similar in essence to the U.S. courts in stressing the importance of proving knowledge of cache, the BGH ruling reasons this that the suspect must have the knowledge to retrieve files from cache, and showing the defendant's desire to see the illegal images again.

The U.S. courts' ruling primarily focused on inferring knowledge and assume possession when knowledge is confirmed. The big question in the U.S. courts was what factors should be considered to confirm knowledge.

By analyzing the cases of both countries, it can be concluded that while both countries find similar indicia for the crime; German courts are attempting to meet the requirement of the traditional definition of possession, whereas the U.S. courts take a more aggressive approach and aim to achieve the highest sentence by contemplating all evidence to fit the possession charge\(^58\). What indicia should be considered the most reasonable is debatable.

The control of the image and knowledge of the cache function approach can be considered the standard indicia the courts lean on. Both German and U.S. courts understood possession as established if the defendant had actual control over the images or the device in which it was stored.\(^59\) Manipulating, enlarging and printing has been a factor to infer control as well; in the U.S., deletion of files was also considered an indicator to make a logical deduction and confirm the defendant's control over the item. In Germany, however, immediate deletion could mean the lack of desire to possess the item.

Knowledge about cache is a factor both countries focus on heavily. As shown in United States v. Stulock\(^60\), United States v. Kuchinski or the initial court decision of district court Hamburg-Harburg\(^61\), if ignorance of the defendant is confirmed, possession cannot be established.

While it is understandable the courts were likely to dismiss the charges if it was evident the defendant had no knowledge about cache, it does not seem just that a person who had viewed, knowingly accessed and controlled images of a sexually exploited child cannot be found guilty because of his ignorance of

\(^{58}\) A.W.J. Dubach, Convicting for Computer Child Pornography (2011)

\(^{59}\) BGH, Urt. v. 18. 01. 2012 -2 StR 151/11, Rn. 17

\(^{60}\) One cannot be guilty of possession for simply having viewed an image on a website, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image, U.S. v. Stulock, 308F.3d 922, 2002

\(^{61}\) OLG Hamburg, Beschl. V. 11.11.2008 -1-53/08(REV) 1 Ss 180/08
technology\textsuperscript{62}. Also from United States v. Bass, it is arguable what proficiency level is used as the stepping stone for the logical jump from knowledge to possession. Judge Kelly in Bass notes, “the court's decision effectively rewrites the statute to criminalize viewing child porn via computer”\textsuperscript{63} as the question that needs to be answered is “whether he knowingly possessed child pornography;” \textsuperscript{64} which is debatable as Bass used a file removing software but claimed to have not known about the cache function.

Considering these aspects, the active search approach appears to be the better solution. U.S. courts have shown that they are willing to take patterns of active search as evidence to infer possession.\textsuperscript{65} From court rulings as OLG Hamburg 2010, it can be assumed Germany was even attempting to criminalize the previous step of saving the data in cache, labelling loading the data in RAM as possession.

However, when OLG Hamburg overturned the district court Hamburg-Harburg’s decision to accept possession of CEM based on the act of actively searching specifically for illicit material, it was heavily criticized. For one, this decision blatantly overlooked the difference between preparation, attempt, and completion. Distinguishing between those stages of action is crucial as the first is generally not punishable while the other two could be. It can be understood in the analogy of a potential thief in a store holding a bottle of beer, considering whether he should take it or buy it. Being so strict would be the equivalent of arresting a potential thief who is just holding the bottle before walking out of the door.\textsuperscript{66} Another critique is that it gave up the relatively clear interpretation of possession; as the mere possibility of saving an image is set to have the same consequences as actually saving the image to a hard drive.\textsuperscript{67}

In the United States, the factor of active search is accepted as an indicator, however, the “pattern of methodically seeking out”\textsuperscript{68} is to be combined with other evidences to support possession. Standing as the only evidence, a conviction for possession is less likely.

As mentioned before, while the pertinent law is similar and court decisions have also been based on similar factors, the way both countries approach the issue differs. Proposing a uniform solution without setting a shared guideline would be meaningless.

The issue comes back to the fact that there are inconsistencies in how to adjust the traditional concept of ‘possession’ to cover intangible, automatically-saved data. Such an issue could lead to the broadening of legal terms in a way that allows abuse of such definitions. The various interpretations of a similar law (illegalizing possession of CEM) show the core of the discrepancy lies in the legal structure of both countries. Germany was more focused on interpreting a legal term to adapt to a new technology, while the United States were more adamant in building up cases

\textsuperscript{62} Gianna Marin, “Possession of Child Pornography: Should You be Convicted When the Computer Cache Does the Saving for You?”, at p. 1227

\textsuperscript{63} Bass, 411 F.3d

\textsuperscript{64} Id.


\textsuperscript{66} http://blog.beck.de/2010/02/28/olg-hamburg-zum-besitz-von-internet-kinderpornographie-urteilsbegrundung-liegt-vor

\textsuperscript{67} Id.

\textsuperscript{68} United States v. Dobbs, 629 F.3d 1199, 1200-01 (10th Cir. 2011).
against CEM consumers. However, even without taking the difference in legal structure under consideration, the controversy within the nation proves the lack of a precise guideline. Considering this, a generally accepted, internationally agreed solution seems near impossible.

Therefore, the question is how to define the law to come to a uniform solution that does not base its reason on an unclear definition or factor. For this reason, the United States has added “access with the intention to view” in its law since 2008. The EU guideline in 2011 has been encouraged to include penalization of “access of child pornography” in the pertinent law as well, and although Germany considers this already addressed by their existing law adequately it does not deny the meaningfulness of having a more detailed, explicit regulation.

6. CRIMINALIZING ‘KNOWING ACCESS WITH THE INTENTION TO VIEW’ AS THE UNIFORM SOLUTION?

To combat child exploitation more efficiently, the United States Congress has amended their law to include “knowing access with the intention to view.” In 2009, a defendant was convicted for knowingly accessing of CEM in case United States v. Cruikshank. The case shows similarity to Kuchinski, as Cruikshank viewed CEM of young children using an online search engine. Cruikshank did not actively save the files, and had shown no evidence that he had access to the 986 files automatically stored in his cache. However, the police found that Cruikshank had bought a membership to view CEM. If we applied the ruling of Kuchinski, or the definition of possession according to BGH in 2012 to this case, Cruikshank would have been freed from charges.

However, because of the added clause, the court found Cruikshank guilty of knowing access, stating the seriousness of the crime: “By paying for access to images of child pornography, Mr. Cruikshank supported the creation and distribution of images depicting the sexual abuse of children by driving up demand for new images and rewarding those who create them.”

The European Union have included “knowing access” in the directives to fight sexual abuse and sexual exploitation of children as well:

Knowingly obtaining access, by means of information and communication technology, to child pornography should be criminalized. To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing

---

69 In cases like United States v. Bass, knowledge of cache, which was considered a decisive factor of possession, was inferred from another action (deletion of files by a program). There was no evidence that exclusively stated Bass had knowledge how to access his temporary internet files.

70 18 U.S. Code §2252 Notes 2008 Amendment, Id.

71 Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht, 21.01.2015

72 18 U.S. Code §2252 Notes 2008 Amendment, Id.


74 Id.
child pornography. The intentional nature of the offence may notably be deduced from the fact that it is recurrent or that the offence was committed via a service in return for payment.\textsuperscript{75}

By clearly stating intention to view is required, the knowing access clause purposely leaves an escape route for people inadvertently accessing websites.

As mentioned before, it can be inferred from the case study above that inconsistencies in the interpretation of possession of CEM have occurred in the attempt to broaden the term of the law to criminalize offenders who have unmistakably viewed CEM but could not be charged due to technicality. In that aspect, it does not seem wrong to assume that “knowing access” can be a solution to penalize CEM consumers more efficiently.

The “knowing access,” according to U.S. law and EU directives, is accepted if the person has or wants to exercise control or dominion over the material, which can be understood as the precondition of knowing possession of CEM. The addition seems to be more intended to support and to build up a constructive case against possession of CEM.\textsuperscript{76}

While there have been guilty verdicts regarding the knowing access of CEM, they rarely stand alone or more likely are used as a stepping stone to pursue the charge of possession.\textsuperscript{77} Cruikshank was a rare case the defendant was found guilty particularly because of knowing access; the court stated the seriousness of the crime by quoting Congress: "...where children are used in its production, child pornography permanently records the victim's abuse, and its continued existence causes the child victims of sexual abuse continuing harm by haunting those children in future years."\textsuperscript{78} and found evidence to support the verdict in the fact Cruikshank had paid for membership to view CEM.

While punishing men like Cruikshank under the law to hurt the CEM market and deter others from engaging in such is a step towards prevention, it cannot be dismissed that there needs to be detailed standards for this law as well. The struggle of applying anti-possession law on images in cache has shown that with the development of new technology, the law can be unclear in practice and needs clear guidelines.

7. CONCLUSION

The courts in both United States and Germany have long established that reducing the market of child exploitation material will ultimately protect children from further abuse. Laws against possession of child exploitation material are the direct results of that thought. With the development of technology, however, applying the existing law and terms have caused a discrepancy between verdicts. It is important to note that the term “possession” has evolved from being near or on the body to having actual control over the item, and ultimately determined by knowledge and intention. From the comparison above, it can be concluded that the courts are aiming in the same direction, while interpreting the indicators in different aspects. This slight difference in analysis could mean that in one country a defendant will be found guilty of possession while in the other country he could be found free of charges.

When both legislation and technology is common, consistency in rulings will do much

\textsuperscript{75} Id.
\textsuperscript{76} Dubach, at p. 70
\textsuperscript{77} Id.
towards prevention of illicit behavior. However, how to determine the most reasonable approach is arguable. The 'knowledge' and 'actual control' approach to possession leaves a loophole as defendants who are not proficient in technology cannot be penalized for possession. The 'active search' approach is met with critiques that it criminalizes mere viewing, more or less deserts the definition of possession and that the confirmation of a search pattern is more a supportive evidence than direct evidence.

An alternative solution is to criminalize "knowing access with the intention to view." With this additional clause, the term of possession would not be broadened unreasonably, and it would serve as a legal basis to convict active viewers of CEM more efficiently. The United States added this clause in 2008 and the EU directives also encourage criminalizing knowing access.

Adding a specific law to close a loophole in the legal structure is not an uncommon thing; to efficiently pursue offenders who took a vehicle from others but without the intention of stealing it (offender was planning to bring it back), South Korea has amended its law to include "theft of usage." This penalizes not the theft of the item itself, as it is stated in the theft law, but the taking away of the original owner's ability to use the time.

In our opinion, viewers of child exploitation material must be treated as consumers of the market. Especially nowadays, with the explosive growth of the Internet and access to online sources, criminalizing only those who stored the images permanently in a storage device seems unrealistic and discarding the purpose of the law. Amending the law to include "knowing access with the intention to view" could be considered similar to the usage theft law in South Korea; it would close the loophole courts were struggling to block.

This solution, however, is also not without concerns. Until now, knowing access has served mostly as supporting evidence rather than direct evidence. If this solution was implemented internationally, it needs to be addressed how to set the standards pertinent to this law to maintain legal structure.