UNITED STATES, Appellee

v.

Andrew P. OBER, Specialist
U.S. Army, Appellant

No. 07-0722

Crim. App. No. 20040081

United States Court of Appeals for the Armed Forces

Argued March 17, 2008

Decided June 16, 2008

EFFRON, C.J., delivered the opinion of the Court, in which BAKER, STUCKY, and RYAN, JJ., joined. ERDMANN, J., filed a dissenting opinion.

Counsel

For Appellant: Captain William J. Stephens (argued); Major Teresa L. Raymond (on brief); Lieutenant Colonel Steven C. Henricks, Captain Seth A. Director, and Captain Sean F. Mangan.

For Appellee: Captain Larry W. Downend (argued); Colonel John W. Miller II and Major Elizabeth G. Marotta (on brief).

Military Judges: Debra L. Boudreau (arraignment) and Gregory A. Gross (trial)

Chief Judge EFFRON delivered the opinion of the Court.

A general court-martial composed of officer and enlisted members convicted Appellant, contrary to his pleas, of making a false official statement, knowingly and wrongfully transporting child pornography in interstate commerce, and knowingly and wrongfully possessing child pornography, in violation of Articles 107 and 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 907, 934 (2000). The sentence adjudged by the court-martial included confinement for three years, a dishonorable discharge, forfeiture of all pay and allowances, and reduction to the lowest enlisted grade. The convening authority approved confinement for thirty months and approved the balance of the sentence. The United States Army Court of Criminal Appeals affirmed. United States v. Ober, No. ARMY 20040081 (A. Ct. Crim. App. May 25, 2007) (unpublished).

On Appellant's petition, we granted review of the following issues:

I. WHETHER THE EVIDENCE IS LEGALLY INSUFFICIENT TO SUPPORT A FINDING OF GUILT FOR TRANSPORTING CHILD PORNOGRAPHY IN INTERSTATE COMMERCE WHEN NO EVIDENCE EXISTS THAT APPELLANT UPLOADED CHILD PORNOGRAPHY FROM HIS COMPUTER TO THE INTERNET FILE-SHARING PROGRAM "KAZAA."

II. WHETHER THE ARMY COURT ERRED IN AFFIRMING THE FINDING OF GUILTY FOR SPECIFICATION 1 OF CHARGE I WHEN THE COURT AFFIRMED UNDER A DIFFERENT THEORY OF LIABILITY THAN WAS PROFFERED TO THE MILITARY PANEL, IN CONTRAVENTION OF CHIARELLA v. UNITED STATES, 445 U.S. 222 (1980).

III. WHETHER THE MILITARY JUDGE FAILED TO PROPERLY INSTRUCT THE PANEL ON THE ELEMENTS FOR SPECIFICATION 1 OF CHARGE I, BY: (1) OMITTING THE CHARGED LANGUAGE "CAUSE TO BE TRANSPORTED" FROM THE ORAL AND WRITTEN INSTRUCTIONS; (2) FAILING TO INSTRUCT ON A POSSIBLE GOVERNMENT ALTERNATE THEORY OF LIABILITY UNDER ARTICLE 77, UCMJ; AND (3) FAILING TO PROPERLY INSTRUCT ON THE TERM "UPLOADING" WHEN THE COMPUTER EXPERTS AT TRIAL PROVIDED TWO VARYING DEFINITIONS.

For the reasons set forth below, we affirm.

I. BACKGROUND

The present appeal focuses on the circumstances under which child pornography was obtained through the use of Appellant's computer. The prosecution's primary theory was that Appellant used a peer-to-peer file sharing program to obtain child pornography from other participants in the file sharing network. The primary defense theory of the case was that other individuals were responsible because they had access to Appellant's computer, Appellant had an alibi for the times when child pornography was transported to the computer, and there was ample exculpatory evidence to place the blame on others.

Section A describes the file sharing program at issue in this case. Section B summarizes the evidence developed during the initial investigation. Section C sets forth the evidence and the theories presented by the parties at trial.

A. APPELLANT'S FILE SHARING PROGRAM

Appellant built a computer from individual parts, which he maintained in his barracks room. He also created a network that connected his computer with the computers of three other soldiers in the barracks, enabling them to utilize his high-speed Internet connection. The computers on the network included the computer of Appellant's roommate, Specialist B. Appellant permitted Specialist B and several other soldiers to use his computer.

Appellant installed various programs on his computer, including KaZaA, a peer-to-peer file sharing program.[1] According to expert testimony introduced at trial, the KaZaA program installed on Appellant's computer enabled KaZaA users to share computer files, including music, movies, and images, over the Internet with other KaZaA users.

The KaZaA program provided two primary means of moving files between users of the program. In the first method, a KaZaA user who wanted to make files hosted on his or her computer available to other KaZaA users could do so by configuring the KaZaA program preferences to permit access by others. Setting the preferences involved a simple adjustment

[1] The opinion of the court below and the parties' briefs refer to various spellings of the program's name. For purposes of this opinion, we use the spelling reflected in the record of trial.

that could be changed at will by the host computer's user to enable or preclude access to files by other KaZaA users.

In the second method, the KaZaA program enabled a user to utilize a search function, similar to an Internet web browser, to obtain files hosted on the computers of other KaZaA users. To obtain files from other computers, the KaZaA user would open the KaZaA program and enter a search term. In response to the search request, the KaZaA program would display a list of file names and descriptions obtained from other KaZaA users whose preferences permitted such access. The KaZaA user who initiated the search could then view the names and file descriptions identified by the search and double click on the name of the files that the user wanted to obtain. The download process would begin once the user double clicked on the desired file. The KaZaA program would complete the download without further action by the user. The KaZaA user could limit the number of downloads that could take place at any one time. If the host logged out of the KaZaA program or otherwise blocked access to a file before the requested download was completed, the KaZaA program would attempt to obtain the file from another available user or would reinitiate the download when the host subsequently reopened the KaZaA program. Through the search function, the KaZaA program enabled the user, through a series of keystrokes, to identify a file, upload the file from the host computer, and

download the file to the user's computer. From the perspective of the KaZaA user seeking to obtain a file hosted by another computer, the actions of uploading and downloading were part of a continuous process managed by that user.

B. THE INITIAL INVESTIGATION

Appellant spent a substantial amount of his free time maintaining and upgrading his computer. The chain of events leading to the present case began when he returned from shopping for a computer device and thought that he was locked out of his third-floor barracks room. He attempted to enter through an outside window, but fell to the ground and suffered a serious injury requiring about a week of hospitalization and thirty days of convalescent leave.

While Appellant was absent from the barracks on convalescent leave, Specialist B and another soldier used Appellant's computer to play video games. As they were perusing his files for other available video games, they came across a file titled "13 year old," located in a KaZaA folder. They opened the file, saw a picture of a young, naked female, and closed the file. At that time, they did not advise anyone of what they had seen. A month later, Specialist B mentioned the incident in the course of a casual conversation with a noncommissioned officer. After an initial inquiry by the

noncommissioned officer, the Army's Criminal Investigation Command (CID) initiated a formal investigation.

CID agents obtained a statement from Appellant in which he acknowledged using his computer to access adult pornography but denied using it to access child pornography. In the course of the interview, Appellant provided CID with consent to examine the hard drive of his computer.

CID arranged for an analysis of the hard drive by a forensic expert. The forensic analysis identified 592 files containing possible child pornography on the hard drive, including 460 files located in a KaZaA folder. At the time of the forensic analysis, the preferences for the KaZaA program on Appellant's computer were set to: (1) permit the user to obtain files from other KaZaA users and download up to ten files at a time; and (2) preclude other KaZaA users from obtaining files from Appellant's computer.

In a second interview with CID, Appellant stated that he had downloaded and saved approximately forty files containing child pornography on his computer. He acknowledged that he had been viewing child pornography on his computer "[o]nce every two weeks" for about eight months, and that he knew that it was illegal to view and download child pornography. When asked whether he knew that the files contained pictures of children before he opened the files and viewed them, he said: "Some of

the pictures did not have accurate descriptions of what was in the file. Others had a description. I knew that some of the files would contain underage people in the pictures before I opened them." In response to the question of whether he saved some of the pictures, he stated: "You can't open the pictures until you download them. After I downloaded the pictures and viewed them I never deleted them." When asked whether he had passed on the child pornography to anyone else through the computer, he responded: "No." Appellant explained that in his previous statement to CID agents, he had denied using his computer to view child pornography because he was afraid of the consequences. In addition, Appellant stated that he had acted out of a lack of self-control and he knew that what he did was wrong.

Following the investigation, the Government charged Appellant with three offenses: (1) transporting child pornography in violation of Article 134, UCMJ; (2) possessing child pornography in violation of Article 134, UCMJ; and (3) making a false official statement about the use of his computer to access child pornography in violation of Article 107, UCMJ. The present appeal focuses primarily on the first offense, in which Appellant was convicted of a charge that he "did . . . knowingly and wrongfully cause to be transported in interstate commerce child pornography by uploading pictures of child

pornography to a shared internet file named 'KAZAA', in violation of 18 U.S.C. 2252A(a)(1)."

C. DEVELOPMENTS AT TRIAL

1. The prosecution and defense theories of the case

The prosecution, in its opening statement, advised the members that the evidence would show that Appellant "searched for, possessed, stored, shared, and viewed child pornography on his personal computer" and that "the evidence is going to show . . . that he was downloading child pornography on [his] computer." The prosecution stated that it would offer expert testimony to show that the KaZaA program "allows subscribers to download files." The prosecution also noted that the expert testimony would show that KaZaA "allows subscribers to upload their own personal files and retrieve files from other computers, and that these pornographic images, these movies, and these still photographs were obtained via this file sharing program." The prosecution described two methods used by Appellant to transport pornography: (1) Appellant "downloaded these images and possessed them on his computer"; and (2) "he allowed others to view them as they were transmitted from his computer."

Defense counsel, in his opening statement, observed that "if what the government promises you is true, it looked like they've got a pretty good case." Defense counsel reminded the

panel that the issues of "alibi" and "false confessions" had been discussed during voir dire.

With respect to the forensic evidence, counsel emphasized that the defense was going to focus on whether the evidence established that Appellant was the person responsible for the child pornography on his computer:

> They're going to bring in detectives to show you there's child pornography on this computer; and they may, in fact, show you that there is real child pornography on the computer, but the issue here is that the government's got the wrong guy. Now that may be hard to believe based on what you've heard.
>
> Now, what the defense is going to ask you to do is take a look as this case develops, keep an open mind, and see how good a job CID did do, how good a job the Defense Computer Forensic Lab did. Take a look at Specialist Ober and figure out if this is really the right guy for this crime.

Defense counsel proceeded to detail the defense theory of the case, based on alibi and exculpatory evidence: many others had direct access to Appellant's computer and access through the network established by Appellant; Appellant was in the field or on leave for extended periods when others had access to the computer; and his admissions to CID agents were the product of traumatic brain injury and stress. Defense counsel told the members that "at the end of this trial you're going to see the government does have the wrong guy."

2. Evidence presented by the prosecution

The prosecution introduced into evidence Appellant's confession that he downloaded child pornography on his computer knowing that it was illegal to do so, as well as related testimony regarding the circumstances surrounding the CID investigation and interrogation of Appellant. The prosecution also introduced into evidence specific images of the alleged child pornography, as well as expert testimony identifying the images as depictions of actual children. The defense stipulated that certain of the images consisted of child pornography of actual children.

The prosecution presented the testimony of a computer forensics expert, Jason Upchurch, regarding the alleged child pornography on Appellant's computer. The evidence presented by Mr. Upchurch indicated that there were 592 images of possible child pornography on the hard drive of Appellant's computer, and that the majority of the images were in the folder used for sharing files through KaZaA. Mr. Upchurch testified that there was no evidence that a computer virus had placed the pornography on the hard drive.

In response to a question from the prosecution, Mr. Upchurch noted that from his analysis, he could not determine the individual responsible for the images on Appellant's computer. Mr. Upchurch explained: "We can determine in most

cases . . . which account it came from, as well as, file dates and times; but as far as who put the images there, no, we can't determine that." When asked whether there were "any pointers" to Appellant as "the individual who downloaded the child pornography found on the computer," Mr. Upchurch testified that "the majority of the images belonged to the account called 'Oberator,' as well as, the computer was registered to a Mr. Ober."

Mr. Upchurch testified that the KaZaA preferences on Appellant's computer were set so that Appellant could obtain files from other KaZaA users. The settings permitted him to "download 10 files at a time," which was "a fairly optimized setting to maximize your download."

Mr. Upchurch explained how files were moved to Appellant's computer using KaZaA. He noted that there were "many versions" of KaZaA, and the version on Appellant's computer operated as a modified web browser. When the computer was turned on and the Internet connection was active, the user of the KaZaA program could "click on the search button," which enabled the user to "search for anything from movies to music or any other files by either keywords or file name." The KaZaA program also provided the user with the ability to search for particular types of files by descriptions.

According to Mr. Upchurch, KaZaA would not cause child pornography to be downloaded on the computer without the user's knowledge. He explained the specific actions that a user would have to take to obtain files from another computer using KaZaA:

> When you do the search it doesn't automatically download everything. All it does is present you with files to download. So you go through and look at which files that you particularly want to download, the human element in it, and download those particular files. So the search term gives you the results, and then a human goes in and picks those results.

The expert added that the user could not view the image based upon the results of the search. The user first had to make a determination whether to download the file based upon the file name and other information associated with the file. He added that with regard to some of the child pornography found in the KaZaA file on Appellant's computer, the file names and other information associated with the files were consistent with the age of the children depicted in the images.

The expert further explained the process used by KaZaA to obtain files selected by the user from another computer:

> [I]f the computer is on and KaZaA is running and you've selected files, KaZaA will continue to try to download those continuously until you tell it to stop. Even if at the other end if somebody logs off and the . . . file transfer is stopped because the other end is no longer available[, w]hen that other end comes back up KaZaA will see that and begin downloading again from the . . . same user because it all actually keeps track of files . . . .

> Q. So the user can be away from the computer at the time that the --
>
> A. Absolutely, days, weeks, yes.

At the time Appellant's computer was seized, the settings for the KaZaA program were set to prohibit other users from obtaining files from Appellant's computer. However, there was no way to determine when those settings took effect.

Defense counsel used the cross-examination of Mr. Upchurch to confirm that other KaZaA users could not upload files from Appellant's computer when the file sharing option was turned off. Counsel then focused on the dates that files were downloaded and accessed on Appellant's computer, with a view toward showing that someone other than Appellant had downloaded the files. On recross-examination, defense counsel again focused on questions that would suggest that Appellant was not the person who obtained the files.

During cross-examination of the other Government witnesses, defense counsel pointed to evidence that other individuals had access to Appellant's computer and the potential that others may have been responsible for the child pornography on his computer, the impact of the injury from Appellant's fall on his cognitive abilities and emotional state, the extended period in which Appellant was not in his barracks room, and related matters concerning the reliability of his confession.

3. Motion to dismiss

At the conclusion of the prosecution's case, the defense moved to dismiss the transportation of child pornography charge (Specification 1 of Charge I) on two grounds. First, the defense asserted that the prosecution "has failed to prove the element of distribution." Second, the defense contended that the prosecution "has failed to show any evidence that pictures were uploaded to the KaZaA file. All the evidence that came in this case indicated that pictures were downloaded to that file . . . ."

The prosecution responded that the charged offense at issue involved transportation, not distribution, of child pornography. The prosecution also noted that the manner in which a user of the KaZaA program obtained a file involved transportation: "Specification 1 merely requires that we show that child pornography was transported via the Internet so even by virtue of conducting a search and accessing child pornography from another KaZaA user that causes that particular image to be transported via the Internet."

The military judge observed that Appellant was charged with transporting, not distributing, child pornography; that he would give the members a definition of transporting; and that there was enough evidence on every element of the offense for the

issue to be decided by the panel rather than by a motion to dismiss.

4. The defense

Appellant testified as the first witness called by the defense. In response to defense counsel's question as to whether he committed the charged offenses, he responded: "No. I never did the offenses I'm accused of." He detailed the number of other individuals who had access to his computer. He also stated that he was not protective of his password, that he rarely logged off of his computer, that he frequently kept the computer on when he left his room, and that he was frequently away from his room performing assignments in the field. Appellant explained that other individuals who had access to his computer had an interest in pornography. He testified that his fall from the third floor of the barracks left him barely conscious, unable to eat, and fatigued, that he spent time on convalescent leave away from the base, and that the accident affected his memory and his performance.

Appellant acknowledged that he used the KaZaA program on his computer, that he had viewed adult pornography on his computer, and that child pornography was found on his computer. He denied downloading the child pornography himself or knowing that it was there before CID confronted him with the accusation. He stated that he confessed to downloading child pornography

during his second interview with CID because of his brain injury. Appellant testified that after a CID agent accused him of offenses involving child pornography, he felt his situation was hopeless. Appellant further explained that the agent told him that if he cooperated, the command would go easy on him. Appellant stated that the confession he gave to the CID agent was not true.

With respect to KaZaA, Appellant testified that it "was accessible to everyone." He added: "I used KaZaA to download music, and -- music was pretty much all I downloaded." He stated that he did not use KaZaA to download any pornography, child or adult.

The defense presented the testimony of a computer forensics expert who had performed an examination of Appellant's computer similar to the examination conducted by the prosecution's expert. The defense expert testified that he reviewed the computer files at issue in the present case to determine where in the hard drive they were located, the dates and times associated with the files, and "where those files came from." He also sought to determine whether other individuals had connected to Appellant's computer, and identified information indicating that at a particular time "someone was on this computer system, and the name does not correspond with the defendant." When the trial counsel questioned the relevance of

the defense expert's testimony, defense counsel responded: "[F]irst we're showing alibi, and the second portion is for showing that other people used Specialist Ober's computer, and that goes to possible exculpatory evidence." The military judge overruled the prosecution's objection. The expert then testified that there was information indicating that a person with a user name other than the name typically employed by Appellant used the computer at the time that child pornography "came into the system" onto Appellant's computer, and that the date in question was a date on which Appellant was in the hospital.

In response to questions from the military judge about the meaning of the "File Created" designation on the computer, the defense expert noted that the date of creation would be "the date that [the] file was, in this situation, brought in . . . from KaZaA." The expert also noted that files could be added to the hard drive without a person actually sitting at the computer if the person had scheduled the downloads to take place on a particular date.

The military judge asked about the relationship between "download" and "upload." The defense expert responded that downloading "is brining [sic] something to you." He then noted that uploading could involve two different types of activity by the user of the computer hosting the files: first, "if you had

an open portal where you're allowing somebody to take away from you," and second, if "you're physically going out and sending something out."

The military judge then asked the defense expert whether it would be "fair to make an analysis or an analogy that downloading is pulling, and uploading is pushing." The expert responded that the evidence in the present case involved the host allowing another user to obtain the material from the host's computer:

> In this situation, which we really didn't see any uploading going on, but in that type of situation it's -- if you were to open up the portal you are letting people pull it from you. You're not pushing it to them.

The expert also testified that he had seen no evidence that files from Appellant's computer had been pulled to another computer, but the expert noted that he did not have the equipment necessary to verify that determination. In addition, the expert stated that files could have been placed on Appellant's hard drive by another computer in the network.

The military judge then asked the defense expert whether it was necessary for a person to participate actively in the physical downloading of material from KaZaA:

> Q. Could a file that is on that hard drive that came from KaZaA . . . be inserted or put onto that hard drive, whatever the correct term might be, without someone sitting at the computer and downloading that?

A. That's always possible. Yes.

In response to a question from the prosecution, the expert clarified that a download from KaZaA might be initiated by a virus; otherwise, however, it would be necessary for an individual to start the download by clicking on a file.

During recross-examination by the prosecution, the defense expert witness emphasized that: "[I]f you are using KaZaA you are actually searching for something." The expert also explained that a download may not be completed on the day that the user first seeks to obtain the material. For example, if the user of the host computer prevented access to a particular file during the downloading process, that file could not be downloaded. In such a case, KaZaA would continue searching, and once another host opened up the file to permit access, KaZaA would complete the download of the file. Similarly, if the requested file was large, or if a user's KaZaA settings limited the number of downloads, the download might take place on a different day.

The military judge asked the defense expert about the origin of files downloaded through KaZaA. The expert reflected his agreement with the description of KaZaA offered by the prosecution's expert:

> KaZaA is just a tool, for instance, like Mr. Upchurch had said it's like a browser and you're looking at the whole Internet and other folks who have KaZaA running

> and shares running on their computer systems. You -- depending on the software, if you're using their versions you can get an address of who it's coming from, but it's coming from somebody else's computer generally out there on the World Wide Web.

The expert's answers to a member's questions clarified that the expert was able to identify use by different user names, but not by specific individuals.

5. Rebuttal

In rebuttal, the prosecution recalled Mr. Upchurch to discuss the evidence in light of the defense theories that others had used Appellant's computer at the time child pornography had been obtained. During the rebuttal testimony, the military judge asked the expert whether any action was required on the part of the owner of the host computer beyond making the host computer's files available through the KaZaA settings:

> Q. Mr. Upchurch, another question that was asked in this case was the definition of upload. I believe Mr. Lakes stated that when you -- uploading something is actually -- is not necessarily receiving --
>
> A. Giving.
>
> Q. Giving. Right. Now, on KaZaA when a user conducts a search on KaZaA or if you download a file from KaZaA, what happens on the computer that you're downloading from, on the actual user that you're trying to share from? What happens on that computer?
>
> A. So if I was downloading a file from my computer -- from someone else's computer, what happens on the other person's computer?

> Q. On the other person's computer if you seek to access a file on the other computer?
>
> A. It causes an upload to occur on the other person's computer.
>
> Q. Okay, and is that -- does that person have to specifically do anything to cause that upload?
>
> A. No. Everything is done prior in his settings.
>
> Q. So by virtue of the software you can cause the uploading [of] something on another individual's computer?
>
> A. On your computer.
>
> Q. On your computer?
>
> A. Yes, on your computer.

In its cross-examination of Mr. Upchurch, the defense focused on matters related to Appellant's alibi defense, suggesting that the use of the computer to play a particular computer game pointed to another individual as the user. The defense did not challenge Mr. Upchurch's explanation of the process used to obtain files by KaZaA.

At one point during Mr. Upchurch's testimony, he identified a series of dates and times that suspected child pornography was created and accessed on Appellant's computer. The military judge specifically instructed the members that the information about dates was being offered in regards to the defense of alibi; that the defense had stipulated that several of the images consisted of actual minors; and that it was the panel's

responsibility to decide whether the other images consisted of real children.

6. The military judge's instructions to the panel

The military judge provided the parties with his proposed instructions. He noted for the record that he had "asked if there were any specific instructions that either side wanted" and that the parties had replied in the negative. Later, following argument, the military judge asked if there were any objections to the instructions or requests for additional instructions, and noted that no objections were made.

The military judge instructed the members regarding the transporting charge:

> In Specification 1 of Charge I, the accused is charged with the offense of knowingly transporting child pornography in interstate commerce, in violation of Title 10 [sic], U.S. Code, Section 2252A(a)(1). In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt:
>
> One, that on or about and between 1 April 2002 and 27 December 2002, at Fort Hood, Texas, the accused knowingly transported material containing one or more visual depictions by uploading the material to a shared Internet file named KaZaA . . . .

The military judge provided further instructions on the remaining elements of the transporting charge, along with specific instructions on the terms "wrongful," "visual depiction," "minor," "sexually explicit conduct," "lascivious," "interstate commerce," and "knowingly."

In defining "visual depiction," the military judge noted that the term "includes . . . data stored on a computer disk or hard drive or by electronic means, which is capable of conversion into a visual image." With respect to interstate commerce, the military judge stated:

> Material traveling over the Internet, by its very nature, is within the definition of interstate commerce. The use of the Internet to send an image from one computer to another constitutes transporting the image in interstate commerce even if the receiving computer and the sending computer are located in the same state.

With respect to the term "knowingly," the military judge explained that the accused must have known the "nature and character of the material being transported . . . that it was a minor engaged in sexually explicit conduct." He added that "while the accused did not have to know that he was placing the items in interstate commerce, the items must have actually been transported in interstate commerce."

The military judge's instructions also expressly recognized Appellant's alibi defense:

> The evidence has raised the defense of alibi in relation to the offense of transporting child pornography. "Alibi" means that the accused could not have committed the offense charged because the accused was at another place when the offense occurred. Alibi is a complete defense to the offense of transporting child pornography. In this regard, there has been evidence that the accused was in the field and/or on leave during portions of time alleged in the specification.

> The burden is on the prosecution to establish the guilt of the accused. If you are convinced by [sic] a reasonable doubt that the accused was present at the time and place of the alleged offense, then the defense of alibi does not exist.

The military judge's instructions provided that the offense of transporting was not limited to the question of whether the accused committed the offense by uploading:

> [I]f you have doubt that the alleged material was transported by uploading, you may still reach a finding of guilty so long as the elements of the offense are proved beyond a reasonable doubt, but you must modify the specification to correctly reflect your findings.

7. Closing arguments by the parties

The prosecution, in its closing argument, noted Appellant's confession to knowingly downloading, retaining, and repeatedly viewing child pornography on his computer. The prosecution also addressed the evidence in the case apart from the confession, particularly in light of the defense position that Appellant did not know that there was child pornography on his computer, including his alibi defense. In the course of arguing that the members should reject Appellant's alibi defense, the prosecution noted: "Don't step on that land mine. He downloaded that child pornography. He viewed that child pornography."

With respect to the charge of transporting child pornography, the prosecution specifically addressed the mechanics of transporting images over the Internet using KaZaA.

The prosecution reiterated its argument that Appellant was guilty of transporting child pornography because downloading the images caused an upload to occur on the host computer. The trial counsel said to the members:

> On the Internet it's not like someone has to deliver it to you. You can deliver it to yourself, and read the specification. He's charged with causing child pornography to be uploaded and transported via the Internet, so he could -- on the Internet you could reach out that long arm, and nobody has to give it to you. It's there. It's just sitting there out in cyberspace, and all you've got to do is reach out, grab it, and carry it over interstate lines to your computer, and that's what he did. No one caused that file to be uploaded on the Internet except him because KaZaA allows you to reach out and grab it, and that's what he did. So consider the definition of transport, consider the nature of the Internet and how it allows us to transport without it being a two-party transaction.

The defense, in its closing argument, emphasized the alibi defense:

> Members of the Panel, we've seen a lot of evidence on the case today. We talked with you a lot about could somebody else have done it? Do they have the wrong guy?

The defense described the time periods in which Appellant was in the hospital or otherwise away from his computer. In addition, the defense focused on the evidence that other individuals had access to his computer, the different accounts used to access child pornography, and the relationship between his injury and the likelihood of a false confession.

In an effort to underscore Appellant's alibi defense, the defense counsel specifically acknowledged the use of the KaZaA program on Appellant's computer to access child pornography:

> Now, we also know that KaZaA was used at the same time Specialist [B] was on the computer. You found that KaZaA logo floating out there at the same time that [Specialist B] was on the computer, again, from Specialist Ober's hard drive.

Defense counsel also acknowledged the presence of child pornography in the KaZaA folder in the course of contending that the material was accessed by someone else, as suggested by the presence of child pornography in other folders associated with a different user name.

While suggesting that the members should not rely on Appellant's confession, defense counsel sought to contrast the presence of child pornography in the KaZaA folder with the absence of any reference to KaZaA in his confession: "Is there child pornography on this computer? No one's denying that there's child pornography on his computer, but this statement is not corroborated by the evidence." Moreover, in discussing the expert testimony, defense counsel questioned whether the Government expert's testimony could be used to identify who was using Appellant's computer when files were downloaded via the KaZaA program, and highlighted the defense expert's testimony to suggest that another person was using the computer at that time.

Defense counsel's closing argument addressed the charge of transporting from two different perspectives -- whether Appellant permitted others to transport child pornography from his computer and whether Appellant used KaZaA to obtain images from other computers:

> Let's talk about that first charge that he's charged with, uploading files to the Internet using KaZaA. Well, we know from his end of it, the KaZaA shared feature was disable[d], and so nobody took a single file off of his computer. We have no evidence one way or the other to tell you if Specialist Ober was even using it to take MP3 files, but you've got zero evidence that he himself was going out and reaching for these things, and there's zero evidence to tell you a single file was taken off of his computer.

Defense counsel proceeded on the basis that KaZaA had been used to access child pornography on Appellant's computer, but asked the members to conclude that "access" to child pornography on Appellant's computer occurred "when Ober wasn't there," emphasizing that his roommate, Specialist B, had access during that period. As such, defense counsel's closing argument focused on who used Appellant's computer to access child pornography, not whether the computer was used to transport child pornography.

II. DISCUSSION

We are presented with three separate questions in this appeal: (1) whether the evidence is legally sufficient to support Appellant's conviction for transporting child

pornography; (2) even if the evidence is legally sufficient, whether the Court of Criminal Appeals affirmed on a different theory of liability than was presented by the prosecution at trial; and (3) whether the military judge failed to properly instruct the members.

A. LEGAL SUFFICIENCY OF THE EVIDENCE

We review de novo the question whether the evidence is legally sufficient to support a finding of guilty for transporting child pornography in interstate commerce. See United States v. Young, 64 M.J. 404, 407 (C.A.A.F. 2007). The test for legal sufficiency of the evidence is "whether, considering the evidence in the light most favorable to the prosecution, a reasonable factfinder could have found all the essential elements beyond a reasonable doubt." United States v. Turner, 25 M.J. 324, 324 (C.M.A. 1987) (citing Jackson v. Virginia, 443 U.S. 307, 319 (1979)).

At trial, the prosecution initially offered two theories of transporting: (1) that Appellant used KaZaA to download child pornography on his computer; and (2) that Appellant made child pornography available to other KaZaA users. See supra Part I.C.1. These two theories were not mutually dependent. Even if the prosecution did not provide sufficient evidence to prove that Appellant allowed other KaZaA users to obtain child pornography hosted on his computer, the prosecution could rely

on its other theory, that Appellant transported child pornography by using KaZaA to obtain files hosted on other computers.

During its case-in-chief, the prosecution offered extensive testimony about how KaZaA operated to prove that Appellant transported child pornography by obtaining it from other KaZaA users. See supra Part I.C.2. The evidence demonstrated that a user could obtain child pornography via KaZaA by entering search terms into the KaZaA program, reviewing a list of shared file names and descriptions generated by the search, and initiating a process that uploaded files from the host computer and downloaded them to his computer.

The defense did not challenge the prosecution's evidence that child pornography was transported from a host computer to Appellant's computer through the KaZaA program. The defense and Government experts both agreed that a file could be moved through the Internet via the KaZaA program when a KaZaA user selected a file from a host computer's shared files and caused the host computer to upload the requested file. See supra Part I.C.2, I.C.4, I.C.5. The contested issue at trial was not whether Appellant's computer had been used to upload child pornography from another computer and download it to Appellant's computer. The issue at trial was whether the person using the

computer to transport child pornography was Appellant or whether it was another person who had access to the computer.

On appeal, Appellant argues that there is no evidence that he "uploaded those [child pornography] files, made those files available for uploading, or stored those files in a location where other individuals could access them through the internet." This argument fails to take into account Appellant's admissions that he acquired child pornography via the Internet, the evidence introduced by both the prosecution and the defense regarding the use of Appellant's computer to transport child pornography, and the expert testimony that using KaZaA to download files also involved uploading from the host computer. See supra Part I.C.2, I.C.4, I.C.5. In light of Appellant's pretrial confession to CID agents, the expert testimony regarding the files found on Appellant's computer, and the testimony regarding the underlying investigation of Appellant, the evidence at trial provided a legally sufficient basis upon which a reasonable factfinder could have found beyond a reasonable doubt that Appellant transported and possessed child pornography.

B. THE THEORY OF LIABILITY ON APPEAL

An appellate court cannot affirm a criminal conviction on the basis of a theory of liability not presented to the trier of fact. Chiarella v. United States, 445 U.S. 222, 236-37 (1980).

"To uphold a conviction on a charge that was neither alleged in an indictment nor presented to a jury at trial offends the most basic notions of due process." Dunn v. United States, 442 U.S. 100, 106 (1979); see also United States v. Riley, 50 M.J. 410, 415 (C.A.A.F. 1999).

As noted above, Appellant was expressly charged with "knowingly and wrongfully caus[ing] to be transported in interstate commerce child pornography by uploading pictures of child pornography to a shared internet file named 'KAZAA.'" The prosecution offered two different theories of transporting at the outset of the trial: (1) that Appellant downloaded child pornography onto his computer via the KaZaA program; and (2) that Appellant allowed other KaZaA users to obtain child pornography from his shared files. See supra Part I.C.1. After the Government's computer forensics expert testified that Appellant's KaZaA settings did not permit other KaZaA users to access his files, the Government focused primarily on the theory that Appellant was guilty of transporting child pornography based on his act of downloading such files via KaZaA. See supra Part I.C.2, I.C.5. The Government's expert testified that downloading images to Appellant's computer through KaZaA caused an upload to occur on the host computer. The prosecution's closing argument specifically contended that by downloading

child pornography via the KaZaA program, Appellant "caused that file to be uploaded on the Internet."

The Army Court of Criminal Appeals sustained Appellant's transporting conviction on the theory that "[A]ppellant's method of acquiring child pornography through use of peer-to-peer file sharing constituted transportation by uploading." Ober, No. ARMY 20040081, slip op. at 4. In reaching its decision, the Court of Criminal Appeals cited the testimony of the Government's computer forensics expert that a KaZaA user's download caused an upload on the host user's computer. Id. at 2-3. Although that specific description was not initially placed before the members in the prosecution's opening statement, it was referenced in the charging document ("uploading pictures of child pornography to a shared internet file named 'KAZAA'") and it was presented through expert testimony during the course of the trial. That is sufficient under Chiarella. Chiarella, 445 U.S. at 236. Under these circumstances, we conclude that the theory of liability relied upon by the Court of Criminal Appeals was one of the alternative theories of liability presented by the Government at trial, not a different theory.

C. ADEQUACY OF THE INSTRUCTIONS

Whether a panel was properly instructed is a question of law reviewed de novo. United States v. Maxwell, 45 M.J. 406,

424 (C.A.A.F. 1996) (citing United States v. Snow, 82 F.3d 935, 938-39 (10th Cir. 1996)). The military judge has an independent duty to determine and deliver appropriate instructions. United States v. Westmoreland, 31 M.J. 160, 163-64 (C.M.A. 1990). "'[T]he military judge must bear the primary responsibility for assuring that the jury properly is instructed on the elements of the offenses raised by the evidence as well as potential defenses and other questions of law.'" Id. at 164 (quoting United States v. Graves, 1 M.J. 50, 53 (C.M.A. 1975)).

On appeal, Appellant argues that the military judge made three errors in instructing the members. First, he argues that the military judge erred by omitting the charged language "cause to be" from the oral and written instructions on the transporting charge. According to Appellant, this omission was plain error because the military judge failed to give proper guidance to the members. Second, Appellant claims that the military judge erred by failing to instruct the members on a theory of aiding and abetting under Article 77, UCMJ, 10 U.S.C. § 877 (2000). Appellant claims that this instruction was mandatory because the Government theory of liability on the transporting charge involved the participation of another party. Third, Appellant argues that the military judge erred by failing to give the members a definition of "uploading." He contends that "uploading" was used by the Government in a manner

inconsistent with its normal usage, and thus the military judge should have provided a definition of the term to the members to eliminate any confusion as to its meaning or effect.

We address each of these contentions in turn. With respect to omission of the words "cause to be," we note that the military judge instructed the members that Appellant was charged with "knowingly transporting child pornography in interstate commerce." He further instructed that to convict Appellant, the members had to be convinced beyond a reasonable doubt that, among other elements, Appellant "knowingly transported material containing one or more visual depictions by uploading the material to a shared Internet file named KaZaA." Regarding the omission of the "cause to be" language that appeared in the specification, Appellant contends that the panel might have ignored that language or used it to convict Appellant under another theory of liability for which they were not instructed. As a threshold matter, Appellant has not demonstrated how omission of the words "cause to be" -- which are not part of the underlying statute -- changed the nature of the offense or left the members with a misunderstanding of the transporting charge and its specification. The defense did not object to the military judge's proposed instructions on the transporting charge, nor did the defense request any additional instructions to clarify the elements of the offense. Appellant's speculation

about the effect of the omission does not carry his burden to show an unfair prejudicial impact on the members' deliberations or material prejudice to his substantial rights. See United States v. Powell, 49 M.J. 460, 465 (C.A.A.F. 1998) (holding that plain error not objected to at trial does not compel reversal without a further determination that the error materially prejudiced the accused's substantial rights).

With respect to whether the military judge should have instructed on an aiding and abetting theory, we note that Appellant was charged and prosecuted with transporting child pornography as a primary actor. See Article 77, UCMJ. The Government focused its case on proving that Appellant was guilty of transporting child pornography based on his own act of obtaining files via KaZaA. Neither party requested an aiding and abetting instruction. Irrespective of whether the Government could have relied on an aider and abettor theory in this case, Appellant was not prejudiced by the decision of the military judge to focus his instructions on the primary theory presented by the prosecution.

The military judge did not provide a definition of "uploading" during the instruction phase of the trial. However, the computer forensics experts who testified for the Government and the defense offered comprehensive explanations of the KaZaA process, including uploading. See supra Part I.C.2, I.C.4,

I.C.5. The testimony did not produce a material difference between the parties or their experts regarding the operation of KaZaA or how KaZaA could be used to obtain files. The defense did not challenge the Government expert's testimony that downloading files through KaZaA caused an upload to occur on the host computer. Instead, the defense embraced the evidence of how KaZaA worked in an effort to convince the panel members that someone other than Appellant was responsible for downloading the child pornography on Appellant's computer. See supra Part I.C.1, I.C.4, I.C.7. The defense did not object to the military judge's proposed instructions, nor did the defense request additional instructions on uploading. In light of the manner in which both parties presented their evidence and theories at trial regarding the use of KaZaA, Appellant has not demonstrated that the absence of a further description of uploading -- a description not requested by the defense -- constituted material prejudice to the substantial rights of Appellant. See Article 59(a), UCMJ, 10 U.S.C. § 859(a) (2000).

III. DECISION

The decision of the United States Army Court of Criminal Appeals is affirmed.

ERDMANN, Judge (dissenting):

Because of the cumulative effect of errors at both the court-martial and Court of Criminal Appeals levels, I respectfully dissent. This case involves the Internet-based, peer-to-peer file-sharing network Kazaa. The Kazaa network does not utilize a main server where members can post images and other files, but rather Kazaa allows members to search for and download files located in the Kazaa folders on the individual computers of other members. Ober was a member of Kazaa and had the application on his computer. Images of child pornography which had been downloaded using Kazaa were found on Ober's computer. In addition to being charged with possession of child pornography, Ober was also charged with transporting child pornography by "uploading pictures of child pornography to a shared internet file named 'KAZAA.'"

My initial concern is that in affirming Ober's "transporting" conviction, the Court of Criminal Appeals relied on a theory not presented to Ober or the members until the Government's case in rebuttal. Consistent with the charged language, the Government initially proceeded on a theory that Ober had made images available to other Kazaa users by putting the images in his shared folder. Accordingly, in his opening statement the trial counsel stated Ober was guilty because "he allowed others to view [child pornography images on his

computer] as they were transmitted from his computer." Ober had notice and the opportunity to respond to this "uploading" theory because it was presented in the specification and the opening statement.

In developing this theory during its case-in-chief, however, the Government's computer forensic expert testified that the Kazaa application on Ober's computer was set to prevent uploading. Under this setting Ober could obtain files using Kazaa, but other Kazaa users could not access files on Ober's computer. In other words there could be no "upload" from Ober's computer.

The Government did not present the theory upon which the Court of Criminal Appeals based its decision until rebuttal, when the defense had already responded to the Government's case-in-chief.[1] This alternative theory of the case was presented when the Government's expert testified on rebuttal that when an

[1] The majority contends that the Government presented both theories in its opening statement because trial counsel discussed downloading of images. See United States v. Ober, __ M.J. __ (9, 32) (C.A.A.F. 2008). However, trial counsel never equated downloading images with "causing an upload" during his opening statement, nor did any witness make this strained connection during the Government's case-in-chief. Instead, trial counsel discussed downloading during his opening statement in the context of explaining why Ober would be found guilty of the possession charge, which is not in issue before this court. Only one theory of liability for the transportation specification was presented to the panel before the defense responded with its case-in-chief.

individual downloads a file using Kazaa that action "causes an upload to occur on the other person's computer." During closing arguments, trial counsel focused on the Government expert's rebuttal testimony: "No one caused that file to be uploaded on the Internet except him." While evidence was presented in the Government's case-in-chief that images of child pornography had been downloaded to Ober's computer using Kazaa, this evidence supported the possession specification and the Government did not equate this action with "uploading" until rebuttal. The Government abandoned the theory it relied upon in its case-in-chief and contended that Ober "caused an upload" when he "downloaded" files via Kazaa. The Court of Criminal Appeals affirmed Ober's conviction on this basis. See United States v. Ober, No. ARMY 20040081, slip op. at 3-4 (A. Ct. Crim. App. May 25, 2007) (unpublished).

Affirming a conviction based on a theory not presented in the Government's case-in-chief raises concerns regarding basic notions of due process.[2] Based on the charging language and the Government's case-in-chief, Ober did not have notice that when the Government charged him with "uploading," they intended the term to mean "downloading." Such a convoluted theory begs the

[2] Cf. United States v. Russo, 74 F.3d 1383, 1396 (2d Cir. 1996) (concluding that the prosecutor's behavior was improper where he created a "last minute" argument on rebuttal to which the defendant could not properly respond).

question as to why the Government just didn't charge him with "downloading." Due process notice and fundamental fairness require that the Government present its theory of the case to the factfinder and the accused before the accused's case-in-chief.

If this were the only error, I would be inclined to affirm as the "download means upload" theory was at least presented during rebuttal and the defense did not request additional time to respond. This error is compounded, however, by the military judge's failure to instruct the members on the definition of "uploading" and "downloading" and his failure to instruct the members as to the "cause to be" element in the charged offense.

As Ober was specifically charged with "uploading pictures of child pornography to a shared internet file named 'KAZAA'", the meaning of the term "uploading" was critical to the members' deliberations. There was, however, conflicting testimony as to the meaning of the term. While the military judge provided the members with definitions of a number of terms referenced in the elements of the offense,[3] he failed to instruct the members as to the definition of the most critical term -- "uploading."

During the Government's case-in-chief, the Government expert testified that Ober's computer contained child pornography that had been downloaded from Kazaa and that, under

[3] See Ober, __ M.J. at __ (23-25).

Ober's computer settings, no one could "upload" files from Ober's computer. This testimony would have been helpful to the Government had Ober been charged with "downloading" rather than "uploading." On rebuttal the Government expert revised his definition when he essentially testified that utilizing the Kazaa network, if member A "downloads" a file from member B's computer, that "download" causes an "upload" from member B's computer.

In regard to these terms, the defense expert testified that: "'Downloading' is brining [sic] something to you; and 'uploading,' in this situation, would be is if you had an open portal where you're allowing somebody to take away from you, or you're physically going out and sending something out." At best the various definitions discussed by the experts are very confusing.

While the majority concludes that the experts provided "comprehensive explanations of the KaZaA process, including uploading" and that these explanations were not materially different, this conclusion discounts the significant distinctions between the language initially used by both experts and the Government expert's subsequent recasting of the term. See United States v. Ober, __ M.J. __ (36-37) (C.A.A.F. 2008). Additionally, the "uploading means downloading" definition upon which the Government relies is counterintuitive and contrary to

the common understanding of the term "uploading,"[4] which further supports the need to define the term for the members. In this instance the definition of the term "uploading" is not a disputed fact to ultimately be found by the members, but is a legal term in the specification. Because the experts provided conflicting definitions of this crucial term, the military judge erred in not providing an instruction as to its meaning.

A military judge has an obligation to "instruct the members of the court as to the elements of the offense." Article 51(c), Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 851(c) (2000); see also Rule for Courts-Martial (R.C.M.) 920(e)(1) (requiring the military judge to describe the elements of the offense to the panel). These instructions must be "tailored to fit the circumstances of the case, and should fairly and adequately cover the issues presented." R.C.M. 920(a) Discussion.

Specification 1 charged that Ober did: "knowingly and wrongfully cause to be transported in interstate commerce child pornography by uploading pictures of child pornography to a shared internet file named 'KAZAA', in violation of 18 U.S.C.

[4] See, e.g., A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 n.1 (9th Cir. 2001) ("To download means to receive information, typically a file, from another computer to yours via modem. . . . The opposite term is upload, which means to send a file to another computer.") (citation and quotation marks omitted).

[§] 2252A(a)(1)." While the military judge did explain the various elements of this specification in his instruction, he did not reference or define the "cause to be" language. Although the Government has argued that the "cause to be" language is merely surplusage, it is clear that "cause to be transported" is not the same as "transported." As instructed, the members convicted Ober of "transporting" rather than "caus[ing] to be transported."

Before this court, the Government relied extensively on the Government expert's rebuttal testimony that accessing files on Kazaa "causes an upload to occur on the other person's computer." "Causes to be" must have meaning in order for the Government's rebuttal theory to be successful. As such, the term was critical to the Government's case and cannot be considered surplusage. When a case is premised on particular language in the specification, it cannot be disregarded. See United States v. Smith, 21 C.M.A. 264, 267, 45 C.M.R. 38, 41 (1972); United States v. Rowe, 13 C.M.A. 302, 310, 32 C.M.R. 302, 310 (1962). The military judge, therefore, erred when he failed to explain this phrase to the members in his instructions.[5] The military judge did not meet his clear obligation to present each element to the panel, tailor the

[5] Although the military judge informed that parties that he would define the term "transporting", he also failed to define that term.

instructions to the facts of the case, and give definitions of key terms, particularly those in conflict.

Given the cumulative effect of the due process error and the instructional errors, I would reverse the decision of the United States Army Court of Criminal Appeals as to this specification and order the record of trial returned to the Army Judge Advocate General for a new trial.