MISCELLANEOUS CASES

By Dennis Nicewander
Assistant State Attorney
17th Judicial Circuit
Broward County, Florida
Updated December 31, 2020

Table of Contents

CHILD PORNOGRAPHY ISSUES

Admissibility of Evidence

Expert Testimony

Screen names, significance of

United States v. Campos, 221 F.3d 1143 (10th Cir. 2000):

> Expert testimony in prosecution for transporting child pornography through interstate commerce via computer, that defendant's chosen screen name denoted people involved in sexual exploitation of children, did not violate "other crimes" rule, despite claim that expert thereby stated in effect that those persons using that screen name were necessarily pursuing or actually engaged in sexual activity with children; "sexual exploitation" could refer to distribution of pornographic images of children, and not necessarily to actual sexual activity.

Smith v. State, (Fla. 2009)

> Witness was qualified to offer an expert opinion on the meaning of code terms used in intercepted telephone conversations of gang members, which were introduced into evidence at a trial for capital murders, racketeering, and drug-related offenses; witness, who was third in command of the gang, used the codes on a daily basis and had already testified about the operation and organization of the gang, witness's testimony about the gang was completely substantiated by testimony of other gang members, one gang member independently testified about the codes used by the gang to indicate various types and quantities of drugs, and those codes were the same as witness's interpretation of the intercepted conversations.

Profile evidence in warrants (see Probable Cause chapter)

Cano v. State, 884 So.2d 131 (Fla. 2d DCA 2004):

> In affidavit supporting the warrant, a police officer wrote

regarding the characteristics of people who use computers to disseminate child pornography. The evidence would likely have been inadmissible character evidence, but the fact that such evidence was included in the affidavit does not make the warrant illegal. Expert evidence that might not meet a Frye standard may be considered in evaluation whether a warrant establishes probable cause.

Defense expert testifying about defendant's downloading habits

U.S. v. Shaffer, 472 F.3d 1219 (10th Cir. 2007):

> Exclusion of defendant's computer expert's proffered testimony, that based upon the file structure of defendant's computer hard drive defendant was on a pornography fishing expedition with no particular calculation toward any particular type of material, other than generally sexually explicit material, was warranted, in prosecution for distribution and possession of child pornography; the proposed testimony went to defendant's state of mind or whether he knowingly committed the charged offenses, and expert witnesses were prohibited from testifying regarding such ultimate issues.

Records Custodian testimony regarding cell site data

Perez v. State, 980 So. 2d 1126 (Fla. 3rd DCA 2008):

> Cellular telephone records custodians were not required to be qualified as experts to testify that a typical cell site covered an area of one to three miles, and that the telephone record detailed the actual cell tower involved in a particular call; testimony constituted general background information interpreting the cell phone records, serving to explain the concept of a cell site and how it generally related to cellular telephone company records.

Enhancing Sentencing Based on Butner Study

U.S. v. Crisman, 2014 WL 4104415 (D.N.M.)

> District court would not use study that concluded convicted child pornography offenders were likely guilty of

additional crimes against children, including contact offenses, as evidence in sentencing that defendant, who pled guilty to receipt of a visual depiction of minors engaged in sexually explicit conduct, was a threat to society; study suffered from several methodological flaws, including having a small sample size with 26% of participants already being known contact sexual offenders and relying on offenders to self-report, other studies indicated low rates of recidivism, and study looked at pre-incarceration conduct, rather than likelihood to reoffend.

Forensic Examiner Required to be Qualified as Expert

United States v. Wehrle, 985 F.3d 549, 554 (C.A.7 (Ill.), 2021)

The forensic-examination process here implicated Rule 702 because Wimmersberg testified to technical concepts beyond ordinary knowledge. During her direct examination, she was asked, "How do you go about conducting a forensic examination of a device?" She first explained the use of a "write blocker," a tool that permits access to data while protecting the integrity of the seized device. She then described the use of data-extraction software. She also described the reliability and safeguards in the software that prevent any alteration of the original data, and she discussed other technical concepts such as hashes (which convert one value to another and can establish identity) and metadata (data which gives information about other data).

4We recognize that not all testimony about the use of "technical" equipment will implicate Rule 702. Some uses are commonplace today. But even if a lay person may understand an officer's testimony about one of these concepts in isolation, an explanation of how they work together to preserve information and the integrity of the data crosses into Rule 702 territory. So we conclude Wimmersberg's testimony here concerning technical aspects of a forensic examination constitutes "specialized knowledge" under Rule 702.[4] Admitting her specialized knowledge without formally qualifying her as an expert witness was an abuse of discretion.

Probative Value of Images outweighs prejudice

U.S. v. Finley, 2013 WL 4046390 (C.A.3 (Pa.))

Videos and images obtained from computers in defendant's apartment were probative of the knowledge element of charged offenses of production, receipt, distribution, and possession of material depicting the sexual exploitation of a minor, for purposes of balancing test to determine if the evidence was unfairly prejudicial, even though defense counsel offered to stipulate that the videos and images were in fact child pornography; stipulation would not have relieved the government of proving the knowledge element of the offenses.

Videos and images obtained from computers in defendant's apartment were not unfairly prejudicial, in prosecution for production, receipt, distribution, and possession of material depicting the sexual exploitation of a minor; the evidence was probative of the knowledge element of the offenses, government showed the jury only 13 video segments and two images of what was a collection of more than 30,000 videos and images belonging to peer-to-peer (P2P) file-sharing account on defendant's computer, and district court had informed potential jurors of the disturbing images they might see, had asked the potential jurors if they could be fair, and had even dismissed one potential juror who had doubts about her ability to be fair on the subject matter of child pornography.

U.S. v. Ganoe, F.3d (9th Cir. 2008): **offer of stipulation**

In prosecution for receipt and possession of child pornography, district court did not abuse its discretion in ruling that probative value of selection of images found on computer in defendant's home was not substantially outweighed by danger of unfair prejudice; although defendant offered to stipulate images represented actual children engaged in sexual conduct and that anyone seeing them would know they were child pornography, he refused to stipulate that file titles alone would convey to reasonable user that files contained child pornography, leaving government obliged to prove that he was aware of images' content, and court limited government to ten clips with total duration of under one minute, and gave twice instructed jury to view images in impartial and unbiased manner.

The defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, and thus, agent's use of file-sharing software program to access child pornography files on the computer did not violate defendant's Fourth Amendment rights; defendant had installed and used file-sharing software, thereby opening his computer to anyone else with the same freely available program, and defendant had been explicitly warned before completing the installation that the folder into which files were downloaded would be shared with other users in the peer-to-peer network.

U.S. v. Sewell, 457 F.3d 841 (8th Cir. 2006)

Probative value of images found on defendant's computers, allegedly depicting child pornography, was not outweighed by the danger of unfair prejudice; the images pertained to multiple elements of the offense, including whether the images constituted child pornography and whether defendant knew this, and, prior to the appeal, defendant refused to stipulate to each of the relevant elements of the offenses.

A defendant's objection to evidence based on unfair prejudice, offering to concede a point, generally cannot prevail over the government's choice to offer evidence showing guilt and all the circumstances surrounding the offense.

United States v. Fox, 248 F.3d 394 (5th Cir. 2001):

In prosecution for knowing receipt of child pornography, probative value of images actually received by defendant, as best evidence of whether they were in fact child pornography, was not substantially outweighed by danger of unfair prejudice, despite images' potentially inflammatory nature and possible inclusion of irrelevant pornography depicting young adults.

Admissibility of NCMEC Reports

Elias v. State, 2020 WL 7776926 (Fla.App. 5 Dist., 2020)

Defendant was convicted at trial for 30 counts of sexual performance by a child. Detectives executed a search warrant on his home based on a NCMEC Cybertip concerning child pornography in a Flikr account.

The detective testified at trial that he received the NCMEC Cybertip concerning child pornography uploaded to the account.

The appellate court ruled that this was inadmissible hearsay and should not have been allowed. The court said the case law is clear that the substance of "tips" is inadmissible. The better practice is to say you began the investigation based on a tip without discussing its content. (If the detective had done a search warrant to Flikr, he could have admitted what he needed via the business records exception.) *my comment*

U.S. v. Blakeslee, 423 Fed.Appx. 136 (C.A.3 (Pa.),2011)

Testimony of FBI agent about National Center for Missing and Exploited Children (NCMEC) report indicating that 34 of the images of child pornography found in defendant's possession were matches to "known series" images that had previously been confirmed to contain images of actual children was insufficient to authenticate the report under business records exception to hearsay rule; despite the agent's expertise and general familiarity with NCMEC, he neither made the record nor had personal knowledge of its creation.

U.S. v. Baker, (5th Cir. 2008)

Government failed to present foundation for introduction, at defendant's trial for possessing, receiving, and distributing child pornography, report from National Center for Missing and Exploited Children (NCMEC), which contained filenames of 46 images if child pornography that Internet service provider determined had been uploaded to a Web site from an e-mail address that was later traced to defendant, but did not contain the images themselves; although provider's custodian testified at trial that provider had forwarded 46 images to the NCMEC and he confirmed that the e-mail address was unique and tied to defendant's residence, custodian did not identify any images or the filenames of any images, and no other witness or document in evidence vouched for the source, accuracy, or circumstances surrounding preparation of the NCMEC report.

District court plainly erred in admitting at defendant's trial for possessing, receiving, and distributing child pornography, three-ring binder containing printouts of 46 images of child pornography, which Internet service provider determined had been uploaded to a Web site from an e-mail address that was later traced to defendant, and which were identified by filename in a separate report from National Center for Missing and Exploited Children (NCMEC); officer who testified at trial that the 46 images were the

ones uploaded to the Web site had no personal knowledge of this fact or of the chain of custody for the images, government offered no independent evidence sufficient to show that defendant uploaded the images to the Web site, and images were essential to defendant's conviction for distributing child pornography.

U.S. v. Cameron, 699 F.3d 621 (C.A.1 (Me.),2012)

Documents reflecting data from account management tool and log-in tracker of online services provider and data from connection logs of second provider were non-testimonial business records, and therefore admission of data at trial in child pornography prosecution did not violate Confrontation Clause; data was collected automatically by providers to further their own business purposes, and served business functions that were totally unrelated to any trial or law enforcement purpose.

Tip reports that were passed on to law enforcement by national reporting organization, after it received child pornography reports from online services provider, were "testimonial" statements, since their primary purpose was to establish or prove past events potential to later criminal prosecution, and therefore their admission at trial in child pornography prosecution, without giving defendant opportunity to cross-examine reports' authors, violated Confrontation Clause.

Tip reports that were passed onto law enforcement by national reporting organization, after it received child pornography reports from online services provider, were introduced at trial in child pornography prosecution to prove the truth of at least some of matters asserted therein, as required for tip reports to be hearsay; reports were admitted to show that defendant had uploaded child pornography images onto several accounts with provider, and was the only evidence upon which government could have relied to establish specific dates on which offending images were uploaded.

Admissibility of Project VIC Image Classification

Queen v. State, 2021 WL 1111344 (Fla. 3rd DCA 2021):

In child pornography trial, a computer forensic examiner said he viewed all 300 of the charged images. He testified that he could clearly determine 299 of them depicted children. He said he could not make that determination on one of the images, so he relied on the image's classification in the NCMEC/Project VIC database. The appellate court ruled the defendant could not be convicted on

that count because the classification of the file by an unnamed officer was hearsay

Similar Fact Evidence

Admissibility of adult pornography in child pornography case

U.S. v. Smith, 459 F.3d 1276 (11th Cir. 2006)

In child pornography prosecution, district court did not abuse its discretion in finding that probative value of relevant photographs of defendant naked by himself, of defendant with other women who were not the victim engaged in sexually explicit conduct, and of women who were not the victim striking sexually suggestive positions was not substantially outweighed by any potential for unfair prejudice.

United States v. Nelson, * (9th Cir. 2002)

- Trial court erred in admitting 14,000 thumbnail pornographic images under circumstances where most were adult males and not relevant to charges of receiving and possession child pornography.

- The introduction of sexually explicit gay adult magazines was highly prejudicial evidence in a case involving the sexual abuse of minors.

Admissibility of child erotica in child porn prosecution

United States v. Rodriguez Fernandez, 2020 WL 7090699 (C.A.11 (Fla.), 2020)

Images of child erotica were inextricably intertwined with evidence of charged production of child pornography and possession of child pornography, and therefore district court did not abuse its discretion in not excluding them as "other act" evidence, since child erotica images illustrated

defendant's method of searching for, downloading, and storing child pornography files and, thus, helped complete story of offense, and images also were sufficiently linked in time and circumstances with charged child pornography files.

U.S. v. Fechner, 952 F.3d 954 (8th Cir. 2020)

Child erotica images found on defendant's cellular phone memory card was admissible, in prosecution for transportation of child pornography, and did not constitute inadmissible propensity evidence; defendant's download setting for the peer to peer sharing service he used automatically saved downloads onto his phone, not the memory card, to place the items on the memory card, a user would have to manually copy the items from the phone, and because hash values and thumbnail images of deleted child pornography were also found on the memory card, the evidence was relevant to establish that defendant knew about child pornography on the memory card.

United States v. Alford, 2018 WL 3700582 (Unpublished)

Trial court properly allowed government to introduce child erotica images in child pornography prosecution.

Admissibility of uncharged child pornography in child pornography prosecution

U.S. v. Fechner, 952 F.3d 954 (8th Cir. 2020)

The probative value of independently downloaded child pornography videos, which matched the hash values, name, length, and thumbnail images of unplayable files on defendant's phone and memory card, outweighed any danger of unfair prejudice, and thus the evidence was admissible during prosecution for transportation of child pornography ad receipt of child pornography; the jury saw only short clips of a few independently downloaded videos, and the videos were relevant to establish defendant knowingly possessed child pornography.

Summary of the videos downloaded by police officer during his undercover investigation was admissible, in prosecution for transportation of child pornography and

receipt of child pornography; the summary included the names, the date created, and a brief description of 36 video files downloaded during undercover download sessions, of the files, 15 stated only that "No video could be played" and six were already admitted into evidence, and the descriptions in the summary depicted what occurred in the video but did not make any conclusions or assumptions about the content.

United States v. Moberg, 888 F.3d 966 (C.A.8 (Mo.), 2018)

Even if defendant's statements to law enforcement agents that he had previously viewed child pornography on his computer, and that he was familiar with a known series of child pornography images, were evidence of prior bad acts, and not simply evidence that he committed the charged offenses, these statements were admissible at his trial for receiving and possessing child pornography to show that he acted knowingly, as required to support his conviction; district court also instructed jury on the limited use of the evidence, and defendant did not dispute that the acts he admitted to were factually similar and close in time to the charged offenses.

Baldino v. State, 2017 WL 3085326 (Fla.App. 4 Dist., 2017)

Trial court erred in ruling 124 uncharged child pornography images were inextricably intertwined with 99 charged images. State did not attempt to use similar fact evidence as a basis for admission.

United States v. Ross, 837 F.3d 85 (1st Cir. 2016), cert. denied, No. 16-6348, 2016 WL 5920786 (U.S. Nov. 14, 2016)

In prosecution of defendant for possession of child pornography, district court did not abuse its discretion when it admitted, over defendant's claims of unfair prejudice, a limited number of pornographic images and videos recovered from defendant's computer solely for purpose of demonstrating that defendant could not have somehow stumbled upon such images without immediately realizing their graphic content; while defendant had stipulated that his computer contained child pornography,

he did not stipulate to his knowledge of this pornography, and district court permissibly admitted six images and three videos from among the hundreds present on defendant's computer on theory that their relevance to knowledge issue was not outweighed by danger of unfair prejudice.

State v. Landrum, Not Reported in P.3d, 2015 WL 3932399 (Ariz.App. Div. 1)

Court ruled that State could introduce images that were not included in the charging document. They were relevant to issues of ignorance and some other guy did it.

U.S. v. Nance, 2014 WL 4695068 (C.A.10 (Okla.))

District court did not abuse its discretion, in child pornography prosecution, in admitting evidence that defendant's laptop contained over 1,000 previously-deleted images, pictures, and videos of child pornography, that he used his computer, at time when he claimed it was inoperable, and that, two years before charged offenses, defendant viewed two videos with file names indicating they contained child pornography, where defendant's defense at trial was that he did not know about child pornography on his computer, and court instructed jurors to limit their consideration of evidence to purposes for which it was admitted.

State v. Mercer, N.W. 2d (Wis. March 31, 2010):

"Other acts" evidence, including defendant's uncharged Internet searches for child pornography and his uncharged possession of 19 child pornography images on his hard drive, was admissible in prosecution for possession of child pornography arising from his viewing of Internet images on a particular day, as the evidence went directly to the defense that defendant was not searching for child pornography on that day, and it was extremely similar to the charged conduct.

U.S. v. Hatfield, 358 Fed.Appx. 692, 2009 WL 5033916 (C.A.7 (Ind.))

At trial of defendant charged with possessing child pornography, the district court did not abuse its discretion in admitting forensic computer examiner's limited

description of uncharged materials; because defendant wanted the jury to believe he was ignorant about the child pornography on his computer equipment and storage media, the district court reasonably determined that witness's limited description of the uncharged materials was relevant to corroborate special agent's testimony about defendant's statements and to show defendant's cyber-fingerprints on all the seized computer materials, and any risk of prejudice from this evidence was minimized by the government's decision to have witness describe these items instead of publishing them to the jury and by the limiting instructions given before witness's testimony and again before deliberations.

U.S. v. Schene, 543 F.3d 627 (10th Cir. 2008):

At trial of defendant charged with knowingly possessing material that contained an image of child pornography, the district court did not abuse its discretion in admitting exhibits containing images of child pornography, even images that were not charged in the indictment, despite defendant's willingness to stipulate that the images were child pornography; the images charged in the indictment and admitted as evidence in several of the exhibits were the gist of the government's case against defendant, and the government was entitled to prove its case, and, as for the uncharged images, which were contained in e-mails and a history pertaining to a charged video, they were introduced by the government to show intent and knowledge, and the jury was given limiting instructions.

U.S. v. Betcher, 534 F.3d 820 (8th Cir. 2008):

Probative value of 26 uncharged photographs admitted in defendant's trial for production of child pornography outweighed the danger of unfair prejudice; photographs were part of series of 78 photographs taken of the same five children, on the same fifteen dates, with the same model of camera, in the same home, and transmitted to the same computer in Georgia, from this series 29 photographs constituting child pornography were charged in the indictment, uncharged photographs corroborated the victims' testimony that defendant manufactured the pornographic pictures in his home, contextual clues in the uncharged photographs assisted in identifying the victims

in some charged photos, where the girls' faces were not visible, and the uncharged photographs did not contain graphic depictions of child pornography.

Rule providing that relevant evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice did not offer protection against evidence that was merely prejudicial in the sense of being detrimental to a party's case; rule protected against evidence that was unfairly prejudicial.

People v. Garelick, 161 Cal.App.4th 1107, 74 Cal.Rptr.3d 815 (2008)

Jury was not required to find that defendant possessed images indicative of child pornography with the specific intent to possess child pornography, in order to consider the images as evidence of uncharged acts to prove intent in trial for attempted lewd or lascivious act on a child under 14 and attempted distribution or exhibition of harmful matter to a minor; the volume of images and the fact that they were found in several different locations on defendant's computer made them relevant to establish his knowledge of their existence on his computer, and to establish the diminishing likelihood that their presence on his computer was inadvertent.

People v. Shinohara, 375 Ill.App.3d 85, 872 N.E.2d 498 (2007):

Evidence of child pornography for which defendant was not charged was admissible for purposes of showing defendant's defendant's intent in child pornography prosecution; evidence demonstrated that defendant's admission regarding young people on his computer referred to people younger than 17 year old victim, defendant knew he had images on computer of victim naked and engaged in sexual acts and did not hesitate to show them to police, and he told police he was embarrassed to have them view images of young people younger than victim, thereby demonstrating evidence of requisite intent for proving child pornography as it indicated defendant knew that children in images were under age 18.

United States v. Maxwell, 386 F.3d 1042 (11th Cir. 2004)

Uncharged images and evidence concerning defendant's

Internet activity was admissible "other crimes" evidence in prosecution for knowing possession of child pornography; the uncharged evidence was probative of defendant's knowledge and intent.

United States v. Dodds, 347 F.3d 893 (11th Cir. 2003):

The government introduced 66 out of 3400 child pornographic images found on defendant's computer. The defense argued that the prejudice outweighed the probative value because those pictures were not charged. The court ruled that the pictures were relevant for several purposes and therefore were properly admitted.

The court also ruled that the government circumstantially proved that the defendant downloaded the pictures from the Internet based upon the fact that the images possessed were commonly found and traded on the Internet, the children in the images were from several states, and there was no evidence that the defendant performed the difficult task of hand collecting the images. The government also showed that the defendant had access to the Internet and was familiar with using it.

U.S. v. Simpson, 152 F.3d 1241 (10th Cir. 1998):

The government could introduce child pornography found in a defendant's computer, other than the specific items he was charged with receiving; the evidence was of probative value in discounting the claim that the charged material was in his computer through mistake and to establish that he had knowledge of the type of material he was receiving, and the prejudicial impact of the evidence was minimized through court limitation on the number of items shown to the jury and the duration of the display.

Admissibility of Child Porn to Show Intent in Traveling Case

U.S. V. Mooney, (11th Cir. 2008):

In prosecution for interstate enticement of a minor to engage in sexual activity and aggravated sexual abuse with a minor, evidence of child pornography and Internet chat sessions involving sex with children that were discovered on defendant's computer was relevant to prove defendant's intent

to pursue and prey on young children, where defendant's primary defense at trial was that he lacked the intent to sexually abuse the child he arranged to meet, and that he drove to Georgia to protect her.

In prosecution for interstate enticement of a minor to engage in sexual activity and aggravated sexual abuse with a minor, probative value of evidence of child pornography and Internet chat sessions involving sex with children that were discovered on defendant's computer was not substantially outweighed by danger of unfair prejudice; the evidence contradicted defendant's testimony that the content of the chat rooms made him sick and that he visited Internet sites to prevent the sexual abuse of children, and the limiting instruction given by the district court mitigated any prejudicial effect of the evidence.

U.S. v. Brand, (2d Cir. 2006)

In prosecution for traveling in interstate commerce for purpose of engaging in illicit sexual conduct and using a facility of interstate commerce to entice a minor to engage in illicit sexual activity, evidence of child pornography images found on defendant's computer was admissible to show defendant's intent in attempting to entice undercover agent posing as 13-year-old girl in Internet chat room to meet him and in traveling across state lines to meet her, since the images demonstrated defendant's sexual interest in children.

Admissibility of Child Porn to Child Sexual Assault Case

State of Tennessee v. Rodriguez, 254 W.W.3d 361 (Tenn. 2008):

Presenting evidence suggesting that the defendant in a child sexual assault case possessed and viewed child pornography for no other purpose than establishing a predilection toward sexually abusing children places a defendant in a highly prejudiced posture before the jury and has the effect of converting the trial from an assessment of the charges against the defendant to a general inquiry as to his character.

Admissibility of Prior Acts of Child Molestation in Child Porn Case

United States v. Lafond, 2017 WL 345637 (E.D.Mich., 2017)

> Prior act of molesting child was admissible in child pornography prosecution.

U.S. v. Moore, 2011 WL 1834433 (C.A.5 (La.))

> Stepfather's touching of twelve-year-old stepdaughter's clothed buttocks, which occurred in her bedroom during the night, was an offense of child molestation, and thus admissible as evidence of defendant's similar crime in his prosecution for knowingly receiving and possessing child pornography; statute defined abusive sexual contact as "intentional touching, either directly or through the clothing, of the buttocks of any person with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person," and stepfather's conduct was neither inadvertent nor accidental, since he intentionally entered stepdaughter's bedroom to touch her.
>
> In prosecution for knowingly receiving and possessing child pornography, testimony of defendant's stepdaughter and excerpts from her diary, which indicated that defendant had sexually molested her when she was twelve years old, were admissible to demonstrate defendant's sexual interest in children, since evidence's probative value was substantially outweighed by unfairly prejudicial effect; evidence could help jurors determine whether defendant was correctly charged with child pornography offense and prejudicial effect was limited because of the similarities between alleged molestation and defendant's downloading of child pornography, since both acts involved similar mental states.

U.S. v. Sebolt, 460 F.3d 910 (7th Cir. 2006):

> Prior instances of sexual misconduct with a child victim may establish a defendant's sexual interest in children and thereby serve as evidence of the defendant's motive to commit a charged offense involving the sexual exploitation of children; it also may serve to identify the defendant to the crime.
>
> Evidence from defendant's handwritten confession that two weeks prior to his arrest, he drove to Wisconsin to have sex with a 16-year-old girl whom he first met online, was relevant to his motive, in prosecution for possessing, transporting, and advertising child pornography online; evidence confirmed defendant was indeed looking for "some fun loving molesting," as he advertised.

Portions of defendant's online chats, in which he discussed his past experiences with other molesters, as well as recent attempts, missed opportunities, and potential future opportunities to molest children, were relevant to motive, in prosecution for possessing, transporting, and advertising child pornography online.

Defendant's statement that he used the pair of young boys' underwear, that was found under his bed, when masturbating demonstrated his sexual interest in young boys and therefore was relevant to his motive, in prosecution for possessing, transporting, and advertising child pornography online.

Introduction of pair of young boys' underwear, that was found under defendant's bed, was unfairly prejudicial in prosecution for possessing, transporting, and advertising child pornography online; in light of admission of defendant's confession as to his use of underwear when masturbating, there was no probative value for admitting the physical evidence of his motive.

U.S. v. Burt, 495 F.3d 733 (7th Cir. 2007):

In prosecution for sexual exploitation of a minor and distributing child pornography, district court did not abuse its discretion in admitting child's testimony that defendant molested him; although defendant was not charged with any act of molestation against that child, and none of the pictures underlying the charges depicted defendant molesting that child, defense theory was that photographs defendant took of children were nonsexual, rather than lascivious exhibitions of genitals, and child's testimony that he was repeatedly molested by defendant during same period and in same rooms in which photographs were taken was relevant to question of whether defendant was taking pictures for legitimate, non-pornographic website, or to elicit sexual response in himself or others.

Admissibility of Lewd Literature in Child Porn Case

U.S. v. Shaffer, 472 F.3d 1219 (10th Cir. 2007):

Probative value of written narrative found on defendant's computer entitled “House of Incest” was not outweighed by risk of undue prejudice, in prosecution for possession and distribution of child pornography; defendant's strategy was to claim that he did not

knowingly possess or distribute child pornography, the narrative was relevant to rebut that defense, the narrative was far less prejudicial that the pornography placed before the jury, and the trial court provided a limiting jury instruction, advising jury that it could not consider the narrative as evidence of defendant's propensity to commit the charged offenses.

Admissibility of Sexually Explicit Emails in Child Porn Case

United States v. Norweathers, 895 F.3d 485 (C.A.7 (Ill.), 2018)

At child pornography trial, district court did not abuse its discretion in finding e-mail exchange, in which defendant and other individual discussed drugging and having sex with young boys, to be admissible bad other acts evidence; fact that defendant used e-mail account to discuss his sexual proclivity for young children, if proven, would tend to make it more likely that defendant, and not someone else, used that account to send e-mails containing images of child pornography, and that same fact would also tend to make it more likely that he intentionally, rather than unwittingly, sent charged e-mails and possessed pornographic images located on his hard drive.

Admissibility of Summary Evidence:

U.S. v. Fechner, 952 F.3d 954 (8th Cir. 2020)

Summary of the videos downloaded by police officer during his undercover investigation was admissible, in prosecution for transportation of child pornography and receipt of child pornography; the summary included the names, the date created, and a brief description of 36 video files downloaded during undercover download sessions, of the files, 15 stated only that "No video could be played" and six were already admitted into evidence, and the descriptions in the summary depicted what occurred in the video but did not make any conclusions or assumptions about the content.

Stipulations

United States v. Rodriguez, 2019 WL 6918504 (11th Cir. Dec. 19, 2019)

The trial court abused its discretion when it issued order precluding the admission of any videos or images containing child pornography, during prosecution for possession, receipt, and

distribution of child pornography; defendant could not stipulate his way out of the full evidentiary force of the case as the government chose to prevent it, the child pornography was probative as it tended to show both that the materials possessed, received, and distributed by defendant contained pornography and that he knew he had possessed, received, and distributed child pornography, and the nature and content of the videos were relevant not just to prove the discrete elements of the offense but to establish the human significance of the facts.

United States v. Lampley, 2019 WL 3000903, at *3 (C.A.5 (Tex.), 2019)

Whatever the length of the videos at issue, failing to introduce them will detract from the narrative strength of the prosecution's case and potentially upset jurors' expectations. Put another way, such videos are of significant probative value regardless of their duration. To be sure, the length of a video will increase the risk of prejudice, but the appropriate remedy to such prejudice is to shorten the clips, not to substitute a stipulation.

United States v. Luck, 852 F.3d 615 (C.A.6 (Tenn.), 2017)

District court did not abuse its discretion, in child pornography prosecution, in declining to permit defendant to stipulate to child-pornographic nature of images recovered from his computers, despite defendant's contention that digital images' file names established that they were child pornography; images' pornographic nature played vital role in government's narrative of concrete events comprising charged offense, images tended to establish both fact that they were pornographic and fact that defendant acquired and distributed images knowing they depicted child pornography, and showing images implicated law's moral underpinnings and juror's obligation to sit in judgment.

U.S. v. Finley, 2013 WL 4046390 (C.A.3 (Pa.))

Videos and images obtained from computers in defendant's apartment were probative of the knowledge element of charged offenses of production, receipt, distribution, and possession of material depicting the sexual exploitation of a minor, for purposes of balancing test to determine if the evidence was unfairly prejudicial, even though defense counsel offered to stipulate that the videos and images were in fact child pornography; stipulation would not have relieved the government of proving the knowledge element of the offenses.

Videos and images obtained from computers in defendant's apartment were not unfairly prejudicial, in prosecution for production, receipt, distribution, and possession of material depicting the sexual exploitation of a minor; the evidence was probative of the knowledge element of the offenses, government showed the jury only 13 video segments and two images of what was a collection of more than 30,000 videos and images belonging to peer-to-peer (P2P) file-sharing account on defendant's computer, and district court had informed potential jurors of the disturbing images they might see, had asked the potential jurors if they could be fair, and had even dismissed one potential juror who had doubts about her ability to be fair on the subject matter of child pornography.

U.S. v. Cunningham, 694 F.3d 372 (3rd Cir. 2012):

District court's refusal in defendant's trial on charge of receipt and distribution of child pornography to view video excerpts of child pornography to assess their prejudicial impact and, instead, over objection, rely only on written descriptions prior to admitting them, was arbitrary and unreasonable; although court had vivid descriptions of video excerpts, those descriptions should have heightened court's awareness of need to see videos to assess their prejudicial impact before it decided to admit them.

Stipulation establishing criminal content of child pornography videos was factor that had to be balanced in assessment of probative value of videos against danger of unfair prejudice in a trial on a charge of receipt and distribution of child pornography, although a defendant cannot stipulate away the prosecution's right to determine how to prove its case.

Because of the impact that visual images may have on a jury, if that type of evidence is challenged on grounds of unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence, a court should be prepared to view it before putting it before a jury.

Probative value of videos of pre-pubescent children being bound, raped, and violently assaulted was substantially outweighed by danger of unfair prejudice, and thus district court abused its discretion by admitting them in defendant's trial on charge of receipt and distribution of child pornography, given other available evidence to prove that defendant had knowingly possessed, received, and distributed child pornography.

U.S. v. Hatfield, 358 Fed.Appx. 692, 2009 WL 5033916 (C.A.7 (Ind.))

> At trial of defendant charged with possessing child pornography, the district court did not abuse its discretion in allowing the jury to view clips of 12 charged videos, even though defendant had stipulated that each fit the legal definition of child pornography; although prejudicial, the clips of the 12 videos were not unfairly so, and because they were central to the charged conduct, the government had the right to present them to the jury.

U.S. v. Alfaro-Moncada, 607 F.3d 720 (11th Cir. 2010):

> Risk of prejudice from admission of still images of child pornography on digital video discs (DVD) possessed by defendant did not substantially outweigh the still images' probative value in child pornography prosecution; despite defendant's stipulation, images proved that the DVDs actually contained child pornography, images also tended to show that defendant knew he was in possession of pornography, a fact to which he did not stipulate, and jury was only shown 5 out of 4,650 images on the DVDs.

U.S. v. Caldwell, 586 F.3d 338 (5th Cir. 2009):

> In prosecution for knowing possession and receipt of materials transported in interstate commerce involving the sexual exploitation of minors, trial court did not abuse its discretion when it showed jury short excerpts from three of seventeen different videos of child pornography found on defendant's computer over defendant's objection they were unfairly prejudicial; while defendant had stipulated that videos contained child pornography, stipulation's general, conclusory language did not have the same evidentiary value as actually seeing particular explicit conduct of specific minors.

U.S. v. Schene, 543 F.3d 627 (10th Cir. 2008):

> At trial of defendant charged with knowingly possessing material that contained an image of child pornography, the district court did not abuse its discretion in admitting exhibits containing images of child pornography, even images that were not charged in the indictment, despite defendant's willingness to stipulate that the images were child pornography; the images charged in the indictment and admitted as evidence in several of the exhibits were the gist of the government's case against defendant, and the

government was entitled to prove its case, and, as for the uncharged images, which were contained in e-mails and a history pertaining to a charged video, they were introduced by the government to show intent and knowledge, and the jury was given limiting instructions.

U.S. v. Ganoe, F.3d (9th Cir. 2008):

In prosecution for receipt and possession of child pornography, district court did not abuse its discretion in ruling that probative value of selection of images found on computer in defendant's home was not substantially outweighed by danger of unfair prejudice; although defendant offered to stipulate images represented actual children engaged in sexual conduct and that anyone seeing them would know they were child pornography, he refused to stipulate that file titles alone would convey to reasonable user that files contained child pornography, leaving government obliged to prove that he was aware of images' content, and court limited government to ten clips with total duration of under one minute, and gave twice instructed jury to view images in impartial and unbiased manner.

United States v. McCourt, 468 F.3d 1088 (8th Cir. 2006):

Defendant's stipulation to content of child pornography images did not preclude government from introducing to the jury seven three-second video clips.

Publication of seven three-second video clips of child pornography to jury was not unfairly prejudicial to defendant; only seven videos out of the more than 175 found on defendant's computer were shown to the jury and each for only three seconds.

United States v. Becht, 267 F.3d 767 (8th Cir. 2001):

Defendant's stipulation that 39 images seized from his computer depicted child pornography did not negate probative value, and thus admissibility, of images to prove that defendant was aware that he possessed and transmitted the images on his website at trial for knowingly possessing, and disseminating through interstate commerce, child pornography; illegal nature of images was just one element of crimes, defendant's awareness was additional, and more important, element.

Probative value of 39 images depicting child pornography to prove defendant was aware he possessed and transmitted the images on his website at trial for knowingly possessing, and disseminating through interstate commerce, child pornography, was not outweighed by risk of unfair prejudice; it was likely defendant had seen images when he sorted them to website subdirectories by hand, and images were not "close cases" of child pornography, but depicted children as young as four and five years of age, and admission of still photographs was not unfairly prejudicial.

United States v. Campos, 221 F.3d 1143 (10th Cir. 2000):

Even though defendant charged with transporting child pornography through interstate commerce via computer offered to stipulate that two images he was charged him with transporting constituted child pornography, jury was properly permitted to view those two images; defendant's offer to stipulate did not involve his legal status, but rather, gist of government's current case against him.

United States v. Hay, 9th Cir. 2000

Jury allowed to view images after stipulation

Closure of Courtroom

People v. Robles-Sierra, 2018 WL 1247579 (Colo.App., 2018)

District court's refusal to allow public gallery members in courtroom to see showing of videos and still images in child pornography trial did not constitute a "closure" of the courtroom as would violate defendant's constitutional right to a public trial; although videos and still images admitted into evidence were displayed using a screen that could only be seen by the witnesses and jury, and not by members of the public gallery in the courtroom, witnesses described such evidence in graphic terms in open court and members of the public were not excluded from the courtroom.

Constitutional Issues

United States v. Peterson, F.Supp (D.SC 2004)

This is a very helpful research source. In analyzing the constitutionality of

the law outlawing possession of child pornography, the court discusses the following cases:

- Stanley v. Georgia, 394 U.S. 557 (1969) *(unconstitutional to criminalize mere possession of obscene material)*
    - Osborne v. Ohio, 495 U.S. 103 (1990) *(distinguished a state's compelling interest in destroying the economic market for the exploitative use of children from a state's paternalistic interest in regulating the minds of its citizens.)*
    - New York v. Ferber, 458 U.S. 747 (1982) *(distinguished child pornography from obscenity by holding government has a compelling interest in preventing exploitation of minors)*
    - Ashcroft v. Free Speech, 535 U.S. 234 (2002) *(real children must be used in creation of child porn images to give government compelling interest to prosecute, otherwise, it is a protected form of speech.)*
    - Lawrence v. Texas, 123 S.Ct. 2472 (2003): *(it was a violation of due process for Texas to outlaw same-sex sexual conduct)*

Harm to Children Caused by Child Pornography

U.S. v. Zimmerman, 529 F.Supp.2d 778, 784-85 (S.D.Tex.,2007)

> *The Supreme Court in Raich also looked to the legislative history of the CSA to reach the conclusion that "Congress had a rational basis for believing that the failure to regulate intrastate manufacture and possession of marijuana would leave a gaping *785 hole in the CSA." Id. at 22, 125 S.Ct. 2195. In enacting the CPPA, Congress noted that "child pornography ... [has] become [a] highly organized, multimillion dollar industr[y] that [operates] on a nationwide scale."[10] S. Rep. No. 95–438, at 5 (1977), reprinted in 1978 U.S.C.C.A.N. 40, 42–43. Additional findings supporting subsequent amendments to the Act state, "the existence of ... child pornographic images ... inflames the desires of child molesters, pedophiles, and child pornographers who prey on children, thereby increasing the creation and distribution of child pornography...." S. Rep. No. 104–358, at 2, available at 1996 WL 506545. Furthermore, Congress articulated its belief that "prohibiting the possession and viewing of child pornography will encourage the possessors of such material to rid themselves of or destroy the material thereby helping ... to eliminate the market for sexual exploitation of children...." Id. at 3. In 2006, Congress issued findings specifically addressing the effects that intrastate incidents of child pornography have on the interstate market for child pornography. Child Pornography Prevention Act, Pub.L. No. 109–248, 120 Stat 587 (2006). The findings state that federal control of intrastate incidents of child pornography is "essential to the effective control of the interstate market in child pornography." Id.*

U.S. v. Johnson, 2010 WL 4008882 (E.D.Tex.)

> FN1. The horrors of child pornography are well documented, and the court need not describe them here. *See, e.g.*, *New York v. Ferber*, 458 U.S. 747, 102 S.Ct. 3348, 73 L.Ed.2d 1113 (1982); *United States v. Norris*, 159 F.3d 926 (5th Cir.1998); *United States v. Paroline*, 672 F.Supp.2d 781 (E.D.Tex.2009). The images and videos in this case, as in many other cases, were shared with others via a peer-to-peer network and were available for any interested person to view. Mr. Johnson may not have created these images himself, but there is grave harm in their widespread viewing and dissemination, not just in their initial creation. Violation of these children occurs not only when the images are created, but every time they are viewed. The viewing and possession of child pornography is far from a victimless crime.

Defenses

Cyber Vigilante Defense

U.S. v. O'Keefe, (11th Cir. 2006):

> No due process violation occurred in child pornography prosecution when government used defendant's silence, at time search warrant was executed and at other times prior to trial, to impeach his claim of having set up child pornography Internet sites in order to entrap offenders; defendant was not arrested nor given *Miranda* warnings at time of warrant's execution, and there was no evidence of his having received *Miranda* warnings at any other time. Also see United States v. Polizzi, 545 F.Supp.2d 270 (E.D.N.Y.2008) and United States v. Solomon, 1992 WL 25455, at *2-3 (9th Cir.1992) (unpublished decision)

Defense Attorney Defense

U.S. v. Flynn, 2010 WL 1459476 D.S.D.,2010.

> Peer to Peer investigation led to defense attorney's office. Attorney argued that he looked at child porn websites to properly advise his clients. He argued that federal law violated 10th amendment because it infringed upon the state's regulation of the practice of attorneys. He also asked for a Frank hearing because investigator did not mention in search warrant affidavit that suspect was a defense attorney who represented sex offenders. Defendant lost on all counts.

Forensic Examiner Corrupted Evidence

U.S. v. Flyer, 2011 WL 383967 (C.A.9 (Ariz.))

Government's unintentional corruption of data on defendant's laptop computer did not require suppression of evidence relating to child pornography charges, where corruption was result of negligence, rather than bad faith, and defendant did not show that mishandling of the evidence prejudiced his defense.

Forensic examiner inadvertently directly accessed the Apple hard drive when he was trying to image it. Defense expert argued that thousands of files were altered and potential evidence favorable to the defense was corrupted.

Literary Purpose Defense

United States v. Bunnell, F.Supp (Maine 2002)

Facts: University officials reported defendant for accessing child pornography on a university computer. Police investigated and obtained a search warrant for the defendant's home computer. Child pornography was found on his computer. The defendant said he was gathering the child pornography as part of a research paper he was doing at class.

Holding:

- "Literary purpose" is valid defense, but very rare. It raises First Amendment implications when the material has countervailing social value.
- The existence of a possible defense does not warrant dismissal of charges, but is an issue for the jury to decide.
- **Entrapment by estoppel** is a defense that requires the defendant establish that 1) that a government official told him that the act was legal; 2) that he relied on the advice; 3) that his reliance was reasonable; and 4) that, given the reliance, prosecution would be unfair. This was an issue for the jury, not for dismissal.

U.S. v. Reeder, 1999 WL 985177 (unpublished)

Research purpose could be a valid defense.

U.S. v. Matthews, 209 F.3d 338 (4th Cir. 2000):

> The First Amendment does not permit a bona fide reporter to trade in child pornography in order to create a work of journalism.

Government Failure to Follow DOJ Standards for use of CI

U.S. v. Christie, --- F.3d ----, 2010 WL 4026817 (C.A.3 (N.J.))

> Attorney General's guidelines on use of confidential informants did not themselves create rights for criminal defendant, and even if guidelines were violated in government's handling of informant who advised them of internet website that featured child pornography and provided them with information thereon, that would not mean, in itself, that user of website convicted of child-pornography-related offenses would be entitled to relief.
>
> Any violation of guidelines promulgated by the Attorney General on utilizing confidential informants, in connection with government's handling of fugitive who, acting through his attorney, provided government with information about internet website that featured password-protected forum where users could access child pornography, did not rise to level of outrageous government conduct, of kind violating the due process rights of site user charged with child-pornography-related offenses; while government benefited from information and site access that this individual provided, it did nothing to create or encourage criminal acts, and there was no evidence that information which it received from fugitive was untrustworthy.
>
> Discussion: This case is included because it may help when defense attorneys try to argue that they want to see the ICAC standards to see if the detective complied with them.

Discovery

Providing Child Porn to Defense in Discovery:

U.S. v. McNealey, --- F.3d ----, 2010 WL 4366921 (C.A.5 (Miss.))

> District court did not err in denying pretrial motion to dismiss indictment of defendant charged with possession and receipt of child pornography, based upon alleged restrictions on defense

expert access to his computer hard drive; defendant had full access to the government's exhibits and was free to research origin of images on his computer and create digital image exhibits, and, if he were concerned that his expert might be subject to prosecution, he could have obtained a protective immunity order if one had been warranted.

U.S. v. Wright, --- F.3d ----, 2010 WL 4345670 (C.A.9 (Ariz.))

Child pornography defendant had ample opportunity to inspect, view, and examine mirror copy of computer hard drive seized from his apartment, which allegedly contained images of child pornography, as required by Adam Walsh Child Protection and Safety Act, even if defendant did not have equal access to evidence, where defense counsel and defendant's forensic expert were permitted access to "bit-by-bit image copy" of defendant's hard drive at United States Attorney's Office, expert indicated he was "comfortable" with his access to copy, and defendant was afforded 14 months to conduct his examination of copy and did not claim that parties' arrangement precluded him from pursuing any viable defense theory.

Commonwealth v. Ruddock, Not Reported in N.E.2d, 2009 WL 3400927 Mass.Super.,2009.

Trial court ordered government to provide a "mirror image" copy of child pornography defendant's hard drive to defense expert.

Opinion cites to rulings from various other states on the issue and discusses the federal discovery rule. The case is a good research tool.

United States v. Shrake, 515 F.3d 743 (7th Cir. 2008):

The court found that he Adam Walsh Act provision restricting the possession of child pornography to the government were reasonable, but noted that when the government relinquishes control to a private examiner, they are giving the defense the opportunity to ask for their own private examiner. The court rejected the government's argument that a private expert retained by the government constitutes "government control" as required by the law.

U.S. v. O'Rourke, 470 F.Supp.2d 1049 (D.Ariz.,2007)

Provisions of Adam Walsh Child Protection and Safety Act of 2006, requiring all child pornography used in criminal trials to remain in possession of the government or the court, and prohibiting copying, did not mean that defendant's lawyers, as officers of the court, were to be given independent possession and control of the material, for purposes of his prosecution for, inter alia, transportation of child pornography. 18 U.S.C.A. §§ 2252A(a)(1), (b)(1), 2256, 3509(m).

To extent provisions of Adam Walsh Child Protection and Safety Act of 2006, requiring all child pornography used in criminal trials to remain in possession of the government or the court, and prohibiting copying, meant that government, in prosecution for, inter alia, transportation of child pornography, must either give defendant due-process-level access to hard drive at a government facility, or give defense a copy of the hard drive, statute comported with due process requirements.

Defendant was not deprived of due process, in prosecution for, inter alia, transportation of child pornography, by any government refusal to give defense experts private access to the internet when performing their analysis of the hard drive taken from defendant's computer; experts were free to use their own private wireless internet connections in government's office, and experts were offered, but did not take advantage of, opportunity to suggest other alternatives for internet access.

Defendant was not deprived of due process, in prosecution for, inter alia, transportation of child pornography, by government's provision to defense experts of a copy of defendant's hard drive which contained “malware” which allegedly precluded experts from obtaining necessary information from the hard drive, where issue was not raised during expert's visit; a suitable copy of the hard drive could be provided if expert would work with government to identify precisely what was needed.

Defendant was not deprived of due process, in prosecution for, inter alia, transportation of child pornography, by requirement that defense experts conduct their examination of defendant's hard drive in a government facility, allegedly hindering the ability of counsel, the experts, and defendant to speak freely and openly about possible defense strategies; government offered to make the hard drive available at a location where the defense team could confer privately.

Defendant was not deprived of due process, in prosecution for,

inter alia, transportation of child pornography, by requirement that defense experts travel from Ohio to Arizona to examine defendant's hard drive; experts made one such trip, during which they failed to avail themselves of all the time offered by the government, and in any case, hardship in traveling did not implicate due process concerns.

Hardship of out-of-state counsel in traveling to view evidence generally does not implicate due process concerns.

Defendant was not deprived of due process, in prosecution for, inter alia, transportation of child pornography, by his counsel's inability, due to government's restrictions, to have ready access to his computer's hard drive while preparing for trial; arrangements could be made for counsel to review the evidence in a government facility as often as necessary, and any inconvenience would not deny defendant a fair opportunity to defend himself.

Defendant was not deprived of due process, in prosecution for, inter alia, transportation of child pornography, by requirement that defense experts sign in at government facilities when analyzing defendant's hard drive, on basis that government would then have access to the identities of the experts; government counsel made clear that she had no intent of contacting defense experts, concerns could be addressed by a court order prohibiting such contact, and in any case experts had already contacted government counsel directly to arrange for an earlier inspection.

United States v. Knellinger, _F.Supp 2d-_ (E.D. Va. 2007)

Government, in prosecution for, inter alia, transportation of child pornography, failed to provide defendant with required "ample opportunity" to examine his computer hard drive at a Government facility, requiring provision to defendant of a copy of the hard drive; digital video experts' testimony as to the cost and difficulty of conducting their analyses at a Government facility, which were such that they would not agree to do the work, established that such analysis was not feasible.

Discussion: This is an unusual case in that the defense presented experts at an evidentiary hearing wherein they discussed the tremendous burden it would be to examine the hard drive at a government facility. They described having to transport truckloads of equipment to the facility at great expense. One expert testified that it would add hundreds of thousands of dollars

to the cost. Basically, the experts said they could not do it at the government facility. In an interesting twist, the court ruled that the duplicate hard drive would not have to be turned over to the defense until and unless the defense certified to the court that he had actually retained one of the two expensive experts who testified.

U.S. v. Frabizio, 341 F.Supp.2d 47 (D.Mass. 2004):

Defendant, charged with receiving and/or possessing child pornography, was entitled to obtain copies of images seized from his computer to enable his counsel to investigate how and when images came to appear and be accessed on his computer; there was no reason to think that defense counsel or her expert could not be trusted to abide by proposed protective order, government's concerns about risk of further dissemination were adequately addressed by proposed protective order, and government's concern about re-victimization would be implicated regardless of where defense counsel and her expert viewed images.

United States v. Hill, F.Supp (C.D.CA 2004) **Computer**

- Defense counsel and his expert have a right to copies of child pornography to prepare their defense. Requiring them to examine images at government lab would be unduly burdensome.

  Discussion: This case provides an example of the court order placing conditions on defense counsel to ensure images were not misused.

State v. Ross, 792 So.2d 699 (Fla. 5th DCA 2001):

Notwithstanding state's broad duty to disclose, state was not obligated to turn over to defendant contraband of computerized images of child pornography.

Defendant failed to demonstrate any prejudice or harm which would be caused by state's proposed procedure for review of the materials, which was to allow defendant, defense counsel, and defense experts to review the images provided Florida Department of Law Enforcement retained control over them.

Any concern that defendant might be required to reveal identity of consulting experts, information which is normally protected by work product privilege, can be adequately addressed by trial court

fashioning procedures which would allow consulting experts to review images without identity being disclosed.

Discussion: The court followed the reasoning of United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995).

U.S. v. Cox, 190 F. Supp. 2d 330 (N.D.N.Y 2002):

"Defendant contends that he is entitled to return of the contraband material at issue in this case during the pendency of these criminal proceedings. He is mistaken. The government has indicated it will make any and all evidence seized from defendant's home and computer available to him for inspection but not copying upon reasonable notice. Defendant provides no factual basis for his assertion that physical possession of the government's evidence is necessary to adequately prepare his defense nor does he cite legal authority which suggests he is entitled to return of illegal materials seized in the course of a criminal investigation. Based thereupon, defendant's motion for a protective order requiring the government to provide him with copies of its physical evidence is DENIED. "

U.S. v. Kimbrough, 69 F.3d 723 (5th Cir. 1995):

Government's refusal to allow defendant to copy seized child pornography as part of discovery process did not violate discovery rule, since child pornography was illegal contraband.

U.S. v. Horn, 187 F.3d 781 (8th Cir. 1999):

Trial court did not err in denying defendant's request for copies of video tapes since the tapes were prima facie contraband. Government's offer to allow defendant's expert to view the tapes was sufficient.

Providing Undercover Computer to Defense for Discovery

Siegel v. State, 2011 WL 3107821 (Fla. 4th DCA 2011):

Trial court did not err in refusing to permit the defense to examine the undercover computer of detective engaged in online communications with defendant. State complied with discovery rules by providing defense with copies of online chats.

Discovery of Search Protocols

U.S. v. Fumo, Not Reported in F.Supp.2d, 2007 WL 3232112 (E.D.Pa.,2007)

FTK logs revealing forensic examiners search terms etc… were not discoverable.

Sufficiency of Proof

Age of Child

Henderson v. State, 320 Ga.App. 553, 740 S.E.2d 280 (Ga. 2013)

Evidence was sufficient to show that defendant knew that children depicted in videos engaged in sexually explicit behavior with adults were under age 18, as required to support conviction for sexual exploitation of children, where videos were played for jury, and videos showed small children that were clearly prepubescent.

U.S. v. Noda, 137 Fed.Appx. 856 (C.A.6 (Ohio), 2005)

Admission, in prosecution for aiding and abetting receipt and possession of child pornography by computer, of expert testimony regarding the ages of the children depicted in the images introduced at trial, was not an abuse of discretion; expert, a pediatric nurse practitioner, was well-qualified.

U.S. v. Riccardi, 258 F. Supp. 2d 1212 (Kansas 2003):

"The threshold question--whether the age of a model in a child pornography prosecution can be determined by a lay jury without the [**8] assistance of expert testimony--must be determined on a case by case basis. As the government correctly points out, it is sometimes possible for the fact finder to decide the issue of age in a child pornography case without hearing any expert testimony. However, in other cases, the parties have been allowed to present conflicting expert testimony. In yet other cases, one party presents expert testimony, while the other does not. A case by case analysis will encounter some images in which the models are prepubescent children who are so obviously less than 18 years old that expert testimony is not necessary or helpful to the fact finder. On the other hand, some cases will be based on images of models of sufficient maturity that there is no need for expert testimony. However, in this case, in which the government must prove that a model, who is post-puberty but appears quite young, is less than eighteen years old, expert testimony may well be necessary to

assist the trier of fact to understand the evidence or to determine a fact in issue." Citing *U.S. v. Katz*, 178 F.3d 368, 373 (5th Cir. 1999).

United States v. Nelson, 38 Fed. Appx. 386, 392 (9th Cir. 2002).

- There is no requirement that expert testimony be presented in child pornography cases to establish the age of children in the pictures.

- Detective and probation officer should have not been able to render lay opinion regarding the age of the children because the jury was just as capable of doing that themselves.

United States v. Fox, 248 F.3d 394 (5th Cir. 2001)

- In prosecution for knowing receipt of child pornography via the computer, photographs were admissible in evidence without expert testimony as to subjects' ages as issue was one that could be determined by lay jury without assistance, particularly where defendant conceded that at least some prepubescent children were depicted and jury was not required to find that all 17 images depicted children.

U.S. v. Broyles, 37 F.3d 1314 (8th Cir. 1994):

Defendant's language, Postal Inspector's professional and personal familiarity with child development and pediatric professor's testimony were sufficient.

U.S. v. Anderson, 136 F.3d 747 (11th Cir. 1998):

Medical doctor's opinion sufficient to allow case to go to jury.

U.S. v. Katz, 178 F.3d 368 (5th Cir. 1999):

Whether age can be determined without expert testimony is determined on a case by case basis.

U.S. v. Stanley, 896 F.2d 450 (10th Cir. 1990):

Discusses agent's lay opinion testimony regarding age of images.

U.S. v. Pollard, 128 F.Supp 2d. 1104 (E.D. Tenn. 2001):

Analysis of *Daubert* standard as related to the admissibility of expert opinion of age of female depicted in videotape.

U.S. v. Rayl, 270 F.3d 709 (8th Cir. 2001):

> Court did not err in permitting experienced pediatrician to testify as an expert as to the age of children in photos, magazine and video found in defendant's possession.

Attempt to Produce Child Pornography or Induce Child to Commit a Sexual Act

U.S. v. Pierson, 544 F.3d 933 (8th Cir. 2008)

> Sufficient evidence established that defendant attempted to persuade undercover internet profile to engage in sexually explicit conduct and that defendant believed profile was of minor, as required to support defendant's conviction for attempted production of child pornography; defendant requested naked photos of profile, asked her to perform sexually explicit acts in front of webcam, offered to pay her if she could convince young friends to pose nude in front of webcam, attempted to determine age of profile to confirm he was not communicating with officer, and defendant told profile he believed she was fourteen year old female.

Morphed Images: First Amendment Defense

Ford v. State, 2010 WL 4263764 (Tex.App.-Beaumont)

> "In analyzing the issue of whether expert testimony is required for a jury to distinguish "real" children from "virtual" children, the Fourteenth Court of Appeals held that "the trial court is capable of reviewing the evidence, without the benefit of expert testimony, to determine whether the State met its burden to show the images depicted real children as opposed to "virtual children." *Porath v. State*, 148 S.W.3d 402, 417 (Tex.App.-Houston [14th Dist.] 2004, no pet.). We adopt the well-reasoned opinion of our sister court of appeals in *Porath* and conclude that the jury could determine, without the benefit of expert testimony, whether the images depicted actual children. *See id.* In addition, viewing the evidence in the light most favorable to the verdict, we conclude that a rational jury could have found the essential elements of the offense beyond a reasonable doubt."

U.S. v. Bach, 400 F.3d 622 (8th Cir. 2005):

> Defendant's conviction for receipt of child pornography, related to

receipt via e-mail of photo showing young nude boy sitting in tree with erection that had name of well known child entertainer beneath it and photograph of entertainer's head inserted onto photo of nude boy so that it appeared to be entertainer, did not violate First Amendment; morphed image involved real child with consequential mental harm to entertainer who was victimized every time picture was displayed and image created an identifiable child victim of sexual exploitation.

Stelmack v. State, --- So.3d ----, 2010 WL 4907468
Fla.App. 2 Dist.,2010.

Evidence was insufficient to support convictions for child pornography; defendant was found to be in possession of several images showing faces and heads of two girls, ages 11 and 12, cut and pasted onto images of 19-year-old woman exhibiting her genitals, statute governing offense proscribed knowing possession of photograph or representation that, in whole or in part, includes "sexual conduct by a child," and no part of any of the images displayed child who was actually lewdly exhibiting her genitals, and only sexual conduct in images was that of an adult.

Virtual Porn Defense: Proving "Real Child

U.S. v. Figueroa-Lugo, 2015 WL 4385935 (C.A.1 (Puerto Rico),2015.)

There is no per se rule in child pornography cases that the prosecution is required to produce expert testimony in every case to establish that the depicted child is real, for either guilt or sentencing purposes; rather, juries are capable of distinguishing between real and virtual images, without expert assistance.

U.S. v. Figueroa-Lugo, 2013 WL 43996 D.Puerto Rico,2013.

Evidence that the child pornography images found on defendant's computer depicted real-life minors rather than virtual images was sufficient to support defendant's conviction for possessing child pornography; although there was no expert testimony that the images contained real children, the jury saw the photographs found on defendant's computer, and they were not photographs that could be mistaken for cartoons or drawings.

State v. Tooley, 114 Ohio St.3d 366, 872 N.E.2d 894 Ohio, 2007**.**

Even if defense expert on child pornography established by his testimony that images of real children could be altered or "morphed" without detection to appear children were engaging in sexual activity, those images would not come within the scope of protected "virtual child pornography," which is either entirely computer-generated or created using only adults.

Statutory permissive inference did not render child pornography statute, which prohibited pandering sexually oriented matter involving a minor, unconstitutionally overbroad by improperly equating virtual child pornography, which was protected expression under the First Amendment, with pornography that involved real children, which was not protected; permissive inference that person in material was a minor, if the material, through its title, text, visual representation, or otherwise, represented or depicted the person as a minor, merely allowed state to prove its case with circumstantial evidence.

By presenting actual images to jury, state presented sufficient evidence that such images depicted real, not virtual, minors to support child pornography convictions.

U.S. v. Barker, Slip Copy, 2012 WL 12543 (D.Vt.)

When seeking a search warrant for child pornography, there must be "a probability or substantial chance" that the suspect possesses images of actual children, but the government is not required to make "an actual showing" that real children are depicted in the images.

U.S. v. McNealey, --- F.3d ----, 2010 WL 4366921 (C.A.5 (Miss.))

District court did not abuse its discretion in concluding that allegedly pornographic images of children retrieved from defendant's computer were properly authenticated as images of actual, as opposed to virtual, children, even though no evidence other than the images themselves was presented; jury was capable of distinguishing between real and virtual images, nothing in the record, including the images themselves, suggested that they were anything other than images of actual prepubescent children and young teenage girls engaged in what defendant conceded was lewd and lascivious conduct, and there was no evidence that the state of technology was such that images of that nature could have been generated using virtual children.

U.S. v. Kain, 589 F.3d 945 (8th Cir. 2009)

To support conviction for knowing possession of child pornography, the government is not required to introduce evidence other than the images themselves to prove they depict real rather than computer-generated children.

Evidence was sufficient to support finding that the images found on defendant's computer depicted real minors, as required to support conviction for knowing possession of child pornography; evidence included 27 images found on the computer, testimony of detective who conducted forensic examination of copy of computer's hard drive that the depicted females were prepubescent minors based on their physical features, and testimony of another law enforcement agent that the girl depicted in one image was about nine years old when he interviewed her some years after the photograph was taken, and defendant admitted he owned the computer and had used to download 40 to 50 images of child pornography to the file folder.

Testimony of law enforcement agent in child pornography prosecution, that the girl depicted in one image found on defendant's computer was about nine years old when he interviewed her some years after the photograph was taken, was an opinion based on agent's personal comparison of the girl and the photograph, and thus was admissible.

U.S. v. Bynum, --- F.3d ----, 2010 WL 1817763 (C.A.4 (N.C.))

Sufficient evidence supported jury finding that images and videos in question in defendant's prosecution for transporting and possessing child pornography depicted real children, rather than computer generated, where various officers testified as to identify and age of some of children in photos, and FBI analyst testified that images were not computer generated.

Qualifying FBI analyst as expert witness to determine authenticity of child pornography in prosecution for transporting and possessing child pornography was not an abuse of discretion, where analyst served 18 years with the FBI, had 13 years experience in examining questioned photographic evidence, completed proficiency testing in image authentication, had been qualified as an expert 35 times in the past, and testified as to process used in determining authenticity, including review by two other FBI employees.

State v. Clark, 158 N.H. 13, 959 A.2d 229 (N.H.,2008)

In a prosecution for child pornography, the state is not required to present evidence beyond the images themselves to establish that a real child is depicted.

U.S. v. Salcido, 506 F.3d 729 (9th Cir. 2007):

Government authenticated videos and images of child pornography found on defendant's hard drives and CD-ROM by presenting detailed evidence as to chain of custody, specifically how images were retrieved from defendant's computers.

Whether visual images involve actual minors engaging in sexually explicit conduct is not a question of authentication of images, but is more properly a challenge as to whether the government presented sufficient evidence to prove all elements of its case.

Generally, the government is permitted to present child pornographic images at trial and must subsequently present proof that the images depict actual children, but the government is not required to pre-screen, or pre-authenticate, child pornographic images to make sure that they are indeed real.

The government has the burden of proving beyond a reasonable doubt that the pornographic images offered as evidence are of actual children, not computer-generated images.

Expert testimony is not required for the government to establish that pornographic images depicted an actual minor.

Evidence was sufficient to sustain defendant's conviction of receiving and possessing child pornography, since government presented additional evidence to show that images retrieved from defendant's computer depicted actual not virtual children and that defendant knowingly received and possessed images, including detective's testimony that during prior investigation he had identified and interviewed victim depicted in one video, and another officer testified that defendant admitted to viewing and downloading child pornography on internet and admitted to obtaining child pornography from individuals he communicated with via Yahoo! Instant Messenger.

U.S. v. Sheldon, 223 Fed.Appx. 478 (6th Cir. 2007):

Government was not required to prove the pornographic depictions of children at issue were of real minors, as opposed to virtual

minors, under framework laid out in *Ashcroft v. Free Speech Coalition*, in prosecution for receipt, attempt to distribute, and possession of child pornography; government's contention that images were real were to be credited or discredited by the jury, and *Free Speech Coalition* did not impose a special or heightened evidentiary burden on government to prove that images were of real children.

Evidence was sufficient to support conviction for receipt, attempt to distribute, and possession of visual depictions of minors engaging in sexually explicit conduct; no contrary evidence was offered to suggest either that any of the visual depictions were computer generated, or that they were not produced using actual minors, and jury was capable of making determination on its own.

U.S. v. Halter, 259 Fed.Appx. 738 (C.A.6 (Ohio))

Law enforcement officers did not provide hearsay testimony, at trial of defendant convicted of possession of sexually explicit visual depictions of minors, when they gave testimony regarding people, objects and locations depicted in images in question, after viewing images and then personally observing persons, objects and locations.

"The government witnesses testified in court based on their personal knowledge of what was depicted in the images. Most of the witnesses met the victims while conducting their respective investigations. They personally observed the people, objects, and locations featured in the images. Therefore, the district court did not commit plain error by admitting the testimony."

Jalbert v. State, 30 Fla. L. Weekly D1672 (Fla. 5th DCA 2005):

No error in denying motion to dismiss child pornography charges on ground that state failed to establish that photographs depicted actual children and were not computer-generated children or adults resembling children.

Question of whether photographs depicted actual children is question of fact, not law, and is appropriate for trier of fact to determine.

Discussion: In dicta, the court noted that the State still has to prove the image is real child at trial, but the court did not discuss the quantum of proof.

People v. Shinohara, 375 Ill.App.3d 85, 872 N.E.2d 498 (2007):

> Expert's testimony as to opinion regarding whether particular image was real or virtual was admissible in child pornography prosecution as expert had extensive practical experience working with images of child pornography as well as demonstrated knowledge of computer-generated images.
>
> Testimony about factors that should be considered when determining whether given image is of a real person did not rely on application of scientific principles, and thus, Frye hearing was not necessary as testimony relied on skill, knowledge, experience, and observations as to what factors should be considered when evaluating whether image depicted real person.

U.S. v. Frabizio, 445 F.Supp. 152 (D.Mass. 2006):

> Fact that proffered expert on image authentication had never been subjected to proficiency testing militated against admission, in prosecution for possession of child pornography, of his opinions regarding whether images found in defendant's possession were those of real children; neither Court nor jury could assess the reliability of expert's opinions.
>
> For purposes of determining whether work of proffered expert on image authentication was admissible in prosecution for possession of child pornography, peer review process to which his technique for determining whether images found in defendant's possession were those of real children had been subjected, in which expert's co-worker merely analyzed images contemporaneously with expert's checklist and report, militated against admission; process ran a substantial risk of examiner bias.
>
> Fact that technique used by proffered expert on image authentication lacked a known error rate militated against admission, in prosecution for possession of child pornography, of his opinions regarding whether images found in defendant's possession were those of real children; Court had no way of knowing whether expert's experience amounted to expertise, and jury was unable to assess the proper level of deference to be accorded the expert's conclusions.

Fact that techniques used by proffered expert on image authentication were not subject to standards and controls militated against admission, in prosecution for possession of child pornography, of his opinions regarding whether images found in defendant's possession were those of real children; no guidelines existed as to the number or type of factors needed to conclude that an image was real.

Fact that technique used by proffered expert on image authentication was not generally accepted by others in the field militated against admission, in prosecution for possession of child pornography, of his opinions regarding whether images found in defendant's possession were those of real children; technique was apparently the product of recent work by a group of FBI employees who endorsed one another's work.

Conclusions of proffered expert on image authentication, as to whether images of alleged child pornography found in defendant's possession were images of real children, were inadmissible in prosecution for possession of child pornography; in light of fact that expert had not been shown to be reliable pursuant to *Daubert*, his conclusions asserted a level of certainty unjustified by his methodology and experience.

In the absence of any testimony from a computer expert who could arguably eliminate the possibility that images of alleged child pornography found in defendant's possession were wholly computer-generated, observations of proffered expert on image authentication, regarding the characteristics of images that had been manipulated, were inadmissible in prosecution for possession of child pornography; it was not shown to be possible to evaluate the images based only on visual observation.

U.S. v. Frabizio, 463 F.Supp.2d 111 (D. Mass. 2006):

Question whether jury can evaluate, without expert testimony, whether images of alleged child pornography are real or virtual, which question involves whether technology has advanced to point that virtual image is indistinguishable from real one upon visual observation, is a factual one, not a legal one, and one whose answer may well change over time.

While testimony from computer expert, that images of alleged child pornography found in defendant's possession were not wholly computer-generated, would be required, in order for observations of proffered expert on image authentication,

regarding characteristics of images that had been manipulated, to be helpful to jury in prosecution for possession of child pornography, it was not necessary for computer expert's testimony to establish "to a certainty" that the relevant images depicted real children or that they were not wholly computer-generated.

Discussion: This opinion is a clarification of this courts previous and more lenghthy ruling.

United States v. Irving, 432 F.3d 401 (2nd Cir. 2005)

In prosecution for receiving and possessing child pornography that was based on defendant's possession of video computer files, government was not required to also present expert testimony proving that children in images were in fact real children rather than computer-generated images; proof of children's actuality could be made via images alone, i.e. jury, which was instructed as to requirement for "use of a minor," could decide whether actual children were depicted in images.

United States v. Bach, 400 F.3d 622 (8th Cir. 2005):

Defendant's conviction for receipt of child pornography, related to receipt via e-mail of photo showing young nude boy sitting in tree with erection that had name of well known child entertainer beneath it and photograph of entertainer's head inserted onto photo of nude boy so that it appeared to be entertainer, did not violate First Amendment; morphed image involved real child with consequential mental harm to entertainer who was victimized every time picture was displayed and image created an identifiable child victim of sexual exploitation.

United States v. Deaton, (8th Cir. 2003):

"Further, we have previously upheld a jury's conclusion that real children were depicted even where the images themselves were the only evidence the government presented on the subject. See United States v. Vig, 167 F.3d 443, 449-450 (8th Circuit) (government, as part of affirmative case, was not required to negate unsupported speculation that images may have been computer-generated or other than what they appeared to be.

United States v. Pabon-Cruz, 255 F.Supp.2d 200 (S.D. NY 2003)

Direct proof of defendant's knowledge that visual images he received or distributed were produced using actual minors rather than virtual images is not required for conviction of receiving or

distributing child pornography; proof of knowledge may be made out by circumstantial evidence.

Evidence in prosecution for receiving or distributing child pornography was sufficient to support finding that defendant had knowledge that the visual images he received or distributed were produced using actual minors rather than virtual images; defendant stipulated that various photographs recovered from his file server depicted actual children and were not digital or virtual creations or computer generated images, defendant's computer contained hundreds of child pornography files, neatly organized into categories, thus indicating that he was familiar with the files it contained, and nothing in defendant's ads posted in online chatroom devoted to "preteenrapesex," or in photographs viewed by jury, suggested that the images did not depict real children.

United States v. Guagliardo, 278 F.3d 868 (9th Cir. 2002)

Federal agent's testimony that he had seen questioned images in magazines from the 1970s was sufficient to prove image depicted a real child.

United States v. Nolan, 818 F.2d 1015 (1st Cir. 1997):

- Evidence was sufficient to establish that the magazines contained photographs of minor children. In so ruling, the appellate court held that it was immaterial whether the children came from another country. Further, the prosecution was not required to produce expert evidence to establish that the reproductions were photographs and not drawings or some other type of images not dependent upon the use of actual subjects. Rather, it was within the range of ordinary competence for someone to determine that what was being viewed was a photograph rather than an artistic reproduction. Indeed, appellant presented no expert evidence that the pictures could have been produced by artificial means, much less that the costs of such technical means were low enough to have been practicable for the manufacture of pornographic magazines.

- The test of a factfinder's power to judge evidence without expert help is not whether he or she could ever be mistaken, but whether the subject is within the range of normal experience and knowledge.

  Discussion: The defendant "contended the government never authenticated the pictures because it failed to demonstrate that

producing them had involved *the use* of minors engaging in sexually explicit conduct, as the statute requires. Nolan contends, in particular, that the government did not present evidence sufficient to show that the pictures in the magazines were of actual children and not, for example, of wax figures or mannequins. In a similar vein, Nolan complains that the prosecution failed to prove that the pictures were not composite representations or otherwise faked or doctored, or perhaps computer-generated. He suggests, for example, that the pictures could have been fabricated using photographs of nude children taken from legitimate sources like a medical textbook." The court ruled that it was a basic authentication issue and the government did not have to disprove all of the above.

Zabrinas v McKune, F.Supp (D.K. 2004)

Petitioner claims that the only evidence that the State produced to show that the children depicted in the photographs were "real" was the testimony of Nurse Peterson, who testified that the ages of all the children in the pictures were between 5 to 14 years old. Petitioner asserts that despite the nurse's testimony regarding the ages of the children in the photographs, the State did not prove beyond a reasonable doubt that "the images were in fact digital copies of negatives of real (living) children, or original files of real children taken by a person with a digital camera . . . ." The court has reviewed the opinion of the Kansas Supreme Court and determines that it applied the correct standard in reviewing the evidence presented at trial. The state supreme court concluded that there was sufficient evidence before the jury to support the conviction. Specifically, the court stated that "it is clear from the record that all the images and photographs depict children, and sometimes adult males with children, engaged in sexually explicit conduct." Zabrinas, 24 P.3d at 80. Moreover, the trial court instructed the jury that in order to establish the charge of sexual exploitation of a child, the State had to prove "that the real child was then a child under the age of 16years." (emphasis added). It was for the jury to determine the weight of the evidence and the credit to be given the witnesses. Viewing the evidence in the light most favorable to the prosecution, the court concludes that a rational trier of fact could find that Petitioner [*31] violated K.S.A. 21-3516.

United States v. Fuller, (6th Cir. October 9, 2003):

In particular, defendant argues that although Dr. Rogers testified concerning the developmental stages of the depicted **[*23]** minors,

he conceded that he was not an expert in computers and could not determine whether the images were computerized or were of real minors. When asked if he could tell whether the pictures on defendant's computer were of actual people, **Grummow** testified that some of the pictures were of the defendant and other known persons and that the visual depictions of child pornography "appeared to be" live human beings. Finally, defendant relies on the statement by Rehman, the expert in computer forensics and child exploitation, that: "All of the images appear to have real children in them." When read in context, however, and in the absence of any evidence that the images were computer-generated or "virtual" child pornography, it is clear that there was sufficient evidence that actual minors were involved in the production of the images.

Significantly, no contrary evidence was offered to suggest either that any of the visual depictions were computer generated, or that they were not produced using actual minors. Having not only heard the above testimony, but also having viewed the images in question, the jury was in a position to draw its own conclusions about whether they depicted actual **[*24]** children. Deaton, 328 F.3d at 455 (jury's conclusion that real children were depicted may be upheld even when the only evidence offered was the images themselves); see also United States v. Vig, 167 F.3d 443, 449-50 (8th Cir. 1999) (where defendant simply argues that images may or may not be of real children, the government is not required to negate as part of its proofs the unsupported speculation). n10

U.S. v. Wolk, (8th Cir. July 30, 2003):

The government convicted the defendant of possession of child pornography. The indictment included the prohibited language regarding virtual images. The court sustained the conviction based on the following reasons:

“We come to this conclusion "because (1) the evidence established that the children depicted in the pictures introduced at trial were actual children[,] (2) no one ever claimed, or even hinted, that the images were of virtual children," and (3) Wolk stipulated that these were actual children. United States v. Hall, 312 F.3d 1250, 1260 (11th Cir. 2002).

First, the evidence establishes that the children in the pictures at issue were real. The photos introduced for Count I (Transportation of Child Pornography) were described by the undercover agent in human terms-"boys with erections"; "brother and a sister enjoying

each other"; "girls engaging in sex acts." Trans. of Voir Dire & Tr. at 160, 170, 180 (Sept. 17, 2001). Likewise, FBI Special Agent Jerry Bell testified that the photos introduced for Counts II, III, and IV (Possession of Child Pornography) were images of child pornography, which he defined as "children under [eighteen] engaged in sex acts or sexually explicit activity." Tr. Trans. at 61-62 (Sept. 18, 2001).

Moreover, these pictures are in the record. We have examined them. Upon review, we conclude the children depicted [*14] in these images were real. See United States v. Richardson, 304 F.3d 1061, 1064 (11th Cir. 2002) (performing a plain error analysis and concluding the same); see also Hall, 312 F.3d at 1260 (same); United States v. Pearl, 324 F.3d 1210, 1219 & n.4 (10th Cir. 2003) (Briscoe, J., dissenting) (same).

Second, there was no testimony or evidence presented at trial that the pictures were virtual images. While not evidence in the case, the opening statements of both counsel are illustrative. In the Government's opening statement, the Assistant United States Attorney stated, "Let me be clear here. I am not talking about art. I'm talking about children engaged in sex acts. That's what this child pornography is." Trans. of Voir Dire & Tr. at 96-97 (Sept. 17, 2001). Wolk's counsel stated likewise, "Now what I also want to make clear is we're not disputing that the pictures that they're going to show you are child pornography. Evidence is going to show that [the pictures are] child pornography. We're not standing here defending those disgusting pictures." Id. at 101-02. Wolk's counsel also stipulated to the court the same. Tr. of Testimony [*15] of Alois Larry Wolk Direct Examination Vol. 3 at 21-2 (Sept. 19, 2001). These comments are consistent with Wolk's defense-that he did not knowingly possess or transport the child pornography images.

Finally, Wolk admitted numerous times that the images were child pornography and that there were actual minors in the pictures. He first admitted this during his initial questioning when he told Bell that he had child pornography on his computer. Another officer then advised Wolk that "child pornography involved children engaged in sexual activity, photos of children engaged in sexual activity." Wolk agreed that he had photographs which met the described definition. Tr. of Testimony of Alois Larry Wolk Direct Examination Vol. 1 at 39-40 (Sept. 19, 2001).

Later at trial Wolk testified that the images from the three computer CDs that were introduced into evidence were child

pornography. Tr. of Testimony of Alois Larry Wolk Direct Examination Vol. 3 at 22 (Sept. 19, 2001). He also admitted that it is harmful to possess and trade child pornography because "it's harmful to our society, to the people doing it, to the children." Id. at 44. (emphasis added).

We thus conclude that although [*16] plain error exists in the indictment, Wolk was not prejudiced. His indictment did contain two portions of the definition of child pornography that were later found to be unconstitutional. However, this error did not prejudicially influence Wolk's trial because the pictures he transported and possessed were of real children. n4 As a result, Wolk's constitutional challenge fails."

U.S. v. Kimler, (10th Cir. July 7, 2003):

"We conclude that Free Speech Coalition, did not establish a broad, categorical requirement that, in every case on the subject, absent direct evidence of identity, an expert must testify that the unlawful image is of a real child. Juries are still capable of distinguishing between real and virtual images; and admissibility remains within the province of the sound discretion of the trial judge. The only two circuits to have considered the issue take the same position. United States v. Deaton, 328 F.3d 454, 455 (8th Cir. 2003) (per curiam) (citing United States v. Vig, 167 F.3d 443, 449-50 (8th Cir. 1999)); United States v. Hall, 312 F.3d 1250, 1260 (11th Cir.), cert. denied, 155 L. Ed. 2d 502, 123 S. Ct. 1646 (2002)…

The record does contain the few trial exhibits which the government made available to the court at sentencing in support of the adjustment in question. n12 We have examined those exhibits and have no doubt that some of the images depict children who were so obviously prepubescent that expert testimony would not have been necessary or helpful to the court. The images themselves provided sufficient evidence of prepubescence to support the sentence enhancement."

U.S. v. Deaton, 328 F.3d 454 (8th Cir. 2003):

"Further, we have previously upheld a jury's conclusion that real children were depicted even where the images themselves were the only evidence the government presented on the subject. See United States v. Vig, 167 F.3d 443, 449-50 (8th Cir.) HN2(government, as part of affirmative case, was not required to negate unsupported speculation that images may have been computer-generated or

other than what they appeared to be), cert. denied, 528 U.S. 859 (1999).”

“The pictures themselves support the district [**5] court's determination that the images were plainly of children under age 12, and depicted actual children. See Vig, 167 F.3d at 449-50.”

U.S. v. Ellyson, 326 F.3d 522 (4th Cir. 2003):

This case represents the few that actually go against the government in the post-Ashcroft era. The government witnesses testified that it was possible that the images could be virtual and the jury was erroneously instructed on the “virtual” instruction. Since there was no way of knowing if the jury found the children to be real, the verdict was reversed.

Under § 2256(8)(C), the definition of child pornography also includes images produced by "morphing," a "lower tech means of creating virtual images" whereby a "pornographer can alter innocent pictures of real children so that the children appear to be engaged in sexual activity." Free Speech Coalition, 122 S. Ct. at 1397. Although not presented with the question of whether such morphed images can be constitutionally banned, the Court noted that, unlike virtual images, morphed images "implicate the interests of real children." I

U.S. v. Richardson, 304 F.3d 1061 (11th Cir. 2002):

“We reach this conclusion because the evidence clearly established that the children depicted in the images or pictures were actual children. Special Agent Sheehan of the Innocent Images Task Force, a federal task force investigating [**8] child exploitation on the Internet, testified that, based on his training and extensive experience as a member of the task force, the images depicted actual children, not what simply appeared to be children. We have examined the images shown to the jury. The children depicted in those images were real; n2 Of that we have no doubt whatsoever. Appellant's third point accordingly fails. We turn then to appellant's first two points, which address the district court's denial of the motions to suppress.”

Bender v. U.S, 290 F.3d 1279 (11th Cir. 2002):

“At trial, Dr. Dory Solomon ("Dr. Solomon"), Assistant Professor of Pediatrics at the University of Miami School of Medicine, testified [**4] as an expert witness in the area of pediatrics, particularly in the determination of children's ages. Dr. Solomon

examined 16 pictures found on the hard drive of the Packard Bell computer that agents had seized at Bender's residence. The record shows that, with one possible exception, each of these pictures portrayed at least one female child engaged in sexually explicit conduct. The record also shows that seven of the female children and one male child appeared to be prepubescent or under the age of 12. One of the pictures portrayed an adult male penis penetrating a preadolescent female's vagina. Dr. Solomon stated that this female appeared to be 10 years old. Dr. Solomon noted that the photographs generally portrayed naked children, some orally or digitally stimulating the genitalia of adult males, some digitally stimulating their own genitalia, and some displaying their own genitalia. Dr. Solomon testified that the photographs appeared to portray real children. n2

…

In Ashcroft v. Free Speech Coalition, 2002 U.S. LEXIS 2789, 122 S. Ct. 1389, (U.S. April 16, 2002) (No. 00-795), the United States Supreme Court held that the prohibitions of 18 U.S.C. §§ 2256(8)(B) and 2256(8)(D) are overbroad and unconstitutional. These provisions are not at issue in the present case. Moreover, because there is sufficient evidence that the images portray real children, we conclude that Free Speech Coalition is not pertinent to the issues we must decide."

U.S. v. Vig, 167 F.3d 443 (8th Cir. 1999):

"Donovan Vig also claims that the district court erred in denying his motion [**17] for judgment of acquittal because the government did not present sufficient evidence showing that the subjects of the visual depictions were real minors as required under the statute. See 18 U.S.C. § 2252(a)(4)(B)(i) & (ii). n10 HN7In reviewing the sufficiency of the evidence, we consider it in the light most favorable to the jury verdict and accept all reasonable inferences from the evidence which tend to support the jury verdict. See United States v. Broyles, 37 F.3d 1314, 1317 (8th Cir. 1994). Vig's specific argument is that modern technology can create images so similar to a human being that it would be difficult to decipher what they are by just looking at them. Technology, he speculates, might create computer-generated images that look exactly like real children. He concludes that because the only evidence the government presented to show that the images were of real children were the images themselves, n11 the government failed to meet its burden of proof. We disagree.

- - - - - - - - - - - - - - Footnotes - - - - - - - - - - - - - -

n10 For purposes of this section, "minor" is defined as "any person under the age of eighteen years." 18 U.S.C. § 2256(1). [**18]

n11 At trial, the government presented evidence of the images contained in the computer files through paper copies of what would appear on a computer screen if one were to view the files using a computer or to print the contents of the files using a printer.
- - - - - - - - - - - - End Footnotes- - - - - - - - - - - - - -
The images were viewed by the jury which was in a position to draw its own independent conclusion as to whether real children were depicted. See id. at 1318 (finding sufficient evidence that subjects of video were in fact under the age of eighteen when, among other things, videotape was viewed by jury which could draw its own conclusions as to age of subjects). Furthermore, the jury was aided in its observations by Dr. Rich Kaplan, an associate professor of pediatrics with a specialty in child maltreatment. Dr. Kaplan testified that at least one of the subjects from the image or images found in each of the thirteen files charged against Vig, except one, was a minor.

[*450] Vig, nevertheless, argues that although Dr. Kaplan may have testified that the subjects were minors, he failed to testify that they were real minors and not computer-generated [**19] images. We note, however, that the defense failed to cross-examine or in any way rebut the testimony elicited from Dr. Kaplan. Vig produced no expert evidence at trial to show that the images were computer generated or other than what they appeared to be. In essence, Vig's claim that the images may not have been of real children is purely speculative and we do not think that the government, as part of its affirmative case, was required to negate what is merely unsupported speculation. See United States v. Nolan, 818 F.2d 1015, 1020 (1st Cir. 1987) (stating that uncorroborated speculation that some undefined technology exists to produce pornographic pictures without use of real children is not sufficient basis for rejecting lower court's determination to admit evidence). Proof beyond a reasonable doubt does not require the government to produce evidence which rules out every conceivable way the pictures could have been made without using real children. See id. We think that the government presented sufficient evidence from which a jury could reasonably infer that the subjects of the visual depictions were actual minors engaging in sexually explicit conduct."

United States v. Reardon, (CD Calif. Nov. 6, 2003)

The government offered the testimony of David Mark Verrier Jones, an employee of a visual effects studio, whom the court accepted as an expert in the creation of visual effects based on his training and experience in the film industry. Jones testified that in

his opinion, the images transmitted by Rearden had not been manipulated in any manner. He indicated that they had not been composited (which involves the altering of images by, for example, transferring the head of one person to the body of another) or morphed (which in Jones's view involves the creation of an intermediate image from two other images). Jones stated that it was beyond the limits of modern computer graphics to create a completely artificial picture of a believable photo-realistic human being (except, perhaps, of people who are very small in the background). Rearden put on no evidence to the contrary…He examined the images and opined that they were not manipulated, that any attempted creation of a digital photo realistic human being would be readily apparent, and that these images were entirely consistent as photographs. Based on this testimony the trier of fact could reasonably conclude that the government had carried its burden of proving that the images depicted actual children.

Finally, Rearden submits that the evidence was also insufficient because the government failed to prove the ages of the individuals depicted by adducing testimony from a medical expert. However, Rearden admitted on the stand that he knew at least one of the images he sent was of "somebody under 18," and it is obvious from the pictures themselves that they are of children. Expert testimony was not, therefore, necessary in this case to assist the court.

Lewd Exhibition of the genitals (see Probable Cause chapter for more cases)

U.S. v. Larkin, --- F.3d ----, 2010 WL 5022471 C.A.3 (Pa.),2010.

Photographs of defendant's five-year-old daughter depicting her fully nude body were “sexually explicit” within meaning of statute criminalizing production of child pornography; photograph depicting daughter standing in empty bathtub with her head resting on her shoulder was sexually suggestive, photograph depicting daughter's nude body at close range was not of type traditionally taken by parents eager to preserve memories of their children, and photographs were sent over internet to interested pedophile whom defendant acknowledged would find them sexually stimulating.

U.S. v. Rivera, 546 F.3d 245 (2d Cir. 2008)

Sufficient evidence established that photographs possessed by defendant depicted lascivious exhibition of minor's genitals, as required to support defendant's conviction of illegally enticing

minor to engage in sexually explicit conduct for purpose of producing visual depiction; images showed minor lying naked on hotel room bed with his genitals prominent at or about center of frame, in one photo minor was lying on his chest with his upper body raised on elbows while looking over shoulder at camera, and in another photo minor was lying on his back with the right side of his body resting on his right elbow.

U.S. v. Frabizio, 459 F.3d 80 (1st Cir. 2006):

On defendant's motion to exclude allegedly pornographic photos, a reasonable jury could find the images to be a lascivious display of the genitals or pubic area, as required to meet the statutory requirement of federal child pornography law, and were thus admissible; each of the three photographs depicted a nude girl, who was posed alone and who was looking directly at the camera, each girl appeared on the cusp of puberty, either prepubescent or adolescent, and, each of the girls' legs were parted and the pubic area was plainly visible.

Kimmerling v. United States, * (8th Cir. 2002)

"A factfinder could decide, moreover, without being clearly wrong, that the other pictures are lascivious because they are of children who are nude or partially clothed, the focus of the images is the child's genitals or pubic area, and their purpose appears to be to elicit a sexual response from the viewer. These images were not designed, for instance, simply to provide a clinical view of the portions of the children's anatomy that are pictured. We therefore discern no clear error in the district court's findings of fact."

United States v. Getzel, (N.D. NH 2002)

Facts: German authorities notified U.S. Customs that an America Online customer was posting child pornography to a newsgroup. The German police provided Customs with a CD with the child pornography images on it. Based upon this information and subscriber information, a search warrant was obtained to search the defendant's computer. The defendant argued that there was insufficient probable cause for the warrant because the affiant did not adequately describe the images that constituted probable cause. The descriptions provided in the warrant are as follows:

Agent Lundt describes the following images: (1) "file named Subject pi51(1).jpg. This jpg image depicts a naked prepubescent child male child

[sic], kneeling in profile to the camera with an erect penis."; and (2) "file named Jared39.jpg. This image depicts a naked minor male reclined on a bed with his legs spread and fondling his penis." (Lundt Aff. at P17.) Agent Lundt states that four other images found on the CD-Rom depict the same minor male in Jared39.jpg interacting with a naked adult male. In his affidavit Agent Lundt describes these four images as follows:

a. Jared 06.jpg depicts the adult male performing oral sex on the same minor child as depicted in Jared39.jpg.
b. Jared07.jpg depicts the same minor child depicted in Jared39.jpg with his face on the genitals of the adult male.
c. Jared25.jpg depicts the same minor child depicted in Jared39.jpg performing oral sex on the adult male.
d. Jared38.jpg depicts the same minor child depicted in Jared39.jpg in genital to genital contact with the nude male adult.

Agent Lundt did not attach the above described images to his affidavit.

However, Agent Lundt did attach an image of Getzel from his New Hampshire driver's license, together with image 17.JPG [sic], which Agent Lundt affirms depicts the same minor male and adult depicted in the CD-Rom images described above. n2 The image 17.JPG depicts a naked pre-pubescent male lying down next to a naked adult male on what appears to be a bed against a wall. Both are on their backs. The genitalia of both the boy and the adult are fully visible. The adult's head and left shoulder appear to be propped against the wall. The adult has his right arm around the boy's shoulders, and the boy's head appears cradled in the right arm of the adult. The adult's head and the boy's head are leaning in towards each other and are touching. The adult's body is angled towards the boy, and his right leg is bent somewhat, covering a portion of the boy's left leg.

Holding:

- A bare legal assertion, absent any descriptive support and without an independent review of the images, is insufficient to sustain a finding of probable cause.

- A warrant is issued without probable cause where affiant does not give detailed factual description of images and magistrate does not independently review the images.

- Because the identification of images as lascivious is a subjective determination, that assessment should be made by a judge, not an agent.

- A judge cannot ordinarily make this determination without either a look at the allegedly pornographic images, or at least an assessment based on a detailed, factual description of them.

- In analyzing the single image attached to the affidavit that did not involve any overt sexual activity, the court used the following reasoning to find that it constituted a lewd exhibition of the genitals.

    - In 17.JPG, the image is taken from a horizontal vantage point near the subjects' feet and presents their genitalia at the forefront of the image. The boy is depicted in an unnatural pose, considering his age. The way the adult has his arm around the boy, while both lie naked with their genitalia exposed, is not a natural pose for a minor male, and the boy in the image looks stiff and uncomfortable. The overall positioning of the boy and the adult, naked, with their genitalia prominently displayed, on what appears to be a bed, engaged in an intimate embrace, suggests a sexual atmosphere. Taking into account the Dost factors, the court concludes that the image is intended to elicit a sexual response from the viewer. The court finds that image 17.JPG constitutes a lascivious exhibition of the genitals under § 2256(2)(E).

- In analyzing the image described as a "naked prepubescent male child, kneeling in profile to the camera with an erect penis," the court noted "Although kneeling in profile is not per se an unnatural pose, the court is hard-pressed to imagine an instance where it would be natural for a naked boy to pose in profile with an erection…the erection is highly suggestive of sexuality.

- The other descriptions specifically describe children engaged in sexual conduct and thus, constitute probable cause.

United States v. Brunette, 256 F.3d 14 (1st Cir. 2001):

Facts: Agent Richard Jereski, who had some 18 months of experience investigating child pornography crimes, viewed those 33 images and concluded that they were pornographic. Jereski applied for a warrant to search defendant's home, but he did not append any of the allegedly pornographic images to the warrant application. Nor did his affidavit contain a description of them; instead, he merely asserted that they met the statutory definition of child pornography. After the magistrate judge determined that there was probable cause, the warrant was issued, the defendant's home was searched, and his computers were seized. Other allegedly pornographic images of children were found on those computers.

Holding:

- Bare legal assertions in an affidavit in a child pornography case, absent any descriptive support and without an independent review of the images, is insufficient to sustain the magistrate judge's determination of probable cause.

- The inquiry to determine whether a photograph is a pornographic image is: does a given image fall within the statutory definition of child pornography? Only if there is probable cause to believe so may a search warrant issue. A judge cannot ordinarily make this determination without either a look at the allegedly pornographic images, or at least an assessment based on a detailed, factual description of them. An appellate court's de novo standard of review anticipates that judicial officers at each stage of the process

will consider whether the images at issue are pornographic within the meaning of the statute.

- The six factors used for evaluating whether a photograph depicts a lascivious exhibition of genitals are: (1) whether the genitals or pubic area are the focal point of the image; (2) whether the setting of the image is sexually suggestive, a location generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose or inappropriate attire considering her age; (4) whether the child is fully or partially clothed, or nude; (5) whether the image suggests sexual coyness or willingness to engage in sexual activity; and (6) whether the image is intended or designed to elicit a sexual response in the viewer.

- The identification of images that are lascivious will almost always involve, to some degree, a subjective and conclusory determination on the part of the viewer. That inherent subjectivity is precisely why the determination should be made by a judge, not an agent. The Fourth Amendment requires no less.

United States v. Amirault, 173 F.3d 50 (1st Cir. 2001):

Facts: When the police seized the materials that formed the basis for Amirault's guilty plea, they also seized from Amirault's possessions a photograph of a young naked female, probably a teenager, standing or kneeling in a hole on a beach.

Holding:

- Factors in assessing whether a photograph involves lascivious exhibition of the genitals or pubic area for purposes of 18 U.S.C.S. § 2256(2)(E) include: (1) whether the genitals or pubic area are the focal point of the image; (2) whether the setting of the image is sexually suggestive (i.e., a location generally associated with sexual activity); (3) whether the child is depicted in an unnatural pose or inappropriate attire considering her age; (4) whether the child is fully or partially clothed, or nude; (5) whether the image suggests sexual coyness or willingness to engage in sexual activity; and (6) whether the image is intended or designed to elicit a sexual response in the viewer. These factors are not exhaustive: other factors may be relevant, depending upon the particular circumstances involved. The

factors are neither comprehensive nor necessarily applicable in every situation.

- Using the Dost factors as guideposts, we turn now to the photograph to analyze whether it contains a lascivious exhibition of the genitals. We hold that it does not.

  To begin with, we do not believe that the photograph is significantly focused upon the genitalia. The girl is standing face forward, in a hole in the sand, with her feet below the ground. Her pubic area, which is visible immediately above the opening of the hole, appears in the bottom fourth of the photograph. Although the girl's pubic area is on clear display, there is no close-up view of the groin, and the genitals are not featured in the center of the composition. Moreover, unlike Wolf, 890 F.2d at 243, the girl's legs are not widespread and the lighting of the photograph is not primarily directed at the genital region.

  Nor is the photograph's setting sexually suggestive. The beach setting is a natural landscape that, unlike a bedroom or boudoir, does not evoke associations of sexual activity. The government's assertion that "many honeymoons are planned around beach locations" fails to persuade us otherwise.

  Furthermore, the child is not depicted in an unnatural pose. She is merely standing, face forward and with legs more together than apart, in a large hole in the sand. Cf. Dost, 636 F. Supp. at 833 (finding significant the fact that the "average 10-year-old child sitting on the beach" does not sit with her right leg fully extended at an outward angle and her left leg extended almost perpendicularly from the body). Her arms are slightly raised, as if she were about to pat down the sand surrounding the hole. The pose is not one that is typically associated with sexual activity.

- It is a mistake to look at the actual effect of the photograph on the viewer, rather than upon the intended effect, in determining whether a photograph is sexually explicit under 18 U.S.C.S. § 2256(2).

- In determining whether there is an intent to elicit a sexual response, the focus should be on the objective criteria of a photograph's design.

United States v. Dost, 636 F.Supp. 828 (S.D. Cal. 1986):

Facts: Defendants took 22 photographs, 21 of a 14-year old girl and 1 of a 10-year old girl. In the photographs, the girls were nude and obviously posed in unnatural positions. The stipulated facts established that defendants conspired, used minors as subjects of visual depictions knowing that the visual depictions would be mailed, and knowingly received visual depictions through the mail.

Holding:

- Child pornography is outside the protection of the First Amendment, regardless of whether it is "obscene" under the standard enunciated in prior caselaw. The purpose behind enactment of the various protective laws known commonly as the "kiddie porn" laws is to protect children from the harmful effects of this type of sexual exploitation: a 12-year-old child photographed while masturbating surely suffers the same psychological harm whether the community labels the photograph "edifying" or "tasteless." The audience's appreciation of the depiction is simply irrelevant to the state's asserted interest in protecting children from psychological, emotional, and mental harm.

- In determining whether a visual depiction of a minor constitutes a "lascivious exhibition of the genitals or pubic area" under 18 U.S.C.S. § 2255(2)(E), the trier of fact should look to the following factors, among any others that may be relevant in the particular case: 1) whether the focal point of the visual depiction is on the child's genitalia or pubic area;2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity;3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;4) whether the child is fully or partially clothed, or nude;5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer. Of course, a visual depiction need not involve all of these factors to be a "lascivious exhibition of the genitals or pubic area." The determination will have to be made based on the overall content of the visual depiction, taking into account the age of the minor.

- In determining whether photographs contain lascivious exhibitions of the genitals, it is acknowledged that Congress intended that the standard be lower than that for obscenity.

Special verdict forms regarding which photos jury found to be child pornography

United States v. Nelson, * (9th Cir. 2002)

- Jurors are not normally required to say what evidence they credited to reach a verdict.

- Only one image of child pornography was necessary to support the jury's verdict. Nothing in common law or common courtroom practice required the court to insist that the jury say which particular picture of pictures they found to be child pornography.

Possession of child pornography in deleted files

People v. Kent, 2012 WL 1580439 (N.Y.), 2012 N.Y. Slip Op. 03572

Evidence regarding child pornography video and images of child pornography found in the unallocated space of defendant's computer was sufficient to support convictions for promotion and possession of child pornography; evidence that at some point defendant downloaded and/or saved the video and the images, thereby committing them to the allocated space of his computer, prior to deleting them supported conclusion that defendant acquired the video and exercised control over it and the images, and his pattern of browsing for child pornography sites and deleting illegal images and retaining legal ones established he acted knowingly.

U.S. v. Flyer, 2011 WL 383967 (C.A.9 (Ariz.))

Evidence of child pornography images located in "unallocated space" on defendant's computer was insufficient to show defendant "possessed" such images, as required to support conviction of possession of child pornography, absent evidence that defendant knew of the presence of the files or that he had the forensic software required to see or access the files.

Discussion: In this case, the government charged him with

knowing possession on the date the computer was seized. The opinion did not address whether the conviction would have been proper if the government had charged a date range consistent with the age of the hard drive.

U.S. v. Kain, 589 F.3d 945 (8th Cir. 2009)

"The presence of Trojan viruses and the location of child pornography in inaccessible internet and orphan files can raise serious issues of inadvertent or unknowing possession. See United States v. Romm, 455 F.3d 990, 998-1001 (9th Cir.2006); United States v. Shiver, 305 Fed.Appx. 640, 642-43 & n. 4 (11th Cir.2008); Howard, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, 19 Berkeley Tech. L.J. 1227 (2004). But these are issues of fact, not of law. "[A]ctual or *950 constructive possession is a finding of fact we review for clear error." United States v. Denis, 560 F.3d 872, 873 (8th Cir.2009). The presence of child pornography in temporary internet and orphan files on a computer's hard drive is evidence of prior possession of that pornography, though of course it is not conclusive evidence of knowing possession and control of the images, just as mere presence in a car from which the police recover contraband does not, without more, establish actual or construction possession of the contraband by a passenger. See United States v. Payne, 377 F.3d 811, 815 (8th Cir.2004)."

U.S. v. Simpson, 152 F.3d 1241 (10th Cir. 1998):

The evidence was sufficient to convict a defendant of receiving child pornography, even though the files claimed to have been downloaded by the defendant had been deleted from the defendant's computer files; the names of the files found in the defendant's computer were substantially similar to the names of the downloaded files, and there was expert evidence that computer users frequently delete downloaded files when they are found to contain the same information as existing files.

U.S. v. Lacy, 119 F.3d 742 (9th Cir. 1997):

"If his claim were true, he knew the depictions he downloaded onto his disks and drive were of minors engaged in sexually explicit conduct, but he did not know the depictions were still on his disks and drive. To address this defense, the trial court had to instruct the jury that to convict Lacy it must find that he knew the depictions were on his disks and drive. Because the instructions

allowed the jury to convict Lacy without finding that he knew the hard drive and disks contained the unlawful visual depictions, they were erroneous."

Possession of child pornography by looking at it on screen

State v. Mercer, 782 N.W. 125 (Wis. App. 2010):

> Finding that defendant knowingly possessed child pornography was supported by sufficient evidence, including evidence that defendant had habit of surfing the Internet for child pornography, that on the day in question he clicked to look at a magazine and its images of child pornography and then looked at others magazines and their child pornography images, that he controlled how long an image was displayed on his computer screen and had the ability to and knew how to print, save, or copy it, and that he deleted the files where forensic examiners would have found the child pornography stored in his hard drive.
>
> An individual "knowingly possesses" child pornography when he or she affirmatively pulls up images of child pornography on the Internet and views those images knowing that they contain child pornography, even if there is no evidence that the images were in the computer hard drive

Possession of child pornography in cache files

United States v. Moberg, 888 F.3d 966 (C.A.8 (Mo.), 2018)

> Evidence was sufficient to support jury's determination that defendant knowingly possessed child pornography on his home computer; six thumbnail images depicting child pornography that were found in the thumbnail database cache area of defendant's computer during a forensic examination were admitted at trial, government presented evidence that, in order for the thumbnail images to be present in the thumbnail database cache, a computer user had to purposely save or download a file onto the computer's hard drive, two of the thumbnail images were from a known series of child pornography, and defendant admitted he was familiar with this series.

U.S. v. Rogers, 714 F.3d 82 (1st Cir. 2013)

> Sufficient evidence established that child pornography found on defendant's laptop was downloaded knowingly and deliberately, as

required to support conviction for possession of child pornography; web browser cookies and indexed history found on defendant's laptop computer indicated that someone had used browser to make numerous visits to websites related to, or within names indicative of, child pornography, including "nymphets-first-time-sex.com," "Natural Lolitas," and "innocent-girl.com," discovery of child pornography in temporary internet files folder suggested that those images were downloaded when user visited websites hosting them, and forensic analysis of laptop all but ruled out possibility that images had been downloaded by virus without user's knowledge.

People v. Kent, 2012 WL 1580439 (N.Y.), 2012 N.Y. Slip Op. 03572

Merely accessing and displaying Web images of child pornography does not constitute possession or procurement of child pornography.

Where no evidence shows defendant was aware of the presence of cached temporary Internet files on his computer, such files cannot underlie a prosecution for promotion or possession of child pornography; this is necessarily so because a defendant cannot knowingly acquire or possess that which he or she does not know exists.

Cached images of child pornography stored on defendant's computer can serve as evidence of defendant's prior viewing of images that were, at one time, resident on his computer screen; such evidence, like a pattern of browsing for child pornography, is relevant to the mens rea of both promotion or possession of child pornography by showing that a defendant did not inadvertently access an illicit image or site or was not mistaken as to its content.

Purposefully making child pornography appear on the computer screen—for however long the defendant elects to view the image—does not itself constitute knowing control under statutes barring promotion or possession of child pornography; rather, some affirmative act is required, such as printing, saving, downloading, etc., to show that defendant in fact exercised dominion and control over the images that were on his screen.

Evidence regarding child pornography video and images of child pornography found in the unallocated space of defendant's computer was sufficient to support convictions for promotion and possession of child pornography; evidence that at some point defendant downloaded and/or saved the video and the images, thereby committing them to the allocated space of his computer,

prior to deleting them supported conclusion that defendant acquired the video and exercised control over it and the images, and his pattern of browsing for child pornography sites and deleting illegal images and retaining legal ones established he acted knowingly.

U.S. v. Winkler, 2011 WL 1535237 (C.A.5 (Tex.)

Evidence was sufficient to support jury's determination that defendant knowingly received two video files depicting minor females engaging in sexual activity with adult males, thereby supporting conviction for knowing receipt of child pornography; government elicited evidence from which the jury could infer that the files at issue came from a members-only section of a child pornography site, evidence indicated that defendant repeatedly paid for members-only child pornography sites, evidence indicated that the only way those files could have been copied to the cache was by defendant's decision to click and watch the videos, and jury also heard testimony that defendant had downloaded dozens of images of child pornography and that the files he received from those sites were often hidden behind password walls in his own user account or in unnatural locations in the computer's file hierarchy.

U.S. v. Dobbs: --- F.3d ----, 2011 WL 14459 (C.A.10 (Okla.))

Government offered insufficient evidence to prove that defendant's receipt of two images of child pornography was knowing, precluding his conviction for receiving child pornography; the two images were stored in cache of defendant's computer, there was no evidence that defendant had accessed the files stored in his computer's cache, there was no evidence that defendant even knew about his computer's automatic-caching function, there was no evidence that defendant saw the images, much less exercised control over them by clicking on them or enlarging them, and evidence that defendant engaged in child-pornography-related searches immediately preceding the creation of illegal images in the cache did not apply to the two images submitted to jury.

Government offered insufficient evidence to prove that defendant took a substantial step toward receiving two images of child pornography, precluding his conviction for attempting to receive child pornography; the pattern of child-pornography-related searches immediately preceding the creation of illegal images in cache of defendant's computer did not apply to two images submitted to jury, there was no evidence of suggestive searches immediately prior to creation of two images at issue, and there was no indication that defendant visited suspect websites before the

images arrived in his computer's cache.

U.S. v. Kain, 589 F.3d 945 (8th Cir. 2009)

The presence of child pornography in temporary internet and orphan files on a defendant's computer hard drive is evidence of prior possession of that pornography, but it is not conclusive evidence of knowing possession and control of the images, as required to support conviction for knowing possession of child pornography, just as mere presence in a car from which the police recover contraband does not, without more, establish actual or construction possession of the contraband by a passenger.

Evidence was sufficient to support finding that defendant knowingly possessed the images of child pornography found on his computer, as required to support conviction for knowing possession of child pornography; detective testified that he conducted forensic examination of copy of computer's hard drive in which he found 21 images of suspected child pornography in a desktop icon folder and six other images in the computer's temporary Internet and orphan files, he also testified that the images were not placed in the hard drive by a "Trojan" virus, and defendant admitted he owned the computer and had used it to download 40 to 50 images of child pornography to the file folder.

Ward v. State, So.2d (Alabama 2007)

Defendant admitted to visiting child pornography websites on a university computer, and a forensic examination revealed 288 images of child pornography in the computers "temporary internet files". Because the defendant "reached out" for child pornography, had the ability to copy, print, e-mail, or send the images, and had child pornography on his home computer as well, he was found to be in constructive possession of the images on the university computer. He was properly convicted of possession of child pornography under Alabama's statutory scheme.

Discussion: This case is a good research tool. It reviewed several state and federal cases that have addressed this issue.

Commonwealth v. Diodoro (Pa. Super. Ct. 2006):

Evidence was insufficient to support convictions for knowing possession of child pornography; although pornographic images from websites viewed by defendant were automatically saved to internet cache file on computer's hard drive, there was no evidence

that defendant knew that images were saved, and merely viewing child pornography on internet without intentionally saving or downloading any of the images did not constitute "knowing possession" of child pornography.

U.S. v. Kuchinski, (9th Cir. 2006)

For purposes of sentencing, defendant did not knowingly receive and possess child pornography images found in his computer's cache files, which were automatically downloaded when he accessed web pages, so that when site was revisited the information would come up more quickly than it would have if it had not been stored on computer's hard drive, absent evidence that defendant was sophisticated computer user, that he tried to get access to cache files, or that he even knew of existence of cache files.

Where a defendant lacks knowledge about his or her computer's cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him, for purposes of sentencing, with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images.

U.S. v. Romm, (9th Cir. July 23, 2006)

Defendant had exercised dominion and control over images in his Internet cache files in his laptop computer, for purpose of possessing and receiving child pornography, by enlarging them on his screen and saving them there for five minutes before deleting them; while images were displayed on defendant's computer screen and simultaneously stored to his laptop's hard drive, he had ability to copy, print, or email images to other persons.

In the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it.

Jury rationally could have concluded beyond reasonable doubt that defendant knowingly possessed child pornography, on basis that defendant accessed child pornography from Internet and his computer automatically and contemporaneously stored those images to Internet cache files, on evidence that defendant repeatedly sought out child pornography over Internet, defendant knew that images of child pornography had been saved to his computer disk, defendant had enlarged several thumbnail images

of child pornography for better viewing, and defendant could have printed images, enlarged them, copied them, or emailed them to other persons while viewing them.

Knowingly taking possession of files in Internet cache of laptop computer constituted knowing receipt of those files, for purpose of defendant's conviction for receiving child pornography; although computer automatically and contemporaneously stored images to Internet cache files, it did so as defendant accessed and viewed child pornography from Internet.

U.S. v. Martin, 426 F.3d 68 (2d Cir. 2005)

"Instead, he maintains that "viewing" child pornography on the internet is legal, but this is an open question. *See, e.g.*, *United States v. Tucker*, 305 F.3d 1193, 1205 (10th Cir.2002) (finding defendant knowingly possessed child pornography, where it was saved in his computer's cache); *United States v. Perez*, 247 F.Supp.2d 459, 484 n. 12 (S.D.N.Y.2003) (noting that question of whether 18 U.S.C. § 2252A(a)(5)(B) reaches "mere internet 'browsing' is something of an open question"). *See generally* Ty E. Howard, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, 19 Berkeley Tech. L.J. 1227 (2004). There is no need to decide this question, however. Even if viewing were legal, that would not defeat probable cause because it is common sense that, in the context of this website and the corrected affidavit, those who view are likely to download and store child pornography. The concern that a person who innocently joins an organization with a mixed purpose might be subjected to an unnecessary and unconstitutional search is not present here because the girls12-16 e-group and its technological features served primarily as a *means* for effecting illegal activity. At its core, the modus operandi of the girls12-16 website was criminal, and that is determinative in this case."

United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002)

Evidence was sufficient to support finding that defendant knowingly possessed child pornography, even though defendant only viewed images on his Web browser and did not save or download the images to his hard drive; defendant continued to view child pornography even though he was aware that images were automatically stored in cache files, over which he had control.

Discussion: This is a unique case in that the defendant admitted

that he was aware that his browser automatically saved the images he viewed in his “temporary Internet” or “cache” files. He did not intentionally configure the browser to do so, but he knew it existed. The court specifically refused to address the issue as to whether the mere viewing of images on a screen constitutes possession or as to whether the presence of images in the cache constitute possession even if you do not know they are there.

United States v. Perez, 247 F. Supp. 2d 459, 484 (U.S. Dist. , 2003)

> The statute does not criminalize "viewing" the images, and there remains the issue of whether images viewed on the internet and automatically stored in a browser's temporary file cache are knowingly "possessed" or "received." The question, as the court in United States v. Zimmerman, 277 F.3d 426, 435 (3d Cir. 2002), put it while examining probable cause, is that without evidence that pornography was specifically downloaded and saved to a defendant's computer, the offending images "may well have been located in cyberspace, not in [the defendant's] home." In United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002), the court upheld a conviction for possession of files automatically stored in a browser cache because the defendant's "habit of manually deleting images from the cache files established that he exercised control over them." Id. at 1198. The court clarified, however, that it offered "no opinion on whether the mere viewing of child pornography on the Internet, absent caching or otherwise saving the image, would meet the statutory definition of possession" nor whether "an individual could be found guilty of knowingly possessing child pornography if he viewed such images over the Internet but was ignorant of the fact that his Web browser cached such images." Id.; see United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (noting that the district court (Judge Perry) acquitted the defendant on one count and "explained that one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image").

Commonwealth v. Diodorio, (PA 2006)

> We hold that absent specific statutory language prohibiting the mere viewing of pornographic images or evidence that the defendant knowingly downloaded or saved pornographic images to his hard drive or knew that the web browser cached the images, he cannot be not criminally liable for viewing images on his computer screen. Therefore, we conclude that the evidence was insufficient

to sustain Diodoro's conviction for knowing possession of child pornography under section 6312(d).

File Server

U.S. v. Sebolt, 460 F.3d 910 (7th Cir. 2006):

Evidence was sufficient to support conviction for knowingly transporting and shipping child pornography in interstate commerce by means of a computer; evidence showed that defendant's computer generated a message that pornographic image was "on its way," and special agent testified that for every one of the 53 images he obtained from defendant's file server, he previously received a message that the file was "on its way."

Knowing Possession

United States v. Carroll, 886 F.3d 1347 (C.A.11 (Ga.), 2018)

Evidence was sufficient to prove that defendant knowingly possessed child pornography found on his computer, as required to support conviction for knowing possession of visual depictions of minors engaged in sexually explicit conduct; government presented evidence that child pornography was regularly downloaded to defendant's computer over an 11-month period, that obtaining the files required predicate manual acts of downloading a peer-to-peer file sharing program, searching for files, and initiating file downloads, that defendant lived alone and had exclusive control over his computer during most of that time period, that his computer was used to download child pornography on the same day it was used to file his tax return, and that defendant was traveling without internet access during a notable gap in the child pornography downloads.

United States v. Moberg, 888 F.3d 966 (C.A.8 (Mo.), 2018)

Evidence was sufficient to support jury's determination that defendant knowingly possessed child pornography on his home computer; six thumbnail images depicting child pornography that were found in the thumbnail database cache area of defendant's computer during a forensic examination were admitted at trial, government presented evidence that, in order for the thumbnail images to be present in the thumbnail database cache, a computer user had to purposely save or download a file onto the computer's

hard drive, two of the thumbnail images were from a known series of child pornography, and defendant admitted he was familiar with this series.

United States v. Lowe, 795 F.3d 519, 520 (6th Cir. 2015)

Government failed to prove defendant knowingly possessed child pornography on computer in his home that was accessible by other residents.

U.S. v. Figueroa-Lugo, 2015 WL 4385935 (C.A.1 (Puerto Rico),2015.)

Evidence of testimony that, in order to download files from a peer-to-peer file sharing service, the user had to actively click on the file, was sufficient to establish that defendant intentionally sought to download child pornography, as required to support conviction for knowing possession of child pornography.

Evidence that a child pornography image had been accessed from a peer-to-peer file sharing service through use of an internet browser on defendant's computer was sufficient to establish that defendant viewed child pornography that he had downloaded from the file sharing service, as required to support conviction for knowing possession of child pornography.

Evidence of expert testimony was sufficient to establish that "anti-virus" software on defendant's computer could not download child pornography by itself, as required to support conviction of defendant for knowing possession of child pornography.

Evidence of defendant's admission that he downloaded child pornography, and that the child pornography files were saved in folders bearing defendant's name on defendant's computer located in his bedroom, was sufficient to establish that he, rather than some else, downloaded child pornography to his computer, as required to support conviction for knowing possession of child pornography.

U.S. v. Woerner, 709 F.3d 527 (5th Cir. 2013)

The court's common sense, fact-specific approach to determine constructive possession of material containing child pornography, for purposes of possession of child pornography charge, often hinges on whether the defendant had exclusive or shared control over the place in which the child pornography was found; dominion, control, and knowledge, in most cases, may be inferred if a defendant had exclusive possession of the place in which the contraband is found, but this inference cannot be sustained if the

defendant shared joint occupancy of the place.

For purposes of possession of child pornography charge, if the place where material containing child pornography is found is shared by multiple users, the government must introduce some evidence, in addition to the evidence of shared use, to support a reasonable jury inference that the defendant knew that the images existed and had the knowledge and ability to access and exercise dominion and control over them.

Evidence that even though computer and email account might not have been under defendant's exclusive use and control, defendant knew that pornographic images existed and had the knowledge and ability to access and exercise dominion and control over them was sufficient to show that defendant had knowing, constructive possession of child pornography on his computer, as required for defendant's conviction for two counts of possession of child pornography.

Evidence that profile for account contained defendant's picture as well as other identifying information, other profile was registered in defendant's name, and many emails contained photographs of defendant and information about his daily life was sufficient to show that defendant was responsible for distributing child pornography from his email and related Internet accounts, as required for defendant's conviction for three counts of distribution of child pornography.

U.S. v. Rogers, 714 F.3d 82 (1st Cir. 2013)

Sufficient evidence established that child pornography found on defendant's laptop was downloaded knowingly and deliberately, as required to support conviction for possession of child pornography; web browser cookies and indexed history found on defendant's laptop computer indicated that someone had used browser to make numerous visits to websites related to, or within names indicative of, child pornography, including "nymphets-first-time-sex.com," "Natural Lolitas," and "innocent-girl.com," discovery of child pornography in temporary internet files folder suggested that those images were downloaded when user visited websites hosting them, and forensic analysis of laptop all but ruled out possibility that images had been downloaded by virus without user's knowledge.

Sufficient evidence established that person who knowingly possessed child pornography on defendant's laptop computer was defendant himself, as required to support conviction for possession

of child pornography; name of only user-created account on laptop was strongly associated with defendant, child pornography videos were found in shared folder associated with that user account, password hint for account was “My baby” and password itself was defendant's wife's name, defendant himself provided this password to pawn shop when he sold laptop, and did not point to evidence suggesting that anyone else knew it, laptop's web browser included bookmark for United States Navy's website, and defendant was member of Navy at time of his arrest.

U.S. v. Figueroa-Lugo, 2013 WL 43996 D.Puerto Rico,2013.

Evidence that defendant knowingly possessed child pornography files on his computer was sufficient to support his conviction for possessing child pornography; evidence showed investigators found child pornography files on hard drive of computer in defendant's room in his home, the only user account created on that computer was labeled with defendant's first name, the file names contained phrases typical of those used to name child pornography files, there was evidence that some of the files had been accessed, evidence about other activity on the computer when the files were created indicated defendant was using the computer at that time, and defendant admitted he installed peer-to-peer sharing network software on his computer and searched for files using the software.

To be found guilty of knowing possession of child pornography, an individual need only have known that there was child pornography on his computer yet declined to delete it; the defendant need not know the material's character at the moment that he downloads it, as long as he thereafter learns its character and nevertheless retains it.

U.S. v. Worthey, 2013 WL 2927359 (C.A.8 (Ark.))

Sufficient evidence established that files containing child pornography were knowingly downloaded and saved in permanent memory of defendant's laptop computer, as required to support convictions for receiving and possessing child pornography; evidence, including testimony from law enforcement agents, established that child pornography found on laptop was downloaded through peer-to-peer file-sharing programs onto laptop.

U.S. v. Haymond, 672 F.3d 948 (10th Cir. 2012)

There was sufficient evidence of defendant's knowing possession

of and actual control over child pornography to support his conviction for possessing child pornography, despite defendant's contention that he inadvertently downloaded child pornography from peer-to-peer file sharing client program while attempting to obtain music, where defendant admitted to frequently searching for and downloading child pornography, forensic investigator testified he found peer-to-peer file sharing client program on defendant's computer, government produced three images of child pornography found on defendant's computer, and defense's forensic specialists testified that downloading from file sharing program did not occur automatically.

There was sufficient evidence of defendant's knowledge that images found on his computer depicted minors engaged in sexually explicit conduct to support his conviction for possessing child pornography, in light of evidence that defendant used search terms associated with child pornography to find and then download charged images from peer-to-peer file sharing client program.

U.S. v. Salva-Morales, 2011 WL 5120683 (C.A.1 (Puerto Rico))

Evidence was sufficient to allow reasonable jury to conclude defendant knowingly possessed child pornography files on his computer, as required to support his conviction of knowing possession of child pornography; files were recovered only from two of the hard drives associated with defendant's personal computer and not from other computers in his shop, the names of many of the files clearly indicated that they contained child pornography, forensic examiners testified that several of the pornographic video files recovered from defendant's hard drive were created and placed in a folder titled “Porno” minutes before an image depicting defendant with a female was created and saved to another folder on the hard drive, and evidence showed that pornographic files were being accessed while defendant was alone in his shop.

U.S. v. Koch, 625 F.3d 470 (8th Cir. 2010):

Evidence presented at trial was sufficient to support finding that defendant had knowingly possessed images of child pornography, where well over 100 separate images of child pornography had been found on computer and flash drive seized from bedroom in home that defendant owned and occupied alone, user names on both computer and flash drive were variations on defendant's first name, pornographic images on each were located in folders which had to have been manually created by user of flash drive and

computer, and some images had been moved and others deleted.

U.S. v. Beckett, Slip Copy, 2010 WL 776049 C.A.11 (Fla.),2010.

> "The evidence was sufficient to establish that Beckett knowingly possessed child pornography because: (1) the child pornography was on Beckett's computer; (2) it was contained in an organized fashion in folders titled "porn;" and (3) it was stored under the user name "Timmy" (as in Timothy Beckett)."
>
> "The evidence was sufficient to show that Beckett enticed the victims to create and send pornographic photos because Beckett employed the same tactics on all four victims and ended up receiving the same result, a nude photo of the minor. Beckett's planned actions show that he had specific intentions and was well aware of the type of activity his conversations with the minors implied."

State v. Mercer, N.W. 2d (Wis. March 31, 2010):

> Finding that defendant knowingly possessed child pornography was supported by sufficient evidence, including evidence that defendant had habit of surfing the Internet for child pornography, that on the day in question he clicked to look at a magazine and its images of child pornography and then looked at others magazines and their child pornography images, that he controlled how long an image was displayed on his computer screen and had the ability to and knew how to print, save, or copy it, and that he deleted the files where forensic examiners would have found the child pornography stored in his hard drive.
>
> An individual "knowingly possesses" child pornography when he or she affirmatively pulls up images of child pornography on the Internet and views those images knowing that they contain child pornography, even if there is no evidence that the images were in the computer hard drive.

United States v. Schene, 543 F.3d 627 (10th Cir. 2008):

> Evidence was sufficient to establish that it was defendant, and not his wife, who violated statute prohibiting any person from knowingly possessing material that contained an image of child pornography that was produced using materials that had been mailed, shipped, or transported in interstate or foreign commerce; defendant and his wife were the only people with access to computer on which over 1,900 images of child pornography were

found, the images appeared under both of the operating system's user accounts and under two screen names, defendant had access to both user accounts, defendant admitted to using one of the screen names, images of child pornography started "popping up" only when investigators examining the computer switched to show defendant's account, and two government witnesses testified regarding the likelihood of defendant, rather than his wife, viewing the child pornography.

At trial of male defendant charged with knowingly possessing material that contained an image of child the district court did not commit reversible error in admitting testimony of agent and officer regarding the likelihood of a woman possessing child pornography; agent's testimony in this regard was to explain why he had focused his attention on defendant rather than defendant's wife and to show that he was acting in accordance with his training, and officer's testimony, to which defendant had not raised contemporaneous objection, did not constitute "plain" error, as it could be justified on the same basis as agent's testimony, the jury had already heard similar testimony from agent, and other evidence of defendant's guilt was substantial.

United States v. Irving, 432 F.3d 401 (2nd Cir. 2005)

Sufficient evidence established "knowingly" element in prosecution for receiving and possessing child pornography that was based on presence of video computer files on computer in defendant's apartment; there was no showing that anyone else lived in apartment or had access to computer on relevant dates, someone was at apartment on dates that images were downloaded, and defendant was not working on those days.

United States v. Bass, 411 F.3d 1198 (10th Cir. 2005):

Evidence was sufficient to support finding that defendant was aware of the child pornography saved in his computer, as required in conviction for knowing possession of child pornography; defendant's awareness that the materials were automatically saved to his computer was reasonably established by evidence he used two software programs to try to remove the images.

United States v. Payne, 341 F.3d 393 (5th Cir. 2003):

"We conclude that the number of images in Payne's possession, taken together with the suggestive titles of the photographs and Payne's testimony that he knew he was receiving child

pornography, supports the jury's inference that Payne knew he was receiving child pornography."

Kromer v. Commonwealth, 613 S.E.2d 871 (Va. 2005):

Evidence that defendant had exclusive control over residence in which computer containing sexually explicit images depicting persons under 18 years of age was found and admitted ownership of other items found on premises, that computer was registered in defendant's name, and that computer was configured to give quick desktop access to folder containing images at issue, was sufficient to support finding that defendant knew that images at issue existed, and exercised dominion and control over such images after they were downloaded, as required to support finding of constructive possession as element of misdemeanor possession of child pornography.

Receipt of Child Pornography

U.S. v. Nance, 2014 WL 4695068 (C.A.10 (Okla.))

There was sufficient evidence to support defendant's convictions for attempted receipt of child pornography, even though government was unable to recover visual images associated with deleted computer files and so could not prove that they contained child pornography, where each attempt count resulted from internet search that defendant conducted using search terms connected to child pornography, each file that defendant downloaded had title suggesting it contained child pornography, defendant downloaded all files when his wife and their children were out of town visiting her family, and government was able to retrieve over one thousand images of child pornography that defendant downloaded over several years' time.

State v. Reeves, 2012 WL 2021855 (Or.App.)

Here, the explicit titles of many of the files—which left nothing to the imagination—as well as their sheer volume—amply permitted a reasonable trier of fact to find, beyond a reasonable doubt, that defendant knew the downloaded files contained depictions of sexually explicit conduct involving a child and further that defendant knew that the creation of the visual recording involved child abuse.

U.S. v. Walden, 2012 WL 1537915 (C.A.11 (Ala.))

"Knowingly receiving" child pornography images includes intentionally viewing images sent to a defendant's computer, whether or not the viewer tries to save, edit, or otherwise exert more control over the images. However, inadvertent receipt of child pornography does not violate the statute.

State v. Urbina, 249 Or.App. 267, 2012 WL 1202133 (Or.App.)

Defendant "duplicated" videos containing images of children engaged in sexually explicit acts, as required to support conviction for first degree encouraging child sexual abuse, by installing a software program on his home computer that allowed him to access a peer-to-peer file-sharing network via his internet connection and then using the program to download the videos; defendant's actions created his own copies of the videos, which he could then display on his own computer or share with others.

U.S. v. Pruitt, 638 F.3d 763 (11th Cir. 2011)

A person "knowingly receives" child pornography under child-pornography-receipt statute when he intentionally views, acquires, or accepts child pornography on a computer from an outside source.

Under the child-pornography-receipt statute's "knowingly receives" element, an intentional viewer of child-pornography images sent to his computer may be convicted whether or not, for example, he acts to save the images to a hard drive, to edit them, or otherwise to exert more control over them.

Evidence that a person has sought out—searched for—child pornography on the Internet and has a computer containing child-pornography images—whether in the hard drive, cache, or unallocated spaces—can count as circumstantial evidence that a person has "knowingly receive[d]" child pornography.

Peer to Peer Sharing is Distribution

U.S. v. Layton, 564 F.3d 330 (4th Cir. 2009):

Imposition of sentencing increase for distribution of child pornography was warranted for defendant convicted of possession of child pornography; defendant told FBI agents that as a member of a file-sharing program, he created a shared folder called "My

Music" with privileges that allowed other people to download files that he put into the folder.

Use of a peer-to-peer file-sharing program constituted "distribution," within meaning of sentencing guideline providing for two-level sentencing increase for distribution of child pornography.

U.S. v. Schade, (3rd Cir. 2009): *unpublished opinion*

Evidence that defendant was notified while downloading software for peer-to-peer file-sharing network that it would allow others to upload files from his computer, that he changed the default settings for file-sharing, and that he used the software for file-sharing, was sufficient to show that defendant knew child pornography files on his computer could be downloaded by other users, as required for conviction of transporting child pornography.

Evidence that undercover police officer downloaded child pornography video through peer-to-peer file-sharing network in part from defendant's computer was sufficient to support conviction for transporting or aiding and abetting the transportation of child pornography, even if there was no way of knowing which portion of the downloaded file was contributed by defendant's computer.

U.S. v. Handy, (M.D. Fla. 2009)

In ruling that possession child porn images in a shared folder of a peer-to-peer client may constitute distribution, the court compared the shared folder to a self service gas station where the owner advertises his product and lets people take what they want. The court ruled, however, that the government failed to show that the software was actually configured to allow people to share the relevant files.

U.S. v. Shaffer, 472 F.3d 1219 (10th Cir. 2007):

Defendant "distributed" child pornography when he downloaded pornographic images and videos from a peer-to-peer computer network and stored them in a shared folder on his computer accessible by other users of the network; defendant transferred and dispersed the child pornography to others, in that he freely allowed them access to his computerized stash of images and videos and openly invited them to take or download those items, and defendant understood that the purpose of the shared folder was to allow others to access items he stored in it.

To support conviction for distribution of child pornography, government was not required to prove that defendant had the intent to distribute child pornography and that he caused it to be distributed, but only that he knowingly distributed the child pornography.

Exclusion of defendant's computer expert's proffered testimony, that based upon the file structure of defendant's computer hard drive defendant was on a pornography fishing expedition with no particular calculation toward any particular type of material, other than generally sexually explicit material, was warranted, in prosecution for distribution and possession of child pornography; the proposed testimony went to defendant's state of mind or whether he knowingly committed the charged offenses, and expert witnesses were prohibited from testifying regarding such ultimate issues.

Discussion: This is a good reference case. The Court begins by giving a brief overview of how peer-to-peer works and how a folder is designated as "shared." This language may be helpful to quote to your judge when trying to explain the issue in a legal memorandum. The Court also draws an interesting analogy to a self-serve gas station, noting that the owner is distributing gas even though he may not be present at the station. Finally, the case shows how a good law enforcement interview assists in these matters. The agents got the defendant to admit he knew that others could share what was in his folder and that others had done so.

U.S. v. Abraham, slip copy (W.D. Pa. 2006):

"Having done so, we find that the defendant distributed a visual depiction when as a result of the defendant's installation of an internet peer-to-peer video file sharing program on his computer, a Pennsylvania state trooper was able to download the child pornography from the defendant's computer to the trooper's computer."

"The Court finds that the Government has proven beyond a reasonable doubt that the Defendant knowingly distributed the movie image in question. The Defendant chose to share the movie image in question with anyone using the Gnutella network via the Bearshare file-sharing program which he installed on his computer. His act of choosing to share the movie image was voluntary on his part. He did not have to share the movie image; the Bearshare program allowed him the option not to share any file he

downloaded. Neither the fact that the Defendant did not personally know Trooper Erderly nor the fact that Trooper Erderly had not had any communication with the defendant prior to downloading the chid pornography is relevant."

Copying to disk is production

United States v. Maxwell, 386 F.3d 1042 (11th Cir. 2004):

> Copying child pornography to disk was sufficient to constitute "production."

Proof that defendant is person who sent pictures:

U.S. v. Bynum, --- F.3d ----, 2010 WL 1817763 (C.A.4 (N.C.))

> Sufficient evidence supported conclusion that defendant, and not somebody else in his residence, committed offenses charged in prosecution for transporting and possessing child pornography, where agents found computer in question in defendant's bedroom, which was same bedroom visible in defendant's profile photos taken using computer's camera, computer login used defendant's first name, and computer contained chat log of conversations defendant had discussing photos.

United States v. Campos, 221 F.3d 1143 (10th DCA 2000):

> Evidence supported conviction for transporting child pornography through interstate commerce via computer, despite evidence that defendant's roommate actually sent images in question; defendant admitted that he used screen name used by person who sent images in question, internet service account through which images were sent was in defendant's name and was paid for with his credit card, and document examiner testified that it was probably defendant's handwriting on document with file name resembling file name that contained pornographic photograph.

Pandering Child Pornography

United States v. Williams, 553 U.S. 285, 128 S.Ct. 1830 (2008):

> Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act section prohibiting offers to provide and requests to obtain child pornography does not require actual existence of child pornography and rather than targeting

underlying material bans collateral speech that introduces such material into child-pornography distribution network; thus, Internet user who solicits child pornography from undercover agent violates statute even if officer possesses no child pornography, and likewise person who advertises virtual child pornography as depicting actual children also falls within its reach.

(PROTECT) Act pandering provision's string of operative verbs "advertises, promotes, presents, distributes, or solicits," is reasonably read to have a transactional connotation, i.e., statute penalizes speech that accompanies or seeks to induce transfer of child pornography, via or reproduction or physical delivery, from one person to another.

Term "promotes" in (PROTECT) Act pandering provision does not refer to abstract advocacy, such as statement "I believe that child pornography should be legal" or even "I encourage you to obtain child pornography"; it refers to the recommendation of a particular piece of purported child pornography with the intent of initiating a transfer.

Soliciting parent to make child available for sex is sufficient for solicitation

United States v. Bolen, (11th Cir. 2005)

Statute proscribing the use of a facility and means of interstate commerce for enticement to commit child molestation prohibits an individual from arranging to have sex with a minor, even a fictitious minor, through communications with an adult intermediary, as opposed to prohibiting only direct communications with a minor.

Restitution to Child Depicted in Photo:

U.S. v. Solsbury, 2010 WL 3023913 (D.N.D.,2010)

Although child depicted in pornographic videos defendant possessed was harmed by defendant's offense of receipt of materials involving sexual exploitation of minors, so as to be a victim of the offense, government failed to prove amount of victim's losses proximately caused by defendant's conduct, as required for restitution order following defendant's conviction; although victim's statements and psychologist's reports demonstrated victim faced long and difficult course of treatment for post-traumatic stress disorder and other disorders, all caused and/or related to her sexual abuse and knowledge that images of

her exploitation had been viewed by numerous people, government failed to show portion of victim's losses specifically caused by defendant's possession of pornographic videos.

The statute providing for mandatory restitution for any offense under the statutes criminalizing the sexual exploitation and abuse of children includes a proximate cause requirement, and the statute requires that restitution be ordered only if the defendant's crime is the proximate cause of the victim's losses.

U.S. v. Hardy**,** F.Supp.2d ----, 2010 WL 1543844 (W.D.Pa.)

Even though defendant did not take actual photographs of child pornography which he possessed and distributed to others over the Internet, the individual whose image was depicted in the series of photographs was a "victim" of his receipt, possession and distribution of the images, pursuant to Mandatory Restitution for Sexual Exploitation of Children Act; passive user of child pornography directly contributed to continuing victimization of individual.

Even though defendant did not take actual photographs of child pornography which he possessed and distributed to others over the Internet, defendant's conduct in disseminating images was a substantial factor in causing victim ongoing psychological and economic harm, and thus defendant proximately caused her injuries for purposes of award of restitution pursuant to Mandatory Restitution for Sexual Exploitation of Children Act was warranted; defendant's circulation of photographs perpetuated abuse initiated by producer of images and contributed to individual's ongoing victimization.

Enticing a Child Without Overt Act to Meet Child

Commonwealth of Massachusetts v. Disler, 884 N.E.2d 500 (Mass. 2008):

Commonwealth was not required to prove, in prosecution for child enticement, that defendant engaged in any overt act in accordance with his intention, expressed in sexually explicit instant messages sent over the Internet, to violate one or more statutorily enumerated criminal statutes.

Crime of child enticement is complete when an individual, possessing the requisite criminal intent, employs words, gestures,

or other means to entice, lure, induce, or persuade someone who is under the age of 16, or whom the actor believes is under the age of 16, to enter or remain in a vehicle, dwelling, building, or outdoor space.

Fact that individual believed by defendant to have been 14-year-old girl, to whom he sent sexually explicit instant massages over the Internet, did not in fact exist was not defense to charge of child enticement.

Japanese Anime Cartoon is Obscenity

U.S. v. Koegel, 2011 WL 1441851 (E.D.Va.)

Evidence that the Japanese anime cartoons found on defendant's computer depicted minors engaged in sexually explicit conduct was sufficient to find him guilty of possessing obscene visual representations of the sexual abuse of children; cartoons were obscene, the abundance of the cartoons on the computer demonstrated defendant's awareness of their nature, and the cartoons were shipped through interstate commerce via the internet.

Under community standards, Japanese anime cartoons found on defendant's computer were obscene within meaning of statute prohibiting possessing obscene visual representations of the sexual abuse of children; cartoons appealed to a prurient interest in sex by depicting children in pain from being sexually abused by an adult, they depicted patently offensive sexual conduct, since many of them showed young children engaged in forced sexual intercourse with adults, and they lacked serious literary, artistic, political, or scientific value, since cartoons depicting rape or forced sexual activity with a minor appealed only to the prurient interest of the person viewing them.

ECPA/PPA ISSUES

Legality of spyware program to intercept communications

O'Brien v. O'Brien, 899 So.2d 1133 (5th DCA 2005):

Wife illegally "intercepted" husband's electronic communications with another woman via electronic mail and instant messaging, within meaning of Security of Communications Act, when she installed spyware program

on computer which simultaneously copied electronic communications as they were being transmitted.

Exclusion of illegally intercepted electronic communications between husband and another woman was not abuse of discretion, in action for divorce, even though Security of Communications Act did not include electronic communications in its provision excluding evidence of illegally intercepted wire or oral communications.

Trial court's finding that wife illegally intercepted husband's electronic communications with another woman, which finding was grounds for excluding communications in divorce proceedings, did not either directly, or by implication, constitute conviction of crime under Security of Communications Act.

Application of Wiretap Act to Hackers

United States v Steiger, 318 F.3d 1039 (11th Cir. 2003):

Computer hacker's acquisition of information implicating defendant in sexual exploitation of children and possession of child pornography through use of virus that enabled him to access and download information stored on defendant's personal computer did not violate Wiretap Act, since there was nothing to suggest that any information was obtained by hacker through contemporaneous acquisition of electronic communications while in flight.

Wiretap Act provides no basis to suppress unlawfully intercepted electronic communications.

Application of wiretap law to business's interception of customers' emails

United States v. Councilman, 373 F.3d 197 (1st Cir. 2004):

An online rare book service offered its customer's email services. The company devised a program that would screen incoming mail to its customers to determine which messages were coming from its competitor, Amazon.com. The company would then use this information to its advantage. The government prosecuted the defendant under the wiretap law, but the appellate court ruled that the wiretap law does not apply because under the setup, the data was technically in electronic storage and thus, not covered by the wiretap law. This case has a good discussion as to how the current laws do not keep up with technology. It is a good resource case.

Electronic Storage

Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004):

> E-mail messages which were delivered to recipient and stored by internet service provider (ISP) were in "electronic storage," and thus e-mail messages were protected from unauthorized disclosure by the Stored Communications Act, as messages were stored for purpose of backup protection.
>
> Prior access to e-mail messages stored by internet service provider (ISP) was irrelevant to whether the messages were in "electronic storage" within meaning of the Stored Communications Act; such e-mail messages were in electronic storage regardless of whether they had been previously delivered.

> Wireless communications provider that contracted with city to provide text messaging services for city's employees was "electronic communication service" (ECS) under Stored Communications Act (SCA), rather than a remote computing service (RCS), and thus violated SCA when it knowingly released archived transcripts of police officers' text messages to city at city's request, since city was subscriber but not addressee or intended recipient; provider gave city "ability to send or receive wire or electronic communications," rather than "provi[ding] to the public ... computer storage or processing services."

Text Messages under ECPA:

United States v. May, F.Supp. (D.Minn. 2006):

> Cellular telecommunications provider was not acting as a government agent, for Fourth Amendment purposes, in providing text messages beyond the scope of the time period specified in a search warrant, and thus, the strictures of the Fourth Amendment did not apply to the additional information provided.
>
> Discussion: This case was actually decided under 4th Amendment principles, but it could just have easily been an ECPA issue.

Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008):

> Wireless communications provider that contracted with city to provide text messaging services for city's employees was "electronic communication service" (ECS) under Stored Communications Act (SCA), rather than a remote computing service (RCS), and thus violated SCA

when it knowingly released archived transcripts of police officers' text messages to city at city's request, since city was subscriber but not addressee or intended recipient; provider gave city "ability to send or receive wire or electronic communications," rather than "provi[ding] to the public ... computer storage or processing services."

Police officer had reasonable expectation of privacy, under Fourth Amendment, in text messages sent to and from his city-owned pager, even though department's written computer and e-mail policy decreed that no expectation of privacy should attach to use of those resources, and even assuming that messages constituted public records under California Public Records Act (CPRA); police lieutenant in charge of pagers had established informal policy under which officer's messages would not be audited if he paid for usage overages, and CPRA did not diminish officer's reasonable expectation.

Employees of city police department had expectation of privacy, under Fourth Amendment, in content of text messages that they sent and received using city-owned pagers, and that were archived by wireless service provider that contracted with city; fact that provider had capability to access content for its own purposes did not remove that expectation.

Email Header and Website History Under ECPA

U.S. v Forrester, 512 F.3d 500 (9th Cir. 2008):

Use of pen register, a device that records numbers dialed from telephone line, is not a Fourth Amendment "search."

Use of computer surveillance techniques that revealed "to" and "from" addresses of e-mail messages, addresses of websites defendant had visited, and total amount of data transmitted to or from defendant's Internet account did not amount to "search" in violation of Fourth Amendment; e-mail and Internet users had no expectation of privacy in to/from addresses of their e-mail messages or Internet protocol (IP) addresses of websites they visited.

Even if government's use of computer surveillance techniques to obtain "to" and "from" addresses for e-mail messages and addresses of websites defendant had visited was beyond scope of pen register statute, suppression of evidence government had obtained through such surveillance was not available as remedy, in prosecution for conspiracy to manufacture ecstasy and related offenses, absent showing that surveillance violated the law, or that suppression was remedy set forth in pen register statute.

ECPA Warrants

In re Search of Google Email Accounts, 99 F.Supp.3d 992 (D.Alaska,2015)

> Modification of warrant requiring web-based e-mail provider to provide government with e-mail correspondence from third-party accounts, hosted by provider, that involved "enticement of a minor to engage in sexual activity for which any person can be charged with a criminal offense," such that under modified warrant, provider would not have to inspect e-mails for relevancy or evidentiary value, was warranted; provider lacked law enforcement expertise, provider was not equipped to determine whether particular content of e-mails reflected innocent behavior or was evidence of criminal behavior, there was possibility that provider might overlook important evidence, and efforts would ultimately be repeated by law enforcement once content was disclosed.

Other:

DePugh v. Sutton, 917 F.Supp. 690 (W.D. Missouri 1996):

> Privacy Protection Act, which prohibits government, without first obtaining a subpoena duces tecum, from seizing work product material from possessor of documentary evidence who is not suspect in offense under investigation, and who is reasonably believed to have as purpose the dissemination of information to public, did not protect documents possessed by party with 45-year history of writing and publishing to the extent that documents were sought in connection with investigation of that same party as suspect in government investigation of child pornography. Privacy Protection Act of 1980, § 202, 42 U.S.C.A. § 2000aa-12.

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997):

> Facts: (Quoted from opinion) Mr. Davis operated the Oklahoma Information Exchange, a computer bulletin board system. Computer users could subscribe to the bulletin board, dial in using a modem, then use the system to send and receive messages via e-mail, access the Internet, utilize on-line databases, and download or upload software. According to Mr. Davis, approximately 2000 subscribers used his bulletin board.
>
> In April 1993, the Oklahoma City Police Department received an anonymous tip that Mr. Davis was selling obscene CD-ROMs from his business premises. On three different occasions, an undercover officer purchased "adult" CD-ROMs directly from Mr. Davis. During one of

these visits, Mr. Davis mentioned to the officer that he operated a bulletin board, and that similar pornographic images could be accessed by dialing in to the bulletin board. The officer never actually saw the computer equipment used to operate the bulletin board. In his affidavit for a search warrant, the officer did not mention the possibility that a bulletin board was being operated on the premises, or the possibility that this bulletin board could be used to distribute or display pornographic images. A judge determined that two CD-ROMs acquired from Mr. Davis were obscene, and issued a warrant to search his business premises for pornographic CD-ROMs and "equipment, order materials, papers, membership lists and other paraphernalia pertaining to the distribution or display of pornographic material in violation of state obscenity laws set forth in O.S. Title 21-1024.1." Aplee. supp. app., vol. I at 45.

Several officers, including defendants Anthony Gracey and Mark Wenthold, conducted the search at Mr. Davis' business. During the search, the officers discovered the bulletin board. Attached to it were CD-ROM drives housing sixteen CD-ROM discs, including four discs identified by Mr. Davis to the officers as containing pornographic material. The officers believed from the configuration of the bulletin board computers that the files accessible via the bulletin board included files from the four pornographic CD-ROMs. The officers called for assistance from officer Gregory Taylor, who was reputed to be more knowledgeable about computers than they were. He confirmed that the pornographic CD-ROMs could be accessed via the bulletin board. The officers seized the computer equipment used to operate the bulletin board, including two computers, as well as monitors, keyboards, modems, and CD-ROM drives and changers. The seizure of this computer equipment is the subject of the federal proceedings in this case.

At the time of the seizure, the computer system contained approximately 150,000 e-mail messages in electronic storage, some of which had not yet been retrieved by the intended recipients. The hard drive of the computer system also contained approximately 500 megabytes of software which had been uploaded onto the bulletin board by individual subscribers. Mr. Davis intended to republish this "shareware" on a CD-ROM for sale to the public. Mr. Davis had previously published three such compilations of shareware on CD-ROM.

Mr. Davis, Gayla Davis, John Burton, and TSI Telecommunications Specialists, Inc., > (FN1) filed the instant suit in federal court alleging claims under > 42 U.S.C. § 1983 for violation of First and Fourth Amendment rights, and under the Privacy Protection Act (PPA), > 42 U.S.C. §§ 2000aa--> 2000aa-12, and the Electronic Communications Privacy Act (ECPA), > 18 U.S.C. §§ 2510-> 2711. The crux of the complaint is that the seizure of the equipment was illegal because the

warrant was not sufficiently particular and because the seized computer system contained e-mail intended for private subscribers to the bulletin board, and software intended for future publication by Mr. Davis. Plaintiffs contend these stored electronic materials were outside the scope of the warrant, and are protected by several congressional enactments.

Original defendants in this suit included the City of Oklahoma City, the Oklahoma City Police Department, and several officers of the Oklahoma City Police Department who executed the search and seizure of the computer equipment. The municipal entities were dismissed from the case. Plaintiffs do not dispute that their only remaining claims are against the officers in their individual capacities. The district court entered summary judgment for the officers, holding that their reliance on a valid warrant entitled them to qualified immunity on the constitutional claims, and entitled them to the statutory good faith defenses contained in the PPA and ECPA.

Holding:

- Failure timely to return seized material which is without evidentiary value and which is not subject to forfeiture may state constitutional or statutory claim. Since plaintiffs made no allegation that defendant officers are persons with authority to return materials once seized, their claim fails as to that issue.

- Search warrant which directed police officers to search for equipment pertaining to distribution or display of pornographic material in violation of state obscenity laws was sufficiently particular, and encompassed computer equipment used to access and copy pornographic files.

- Search warrant which directed police officers to search for equipment pertaining to distribution or display of pornographic material in violation of state obscenity laws was not overly broad, as description included only that equipment directly connected to suspected criminal activity, not wide range of equipment used for purposes unrelated to suspected criminal activity, and it did not encompass all equipment one might expect to find at legitimate business.

- If executing officers flagrantly disregard limitations of search warrant, otherwise constitutional warrant might be transformed into general search. The officers in this case were careful to only take that equipment directly related to the distribution of pornography. They left most of the equipment alone.

- Search warrant which directed police officers to search for

equipment pertaining to distribution or display of pornographic material in violation of state obscenity laws, which was supported by probable cause based on defendant's sale of pornographic CD-ROMs to undercover officer, was not invalidated merely because officers knew about defendant's computer bulletin board, through which pornography was also distributed, but did not include this knowledge in affidavit supporting warrant.

- Incidental temporary seizure of stored electronic materials did not invalidate seizure of computer within which they were stored, pursuant to valid search warrant which directed police officers to search for equipment pertaining to distribution or display of pornographic material in violation of state obscenity laws; computer was more than merely container for files, it was instrumentality of crime.

- Fact that given object may be used for multiple purposes, one licit and one illicit, does not invalidate seizure of object when supported by probable cause and valid warrant.

- Seizure of container is not invalidated by probability that some part of its innocent contents will be temporarily detained without independent probable cause.

- Police officers were entitled to seize all of defendant's computer equipment involved in crime of distributing obscenity, not just CD-ROMs and CD-ROM drives, pursuant to search warrant which directed police officers to search for equipment pertaining to distribution or display of pornographic material in violation of state obscenity laws.

- Police officers' reliance on valid warrant when seizing computer equipment involved in crime of distributing obscenity entitled them to qualified immunity on Fourth Amendment claims of equipment owner, his related businesses, and several users of e-mail on his bulletin board, in > § 1983 action.

- Privacy Protection Act (PPA) did not authorize private suit against municipal police officers, who seized plaintiff's computer equipment pursuant to valid search warrant, in their individual capacities; accordingly, Court of Appeals lacked subject matter jurisdiction over PPA claim. Privacy Protection Act of 1980, § 106, > 42 U.S.C.A. § 2000aa-6.

- Municipal police officers who seized computer equipment pursuant to valid warrant, which resulted in incidental seizure of

stored electronic communications, qualified for statutory good faith defense under Electronic Communications Privacy Act (ECPA), as matter of law.

Discussion: This case is full of interesting issues concerning the liability of police officers for violating the Privacy Protection Act and the Electronic Communications Privacy Act. The officers in this case escaped liability based upon their good faith reliance on a valid search warrant, but a careful review of the opinion will demonstrate the various pitfalls awaiting officers who do not thoroughly do their homework prior to a search or seizure of such equipment. One important observation of the court was that the computer seized was seized because it was an instrumentality of the crime, not because of its content. The court specifically rejected the defense claim that the police needed probable cause concerning the contents of the computer prior to seizing it. The court noted that the police never attempted to look at the contents of the computer and they would have needed a second warrant to do so under the circumstances.

United States v. Hambrick, 55 F. Supp. 2d 504 (WD Vir. 1999)

Based on a series of online Internet conversations with defendant, a police officer concluded that defendant sought to entice a teenage boy to leave home and live with defendant. To determine defendant's identity and location, the officer obtained a state subpoena that he served on defendant's Internet Service Provider. The subpoena requested that the service provider produce any records pertaining to defendant's account. The service provider complied, and supplied the officer with the requested information. The subpoena was determined to be invalid, and defendant filed a motion to suppress the evidence gathered from his Internet Service Provider, as well as evidence gathered during a search of his home. The court denied defendant's motion. The court found that, to have any interest in privacy, there must have been some exclusion of others from the information defendant had been placing on the Internet. The court held that defendant had no legitimate expectation of privacy in information he voluntarily turned over to third parties and, therefore, he was not entitled to U.S. Const. amend. IV protection.

OUTCOME: The court denied defendant's motion to suppress all evidence obtained from his Internet Service Provider, as well as all evidence seized from defendant's home pursuant to a subsequent warrant. The court found that defendant could not have had a reasonable expectation of privacy because, when defendant knowingly exposed information to the public via the Internet, he was not afforded Fourth Amendment protection.

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001):

After an Internet Investigation, the defendant sued law enforcement under both the PPA and the ECPA.

- Courts have applied this principle to computer searches and seizures to conclude that computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person--the system operator. **See *Maxwell**, 45 M.J. at 418; **United States v. Kennedy**, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000)* **[**21]** (rejecting a privacy interest in subscriber information communicated to an internet service provider); ***United States v. Hambrick**, 2000 U.S. App. LEXIS 18665, No. 99-4793, 2000 WL 1062039,* at *4 (4th Cir. Aug. 3, 2000) (unpublished) (holding that defendant destroyed any privacy interest in his subscriber information when he conveyed it to an internet service provider) (citing ***Miller**, 425 U.S. at 442).* We conclude that plaintiffs in these cases lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators. In addition, in the **O'Brien** case, subscriber information would be that of the users, who do not have Fourth Amendment standing.
- Moreover, § 2703(c) applies to the service provider and not to the government. **See *Tucker v. Waddell**, 83 F.3d 688, 693 (4th Cir. 1996)* ("The **[**32]** language of § 2703(c) does not prohibit any governmental conduct, and thus a governmental entity may not violate that subsection by simply accessing information improperly")
-

Figueroa v. State, 29 Fla. L. Weekly D876 (Fla. 5th DCA 2004):

> Obtaining cellular telephone records from telephone service provider pursuant to investigative subpoena, as opposed to warrant, did not violate Fourth Amendment.
>
> Obtaining records, which contained telephone numbers only, with no communicative information regarding substance of calls, did not amount to search.

Imparato v. Spicola, 238 So.2d 503 (Fla. 2d DCA 1970):

> This case is not an ECPA issue, but it provides us with language concerning the broad scope of State Attorney subpoena powers and refers to the State Attorney as a "one man grand jury." This issue may be important because section 2703(c) includes the language administrative subpoena, trial subpoena and grand jury subpoena, but does not include investigative subpoena.

EVIDENCE; (Also see Child Porn section)

Admissibility of Computer Forensic Examiner Testimony

People v. Shinohara**,** 375 Ill.App.3d 85, 872 N.E.2d 498, 313 Ill. App. 1 Dist. 2007

State presented sufficient evidence to establish that software was functioning properly when officer used it and ensured that images presented at trial accurately portrayed images on defendant's computer; although officer stated that he did not test software for accuracy before using it to copy hard drives on defendant's computer, he explained that software had computer industry standard built into it that utilized algorithm to verify that image it was taking of hard drive was accurate, and application of standard during copying process reflected that software was operating properly.

Officer's self-created spreadsheet corresponding to child pornography images found on defendant's computer was admissible and not a police report as spreadsheet was created by collecting information generated by computer.

Officer's spreadsheet corresponding to child pornography images found on defendant's computer was not inadmissible on hearsay grounds; contents of spreadsheet were subject to verification, defendant had computer at his disposal and could have tested accuracy of information included in spreadsheet any time prior to officer's testimony, and officer was available at trial and subject to cross-examination by defense counsel.

Authentication of Records, Chat, Email etc..

United States v. Lamm, 5 F.4th 942 (C.A.8 (S.D.), 2021)

Circumstantial evidence was sufficient to establish authenticity of social media accounts in prosecution of defendant for possession, distribution, and production of child pornography; government linked the same cell phone number in defendant's name to both accounts, the same images that appeared on defendant's social media account appeared on second account with a different name, defendant had copies of those images on memory cards in his apartment, those same memory cards also contained screenshots of private messages accessible by only one social media account, and other online subscriptions found on defendant's computer used an e-mail address containing the name on second social media account.

Gilbert v. State, 2021 WL 2385832, (Fla.App. 2 Dist., 2021)

The victim confronted the suspect on Facebook Messenger about his sexual abuse of her. She took screen captures of their conversation. The court ruled the screen captures were properly authenticated even though the State never obtained the records from Facebook or extracted the data from her cell phone. The court relied on State v. Torres, 304 So.3d 781 (Fla. 4th DCA 2020) as precedent. The court noted, "communications can be authenticated by appearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with the circumstances." The victim and suspect discussed facts only known to them and the victim had chatted frequently with suspect so that she was familiar with his online identity.

State v. Torres, 2020 WL 5937416, (Fla.App. 4 Dist., 2020)

The trial court ruled the State did not properly authenticate screen captures of text messages. The state appealed and the Fourth DCA ruled that the messages were properly authenticated. The primary facts are as follows:

> *The State charged the Defendant with sex offenses arising from the sexual molestation of his minor cousin, which took place when the Defendant was about 30 years old and the victim was about 12 years old. The victim testified that when she was 14 or 15 years old, she began receiving text messages from a person she believed to be the Defendant. The content of the messages was mostly sexual. She received these messages on her cell phone for over a year through a social media and messaging application called "Kik." The victim took screenshots of some of the messages with the idea she might report the abuse when she was older.*
>
> *The victim acknowledged that the sender's profile picture did not show the Defendant, but testified she could tell that the Defendant was the sender because of the messages' content. The sender identified himself by using a screen name that was a nickname the Defendant's family members used for him. Significantly, the text messages referenced information known only to the victim and the Defendant, such as a* ***sexual*** *encounter with the victim by a pool and a watch the Defendant had given the victim as a gift. The content of the messages also pointed to the Defendant as the sender because he identified himself as the victim's cousin,*

indicated he was much older than the victim, and, when the victim asked if he was moving to California with "Suzette," the mother of the Defendant's child, he responded, "of course."

The opinion provides a good discussion of the case law on properly authenticating such evidence.

Symonette v. State, 100 So.3d 180 (Fla. 4th DCA 2012)

Photographs of text messages were sufficiently authenticated so as to be admissible at murder trial; driver testified that she texted the defendant when they were sitting next to each other in the car, and later after they were separated, detective recovered cell phone from defendant and later executed a search warrant on the cell phone, investigators took photographs of those messages, and driver identified the text messages between her and the defendant, and discussed the context of the messages.

Eugene v. State, 2011 WL 222159 (Fla.App. 4 Dist.))

Email and text messages from victim to defendant were not hearsay because they were not offered for the truth of the matter asserted. They were offered to: "Text messages and emails between appellant and the victim gave definition to the intensity of their unique relationship."

Officer's explaining his theory of the case to defendant during interrogation was not hearsay for the same reason.

State v. Lumarque, 44 So.3d 171 (Fla. 3rd DCA 2010):

Sexually suggestive images and text messages between defendant's ex-wife and a boyfriend, which were found on defendant's cellular telephone, were sufficiently authenticated as to be admissible as evidence of motive in prosecution for burglary with assault or battery and other offenses arising out of an alleged incident between defendant and ex-wife, even if ex-wife could not authenticate the images and text messages, where State's forensic expert testified that the images and text messages were found on defendant's telephone after it was seized pursuant to a search of defendant's home through a warrant shortly after the alleged incident.

U.S. v. McNealey, --- F.3d ----, 2010 WL 4366921 (C.A.5 (Miss.))

District court's admission of child pornography images did not violate best evidence rule; forensic imaging process used by the government produced an exact copy of the digital files on defendant's computer, these files were

then captured on DVDs and exhibits were printed from the DVDs, the government presented evidence establishing the chain of custody and the technology utilized, and defendant did not argue that the printouts were not accurate representations of the photos on his hard drive but, rather, his argument appeared to be that the government failed to prove that the images depicted actual, as opposed to virtual, children, an argument that was rejected by the appellate court and that was not pertinent to the inquiry under the subject rule.

Cooper v. State, 35 Fla. L. Weekly D2029 (Fla. 4th DCA 2010):

Verizon store manager was allowed to testify as a records custodian to introduce and explain Verizon records that showed the defendant's location at the time of the murder.

Griffen v. State, --- A.2d ----, 2010 WL 2105801 (Md.App.)

Circumstantial evidence was sufficient to authenticate printout from pseudonymous social networking website profile alleged to be that of defendant's girlfriend; profile printout featured a photograph of defendant and his girlfriend in an embrace, contained the user's birth date, which matched defendant's girlfriend's birth date, and identified user's boyfriend as "Boozy," the nickname that defendant's girlfriend ascribed to defendant.

The burden of proof for authentication is slight, and a court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.

Rule permitting authentication by circumstantial evidence permits authentication of electronic communications based on the content and the circumstances of those messages.

Commonwealth v. Williams, 456 Mass. 857, 926 N.E.2d 1162 (2010)

Computer messages on social networking Internet site were not authenticated, although foundational testimony established that the messages were sent by someone with access to account of alleged writer of messages; foundational testimony did not identify the person who actually sent the messages, whether anyone other than alleged writer could communicate from the Web page, how secure the Web page was, who could access it, and whether codes were needed for access.

U.S. v. Burt, 495 F.3d 733 (7th Cir. 2007):

In prosecution for sexual exploitation of a minor and distributing child

pornography, portions of transcripts of online chat conversations between defendant and an online associate consisting of associate's half of the conversations did not constitute hearsay, since they were not admitted to prove the truth of the mat-ters asserted, which related to the associate's sexual activities with particular boys whose photographs he might have been sharing with the defendant.

probative value of transcripts of online chat conversations between defendant and online associate in which they traded photographs of children while making sexual comments, in which transcripts government had substituted defendant's and associate's names for screen names that had originally appeared in transcript, was not substantially outweighed by danger of unfair prejudice; court, while noting evidence that the screen names corresponded to defendant and associate, admonished jury that they were to independently evaluate whether the screen names were actually used by defendant and associate, and there was no unfair prejudice, since transcripts depicted conduct for which defendant was being prosecuted.

U.S. v. Jackson, --F.3d – (D. Neb. May 8, 2007)

Print-out records of online chat preserved by cutting and pasting chat into Word document was not admissible. Chat was not properly authenticated because there was evidence that it was unreliable.

Lorraine v. Markel American Ins. Co**.,** F.Supp.2d (D.Md. 2007)

A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. Id. at § 901 .02[3]. This is not a particularly high barrier to overcome. For example, in United States v. Safavian, the court analyzed the admissibility of e-mail, noting,

**9 [t]he question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is....' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.*

435 F.Supp.2d at 38 (citations omitted)). See also United States v. Meienberg, 263 F.3d 1177, 1180 (10th Cir.2001) (analyzing admissibility of printouts of computerized records); United States v. Tank, 200 F.3d 627, 630 (9th Cir.2000) (analyzing admissibility of exhibits reflecting chat room conversations); United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir.1994)(discussing admissibility of radiotelegrams); United States v. Howard-Arias, 679 F.2d 363, 366 (4th Cir.1982)(addressing chain of

*authenticity); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 WL 2367740, at * 16 (N.D.Ill. Oct. 15, 2004) (analyzing admissibility of the content of a website).*

Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation. See, e.g., In Re Vee Vinhnee, 336 B.R. 437 *(proponent failed properly to authenticate exhibits of electronically stored business records);* United States v. Jackson, 208 F.3d 633, 638 (7th Cir.2000) *(proponent failed to authenticate exhibits taken from an organization's website);* St. Luke's Cataract and Laser Institute PA v. Sanderson, 2006 WL 1320242, at *3-4 (M.D.Fla. May 12, 2006) *(excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts);* Rambus v. Infineon Tech. A. G., 348 F.Supp.2d 698 (E.D.Va.2004) *(proponent failed to authenticate computer generated business records);* Wady v. Provident Life and Accident Ins. Co. of Am., 216 F.Supp.2d 1060 (C.D.Cal.2002) *(sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge);* Indianapolis Minority Contractors Assoc. Inc. v. Wiley, 1998 WL 1988826, at *7 (S.D.Ind. May 13, 1998) *(proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).*

Discussion: This case has a very good discussion on authenticating electronic data, such as email.

U.S. v. Tank, 200 F.3d 627 (9th Cir. 2000):

> In child pornography prosecution, the government made an adequate foundational showing of the relevance and the authenticity of third person's Internet chat room log printouts, though the third person had deleted nonsexual conversations and extraneous material to free space on his hard drive, where the third person explained how he created the logs, the logs appeared to be an accurate representation of the chat room conversations among members of chat room, the government established a connection between defendant and the chat room log printouts through use of his screen name, and the printouts were relevant to prove existence of and defendant's participation in conspiracy.
>
> Where the government, in child pornography prosecution, made prima facie foundational showing of authenticity of third person's Internet chat

room log printouts, the district court did not abuse its discretion by admitting the printouts into evidence, despite their incompleteness, and allowing the jury to decide what weight to give that evidence; where any deletions from third person's hard drive were made by him, not by the government, and nothing prevented defendant from recovering the deleted data, the deletions went to the weight of the evidence, not to its admissibility.

Perfect 10, INC v. Cybernet Ventures, Inc. F.Supp (C.D.Ca)

- Court follows Tank opinion on authentication of records, but discusses some other angles and cites a couple of contrary opinions.

U.S. v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000)

- Defendant's emails sent to individuals he falsely listed as references on application for research grant to National Science Foundation, asking them to tell NSF that he had their permission to use their names, were properly authenticated in fraud prosecution,; e-mails bore defendant's e-mail address and used defendant's nickname, and defendant followed up with phone calls making same request. E-mails were not hearsay, but admissions by party opponent.

State v. Love, 691 So.2d 620 (Fla. 5th DCA 1997):

- The state obtained an unsigned, six-page letter and contended that it was written by defendant. Holding that the contents of the letter established a prima facie case of authenticity, the court reversed the order that suppressed the letter from evidence and remanded. The court stated that evidence could be authenticated as required by Fla. Stat. ch. 90.901 (1995) by circumstantial evidence, and by appearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with the circumstances. Important circumstances that tended to prove the authenticity of a letter included the disclosure in the letter of information that was likely known only to the purported author. The court noted that information likely known only to defendant was contained in the letter, including references to conversations with a codefendant, descriptions of the evidence, statements of codefendants, and references to certain familial and social relationships. The court held that the trial court was limited to determining that the state had made a prima facie case of authentication, and that the ultimate issue of genuineness was for the jury to resolve.

United States v. Whitaker, 127 F.3d 595 (7th Cir. 1997):

Federal agent properly authenticated records of a narcotics business from a computer seized pursuant to a search warrant.

U.S. v. Simpson, 152 F.3d 1241 (10th Cir. 1998):

A computer printout of the alleged Internet chat room conversation between a Federal Bureau of Investigation (FBI) agent and a defendant later charged with receiving child pornography was admissible over the claim that it was not in the defendant's handwriting or writing style, and did not present his voice, and consequently was not authenticated; the contact gave the defendant's name and address, and the agent's e-mail and address, as given to the contact, was found on a piece of paper near the defendant's computer.

The trial court did not abuse its discretion by allowing excerpts from handwritten notes found near the computer of a defendant charged with receiving child pornography to be read into evidence; the portion of the notes setting forth the name and address of the Federal Bureau of Investigation (FBI) agent posing as a purveyor of child pornography was probative of the defendant's identity as the agent's contact, and the recitation of the names of various files, suggestive of sexual subject matter, was not unduly prejudicial.

In re: F.P., 878 A.2d 91 (PA. 2005):

Evidence was sufficient to authenticate internet instant messages as having originated from juvenile, and thus transcripts of these instant message conversations were admissible, in delinquency adjudication of juvenile for aggravated assault; juvenile referred to himself by his first name, he repeatedly accused victim of stealing from him, which mirrored testimony that juvenile was angry about a stolen DVD, he referenced fact that victim had approached high school authorities about the instant messages, and he repeatedly called victim vile names and threatened to beat him up.

People v. Downin, 828 N.E.2d 341 (Ill. 3rd DCA 2005):

Trial court did not abuse its discretion in admitting into evidence copies of e-mail allegedly written by defendant in trial for aggravated criminal sexual abuse; victim testified that she met defendant over the Internet and that they communicated via e-mail, when deputy suggested victim send an e-mail to defendant from the public safety building, she used the e-mail address for him that she had used on all prior occasions, and the reply e-mail was responsive to the e-mail victim sent.

A document may be authenticated by direct or circumstantial evidence,

and circumstantial evidence of authenticity includes such factors as appearance, contents, and substance

Prima facie authorship of a document may include a showing that the writing contains knowledge of a matter sufficiently obscure so as to be known to only a small group of individuals.

Knight v. State, 34 Fla. L. Weekly D2198 (Fla. 5th DCA 2009):

Victim's testimony was sufficient to authenticate a tape-recorded conversation between defendant and victim in prosecution for sexual activity with a child, where victim testified that she was a participant in the conversation, that she had listened to the tape before trial, that the voices on the tape were defendant's and hers, and that the tape fairly and accurately memorialized the conversation.

There is no definitive list of requirements that must be met to authenticate an audio tape, even though courts occasionally suggest these lists.

Computer Generated Information is Non-Hearsay:

United States v. Hamilton, 413 F.3d 1138 (10th Cir. 2005)

Computer-generated "header" information that accompanied each pornographic image that defendant was charged with uploading to Internet newsgroup was not "hearsay," given that header information was generated instantaneously by computer hosting newsgroup, without assistance or input of a person, such that there was neither a "statement" nor a "declarant" involved within meaning of rule's definition of "hearsay."

Avilez v. State, 36 Fla. L. Weekly D4 (Fla. 4th DCA 2010):

A hotel manager assigned a key card to an employee. When that card was found at the crime scene, the manager looked at the card and the key card records, and testified that the particular card had been assigned to the defendant. The manager's testimony was not hearsay because statement or reports not created by a person do not constitute hearsay.

R.L.G. v. State, 2021 WL 2446948, (Fla.App. 3 Dist., 2021)

Juvenile was held in indirect criminal contempt because a probation officer testified his GPS records showed he left his home. The officer did not present records or a detailed description of how the third party monitors the GPS. The majority cited numerous cases that say GPS data

by third parties is hearsay. The dissent cited numerous cases that say machine generated data is non-hearsay. Ultimately, the court ruled that since there was no testimony regarding whether there was human input or not, the case would be reversed. The records should have been introduced as business records. This case provides a good reference as to how to introduce such records.

Digital Imaging: Admissibility of

Kennedy v. State, (Fla. 4th DCA 2003):

The police took photographs of the bloody shoe prints and fingerprints that were later enhanced by two different computer programs. Neither computer program altered the evidence, created evidence, or changed the comparison methods used to match the evidence to a suspect. The appellate court held that the computer programs were merely enhancement tools. As a result, no Frye issue was created.

Necessity to Introduce Original Hard Drive at Trial

State v. Ballard, 276 P.3d 976 (N.M. App. 2012)

Defendant who was charged with sexual exploitation of children based on possession was not entitled to dismissal for lack of corpus delicti, even though the state did not present the hard drive on which the contraband images were discovered but, instead, introduced DVD copies of the image files, and defendant argued that the DVDs were made by an unidentified person from "another copy"; computer forensic analyst provided foundational evidence about the accuracy of a forensic copy of the hard drive, defendant had agreed with the process of copying the charged images to the DVDs so as to keep uncharged images from the jury, defendant did not present evidence of corruption or irregularity in any copying process, and even absent defendant's statements to police, there was abundant proof that defendant possessed child pornography on his hard drive.

FOURTH AMENDMENT ISSUES:

Agent of the Government- AOL and NCMEC

U.S. v. Keith, CRIMINAL ACTION NO. 11-10294-GAO

Federal district court ruled that AOL was not acting as an agent of the government when they detected child pornography files on their network, because they had a legitimate business purpose to do so. Case provides a

good description of how that process works.

Court ruled that NCMEC was acting as an agent of the government when they opened the file sent to them by AOL.

Morales v. State, 2019 WL 2528912, (Fla.App. 1 Dist., 2019)

Detective properly opened a child pornography image submitted by ChatStep based upon a Photo DNA hit even though ChatStep had not previously opened the file. Defendant had no reasonable expectation of privacy in a file he transmitted via ChatStep and the detective's actions did not substantially expand upon the private party search.

Arresting defendant in his home without a warrant

Payton v. New York, 100 S.Ct. 1371 (1980):

Facts: The defendant, Theodore Payton, was accused of murdering the manager of a gas station two days earlier. The police went to his home to arrest him. When they arrived, they saw lights inside and heard music playing. They forced the door open and learned Payton was not home. In plain view, however, they found a shell casing that was later used against Mr. Payton at trial.

Holding:

- Fourth Amendment to United States Constitution, made applicable to states by Fourteenth Amendment, prohibits police from making warrantless and nonconsensual entry into suspect's home in order to make routine felony-arrest.

- Officer's declaration of purpose to arrest defendant, when knocking on defendant's door, is unnecessary when exigent circumstances are present.

- Simple language of Fourth Amendment applies equally to seizures of persons and to seizures of property, and warrantless arrest of person is species of "seizure" required by amendment to be reasonable.

- For Fourth Amendment purposes arrest warrant founded on probable cause implicitly carries with it limited authority to open dwelling in which suspect lives when there is reason to believe suspect is within.

Discussion: This is a landmark case in search and seizure law. It

is interesting to note that New York had a statute authorizing a warrantless entry into a suspect's home for the purpose of arrest. The Supreme Court ruled that absent exigent circumstances, such an entry is unconstitutional. The Court also noted that if the officer had obtained an arrest warrant, they would have been able to enter the defendant's home for the purpose of an arrest. Please note that the Supreme Court ruled on a companion case, Riddick v. New York, in the same opinion. That case involved a robbery with a similar warrantless entry into the suspect's home.

Arresting defendant in doorway of his house

United States v. Santana, 96 S.Ct. 2406 (1976):

- A person standing in the doorway of a house is "in a public place," and hence subject to arrest without a warrant permitting entry of the home.
- When the defendant retreats into the home to avoid arrest, the officers may enter without a warrant to effect the arrest.

Cell Phone Search of Student at School

G.C. v. Owensboro Public Schools, 711 F.3d 623 (6th Cir. 2013):

The legality of a search of a student depends simply on the reasonableness, under all the circumstances, of the search, which involves a twofold inquiry: first, whether the action was justified at its inception, and second, whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place.

A student's use of a cell phone on school grounds, in violation of school policy, does not automatically trigger an essentially unlimited right enabling a school official to search any content stored on the phone that is not related either substantively or temporally to the infraction.

School officials' knowledge that, a year and a half earlier, a public high school student had expressed suicidal thoughts and had admitted that he smoked marijuana, combined with student's violation of school policy barring use of cell phones in classrooms, did not provide reasonable grounds for school officials, upon seizing the phone based on violation of the policy, to search the phone by reading student's text messages.

Consent Search Executed Outside Jurisdiction:

State v. Sills, 852 So.2d 390 (Fla. 4th DCA 2003):

Evidence supported trial court's conclusion that defendant's consent to search of his house was given to municipal police officers due to color of their office, as would support affirming trial court's suppression of evidence obtained from house, which was located outside officers' jurisdiction; waiver form used by officers had crest of municipal police department, officers transported defendant from sight of traffic stop within municipality to house using handcuffs, and possibility of more lenient treatment for cooperating with police was carrot that enticed defendant's actions.

Exigent Circumstances: Preventing Reentry to Defendant's Home:

Illinois v. McArthur, 121 S. Ct. 946 (2001):

Facts: Police officers, with probable cause to believe that respondent McArthur had hidden marijuana in his home, prevented him from entering the home unaccompanied by an officer for about two hours while they obtained a search warrant. Once they did so, the officers found drug paraphernalia and marijuana, and arrested McArthur.

Holding:

- The court found that the warrantless seizure was not per se unreasonable, since it involved exigent circumstances, and the restraint at issue was tailored, avoiding significant intrusion into the home itself. Consequently, the court balanced the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable. The court concluded that the restriction at issue was reasonable, and hence lawful. Police had probable cause to believe defendant's home contained unlawful drugs, and had good reason to fear that, unless restrained, defendant would destroy the drugs before they could return with a warrant. Also, police made reasonable efforts to reconcile their law enforcement needs with the demands of personal privacy, and they imposed the restraint for a limited period of time, two hours.

Exigent Circumstances: Seizing Suspect's Computer

United States v. Boozer, 2021 WL 78865 (D.Or., 2021)

Exigent circumstances did not justify law enforcement's warrantless seizure of defendant's computer; there was no imminent threat that evidence in question would be destroyed or that defendant had possession of evidence in question, defendant was not at home or in possession of computer, there was no evidence he had destroyed evidence in the past or was planning to do so, there was no evidence of ongoing criminal activity

by defendant, defendant's roommate gave agents open-ended invitation to remain inside apartment, agent testified computer was not connected to internet, there was no evidence defendant was capable of remotely destroying evidence, and agents had ample opportunity to seek warrant by electronic means.

Expectation of Privacy (see ECPA section for related cases)

Cloud Storage Accounts

United States v. Maclin, 2019 WL 2352557 (N.D.Ohio, 2019)

Defendant did not have reasonable expectation of privacy in file-sharing account and, thus, could not challenge a search of the account for child pornography under Fourth Amendment; defendant had no subjective expectation of privacy in the account, and, even if he had such expectation, e.g., based on the fact that it was password protected, it was not one society was prepared to recognize as legitimate, as the account was shared with multiple individuals.

Defendant challenged a search warrant on his Dropbox account. The court ruled that since he shared his login info with other CP users, he had not expectation of privacy in the account and thus, no standing to challenge the warrant.

Cell Site Data/Mobile Tracking Devices

Carpenter v. U.S., 138 S.Ct. 2206 (U.S.,2018)

1. An individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through CSLI;

2. Seven days of historical CSLI obtained from defendant’s wireless carrier, pursuant to an order issued under the Stored Communications Act (SCA), was the product of a “search”;

3. Government’s access to 127 days of historical CSLI invaded defendant’s reasonable expectation of privacy;

4. Government must generally obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier.

5. Johnson v. State, 2020 WL 6772596, at *1 (Fla.App. 4 Dist., 2020)
   Under Witt v. State, 387 So. 2d 922 (Fla. 1980), Carpenter was an evolutionary refinement in procedural law, not a development of fundamental significance that applies retroactively to cases on collateral review. Nor does federal law require retroactive application.

Bailey v. State, 2020 WL 6706904 (Fla. 1st DCA 2020)

Murder defendant had no objectively reasonable expectation of privacy in GPS records transmitted from his borrowed car to car owner's financing company such that law enforcement's warrantless acquisition of such records would constitute a "search" implicating the protections of the Fourth Amendment, even though GPS data was technically historical in nature; GPS records of the car's location during the commission of the offense were records of defendant's travels over public thoroughfares, car's owner consented to GPS tracking, and police played no role in recording the GPS information.

U.S. v. Jones, 132 S.Ct. 945 (2012)

Government's installation of Global–Positioning–System (GPS) tracking device on target's vehicle, and its use of that device to monitor vehicle's movements, constitutes a "search," within meaning of Fourth Amendment.

Trespass alone does not qualify as a "search," under Fourth Amendment, rather, it must be conjoined with attempt to find something or to obtain information.

Where Government obtains information by physically intruding on constitutionally protected area, "search" within original meaning of Fourth Amendment has occurred.

U.S. v. Skinner, 2012 WL 3289801 (C.A.6 (Tenn.))

Defendant did not have reasonable expectation of privacy in inherent location data broadcast from his cellular phone with known number that he had voluntarily used while traveling on public thoroughfares, and thus police could track that signal over three-day period without violating Fourth Amendment; while

cellular site information aided police in determining defendant's location, that same information could have been obtained through visual surveillance.

Police, using otherwise legal methods, may so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.

Tracey v. State, 2014 WL 2599917 (C.A.11 (Fla.))

Government's use of "real time" or prospective cell site location information (CSLI) to track location of defendant's vehicle on public roads did not violate Fourth Amendment; monitoring of CSLI occurred only when defendant's vehicle was on public roads, where it "could have been observed by the naked eye."

Government, in obtaining "real time" or prospective cell site location information (CSLI) to track location of defendant's vehicle, violated provision of statute permitting law enforcement officer to require provider of electronic communication service to disclose customer communications or records; application failed to offer "specific and articulable facts" to show that CSLI was relevant and material to ongoing criminal investigation, as required by statute, and application did not even seek court order for CSLI, only a pen register and a trap and trace.

Tracey v. State, 152 So.3d 504 (2014)

Defendant had subjective expectation of privacy in real time cell site location information (CSLI) regarding location of defendant's cellular telephone, as would support finding that police officers' use of CSLI to track defendant was a search falling under purview of Fourth Amendment.

A warrant supported by probable cause is necessary to obtain CSLI.

Email/Chat rooms

U.S. v. Forrester, 495 F.3d. 1041 (9th Cir. 2007):

Use of computer surveillance techniques that revealed the to and from addresses of e-mail messages, the addresses of websites visited by defendant, and the total amount of data transmitted to or from

defendant's internet account did not amount to a “search” in violation of the Fourth Amendment; e-mail and internet users had no expectation of privacy in the addresses of their e-mail messages or the addresses of the websites they visited, because they should know that such information was sent and accessed through their internet service provider and other third parties, and the addresses did not reveal the contents of communications.

Even if government's use of computer surveillance techniques to obtain to and from addresses for e-mail messages and the addresses of websites visited by the defendant was beyond the scope of the pen register statute, suppression of the evidence the government obtained through such surveillance was not available as remedy, in prosecution for conspiracy to manufacture ecstasy and related offenses, absent showing that the surveillance violated the law, or that suppression was remedy set forth in the pen register statute.

United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997):

Defendant had no reasonable expectation of privacy in an AOL chat room.

HN11The expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and recipient of the e-mail. E-mail messages sent to an addressee who later forwards the e-mail to a third party do not enjoy the same reasonable expectations of privacy once they have been forwarded. Similarly, messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy.

ISP Records

United States v. Horton, 863 F.3d 1041, 1047 (C.A.8 (Iowa), 2017)

Federal courts have uniformly held that ‘subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation’ because it is voluntarily conveyed to third parties

U.S. v. Perrine, 518 F.3d 1196, 1204 (C.A.10 (Kan.),2008)

Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation. (Case

provides a string of cases holding no REP in subscriber records.)

U.S. v. Cox, 190 F. Supp. 2d 330 (N.D.NY 2002):

> Defendant had no reasonable expectation of privacy in his AOL subscriber information.

Freedman v. American Online, Inc., 412 F.Supp.2d 174 (D.Conn.,2005)

> Internet service subscriber did not have objectively reasonable expectation of privacy in his non-content subscriber information, which thus was not entitled to Fourth Amendment protection, given that subscriber agreement expressly permitted Internet service provider (ISP) to reveal subscriber information when necessary for providing service requested, and also indicated that ISP would release information about subscriber's account to comply with valid legal process or in special cases involving physical threat to subscriber or others, and that Electronic Communications Privacy Act (ECPA) permitted ISP to voluntarily provide government with subscriber information. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2702(c)(5, 6).

U.S. v. Hambrick, 2000 WL 1062039, at *4 (C.A.4 (Va.),2000)

> While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish the e-mail account, which is non-content information.

Hacker Acting as Agent of the State

U.S. v. Jarrett, 338 F.3rd 339 (4th Cir. 2003):

> Government did not know of and acquiesce in anonymous computer hacker's illegal search of defendant's computer in a manner sufficient to transform the hacker into an agent of the government, as required for Fourth Amendment protections to apply to search; although hacker had similarly aided government in a pornography case seven months earlier and government, in series of e-mails, praised hacker for his efforts and assured hacker that he would not be prosecuted for his actions, the exchanges were

insufficient to create an agency relationship.

Social Network Sites

United States v. Irving, 2018 WL 4681631 (D.Kan., 2018)

Defendant ultimately charged with distribution of child pornography and possession of child pornography had reasonable expectation of privacy in social media account, and thus had standing to object to search of account, although social media provider's terms of service (TOS) generally stated that provider could collect data and information and that user should not post unlawful content, where TOS also stated that user owned all collected content and information and could control how to share it, statement about not posting unlawful content was in context of asking for user's help to keep platform "safe," and TOS lacked explicit terms about monitoring user's account for illegal activities and reporting those activities to law enforcement. U.S. Const. Amend. 4.

Stolen Computers

Duke v. State, 2018 WL 4374747 (Fla.App. 1 Dist., 2018)

Defendant's car was burglarized and three of his flash drives were stolen. The police subsequently arrested the burglar in a drug case and the burglar gave them the flash drives. The burglar stated he received the flash drives as payment for drugs. The burglar told them that he saw a video depicting a sexual battery on one of the drives. He showed them the video and then consented for them to search the drive. The defendant was subsequently arrested based on what was found on the flash drive.

The court ruled that viewing the video on the flash drive was not a search because it was repeating a search already conducted by a private party. The court also ruled that the burglar had apparent authority to consent to the search of the flash drive.

Hicks v. State, 31 Fla. L. Weekly D326 (2nd DCA 2006):

Defendant did not have reasonable expectation of privacy in contents of computer that he did not lawfully possess and to which he asserted no property or possessory interest; defendant did not contest initial traffic stop and failed to establish reasonable

expectation of privacy in stolen computer, although defendant stated at scene of traffic stop that his uncle gave him computer, defendant never introduced any evidence at suppression hearing, for example, how long he had used computer or whether he had any programs on it, and only officers testified at suppression hearing.

U.S. v. Caymen, 404 F.3d 1196 (9th Cir. 2005):

Defendant failed to show that he had acceptable expectation of privacy in laptop seized by police pursuant to search warrant, so as to establish his Fourth Amendment standing to seek to suppress evidence obtained by police's allegedly unlawful search of laptop's files, given that although he never conceded nor was convicted of wrongdoing in connection with laptop, defendant did not submit affidavit or other evidence supporting claim that he honestly bought and owned laptop.

"The Fourth Amendment does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that "society is prepared to accept as reasonable."

"Whatever possessory interest a thief may have, that interest is subordinate to the rights of the owner, and in this case, the business supply store, from which Caymen fraudulently obtained the computer, not only consented to the police examination of the laptop's hard drive, but also specifically requested that the police examine it before returning it, to protect the store from accidentally coming into possession of material the store did not want--like child pornography."

U.S. v. Wong, 334 F.3d 831 (9th Cir. 2003):

Defendant did not have standing to object to search of laptop computer that belonged to defendant's former employer, which search uncovered child pornography possessed by defendant, since defendant failed to establish that he had reasonable expectation of privacy in computer.

Virtual Currency Blockchains

United States v. Gratkowski, 964 F.3d 307 (C.A.5 (Tex.), 2020)

Defendant, who used virtual currency to purchase and download material from a child-pornography website, lacked a privacy interest in his information located on the virtual currency's blockchain, and thus, federal agents' use of software to analyze the blockchain and to identify users who downloaded material from the website did not violate the Fourth Amendment protection against unreasonable searches; users of the blockchain were unlikely to expect that the information published on the blockchain would be kept private, and while they enjoyed a greater degree of privacy than those who used other money-transfer means, it was well known that each transaction was recorded in a publicly available blockchain.

Defendant, who used virtual currency to purchase and download material from a child-pornography website, lacked a privacy interest in his information located on the virtual currency exchange that provided users with a method for transferring virtual currency, and thus, federal agents' use of software to analyze the information and to identify users who downloaded material from the website did not violate the Fourth Amendment protection against unreasonable searches; the currency exchange records were limited, did not provide agents with an intimate window into defendant's life, but rather, only provided information about defendant's virtual currency transactions, and transacting virtual currency through the exchange required an affirmative act on the part of the defendant.

Wireless Signals

United States v. Norris, 2019 WL 5688802 (C.A.9 (Cal.), 2019)

Child pornography defendant had no subjective expectation of privacy in the emission of the signal strength of the media-access-control (MAC) address of the devices in his apartment that reached outside his residence to connect, without authorization, to the internet by sending a wireless signal to password-protected wireless router in a neighboring apartment, for purposes of his claim that the government violated his Fourth Amendment rights by using wireless tracking software program designed to identify computers trespassing on wireless computer networks to capture signal strength readings and identify the address of his wireless devices; defendant's activities reached beyond the confines of his home, and agents made no physical intrusion into, and collected no information from inside defendant’s residence. (LEO used Moocherhunter)

Society generally is not prepared to recognize as reasonable a subjective

expectation of privacy in the content of property obtained through unauthorized means, for purposes of determining whether the property is subject to Fourth Amendment protections.

McClelland v. State, 2018 WL 3040509 (Fla.App. 2 Dist., 2018)

Defendant used neighbor's unsecured wireless router to download his child pornography. Detectives used a Yagi antenna to track defendant to his nearby trailer. Court ruled that defendant did not have a reasonable expectation of privacy in the data he broadcast for his illicit purposes.

U.S. v. Norris, Slip Copy, 2013 WL 4737197 (E.D.Cal.)

Use of Moocherhunter device to detect suspect's wireless signal location did not violate 4th Amendment. Officers did not trespass on suspect's property to obtain signal and suspect did not have reasonable expectation of privacy in signals he broadcast to public.

U.S. v. Saville, Not Reported in F.Supp.2d, 2013 WL 3270411 (D.Mont.)

Detectives traced P2P child porn to a wireless signal from a Comfort Inn. They used Gatekeeper and Shadow devices to hone in on the person using that IP connection to download child porn on the Gnutella network. Detectives obtained a pen register trap/trace order to capture the relevant data, including the word "Gnutella" that was included in a packet. Defense argued that detectives should have obtained a search warrant, especially since contents of communications were intercepted. The court ruled that the pen register trap/trace was sufficient and that the term "Gnutella" was automatically generated by the software as part of the connection process and therefore was not a communication.

U.S. v. Broadhurst, 2012 WL 5985615 (D.Or.)

The court made two important rulings.

1. There is no reasonable expectation of privacy when a suspect broadcasts information about his computer in the process of using his neighbor's unsecured wireless account. Therefor, the use of the Shadow device does not violate 4th Amendment.

2. The police violated the suspect's 4th Amendment rights when they

walked through his front yard to test the signal strength at a particular window of his house. Based on this trespass, the evidence was suppressed.

Lesson: You can use the Shadow device to establish probable cause, but don't venture beyond the sidewalk in front of the suspect's house.

Lesson 2. The court criticized the affidavit for not providing a better description of how the device works. The government tried to argue that a reading they took from the sidewalk was sufficient for PC even after the front window reading was excluded. The court rejected that argument because the affidavit did not describe any correlation between signal strength and distance. Just because the signal spiked when they went in front of his house is not enough for PC unless they can articulate measurements and distances etc...

U.S. v. Stanley, 753 F.3d 114 (3d Cir. 2014)

Defendant did not have reasonable expectation of privacy under Fourth Amendment in unauthorized wireless signal that disclosed his media access control (MAC) address, his private Internet Protocol (IP) address, or the fact that his wireless card was communicating with unsecured router at particular points in time.

Defendant did not have reasonable expectation of privacy in path of his unauthorized wireless signal to share child pornography over the Internet that had been deliberately projected to neighbor's unsecured wireless router, and thus tracking of that signal did not constitute a "search" under the Fourth Amendment; although government used electronic device to track signal from neighbor's unsecured wireless router to its source inside defendant's home, device did not reveal anything about content of data carried by that signal.

United States v. Stanley, 2012 WL 5512987 (W.D.Pa. Nov. 14, 2012)

Use of Moocherhunter to locate user of unsecured wireless network did not violate Fourth Amendment. Suspect had no expectation of privacy in the data he transmitted wirelessly. The owner of the router consented to the procedure.

Preventing Defendant From Entering House While Seeking Warrant

Illinois v. McArthur, 121 S.Ct. 946 (1999):

When police had probable cause to believe defendant had drugs in his home, preventing him from entering his home while a warrant was obtained was permissible under Fourth Amendment, given nature of intrusion and law enforcement interest at stake.

Search Incident to Arrest: Cellular Telephone

U.S. v. Finley, 477 F.3d 250 (5th Cir. 2007):

Police officers could search defendant's cell phone, including call records and text messages, incident to his arrest.

In the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a reasonable search under that Amendment.

In conducting a search incident to an arrest, police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial.

The permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person.

In general, as long as the administrative processes incident to an arrest and custody have not been completed, a search of effects seized from the defendant's person is still incident to the defendant's arrest.

U.S. v. Lasalle, (D. Hawai'I 2007):

"Because the search of Lasalle's phone was not roughly contemporaneous with his arrest, the "search incident to arrest" exception does not apply to the search." Phone was searched over two hours after arrest and at a different location.

Search/Arrest Warrants

Anticipatory Warrants:

US v. Grubbs, US 2006

Because the Fourth Amendment does not require that the triggering condition for an anticipatory search warrant be set forth in the warrant itself, the Court of Appeals erred in invalidating the warrant at issue here.

Anticipatory warrants are constitutional.

U.S. v. King, (3rd Cir. 2006):

> Anticipatory search warrant for residence of individual suspected of possession of child pornography was not facially unconstitutional by reason of omission from four corners thereof of specific language, contained in warrant affidavit, conditioning execution of warrant upon delivery of videotape, where warrant was governed by conditioning language in affidavit, particularity requirement of Fourth Amendment did not require that anticipatory search warrant explicitly mention conditions precedent to search, and warrant particularly described place to be searched and items to be seized.

Citizen Informant:

Redini v. State, 37 Fla. L. Weekly D673 (Fla. 4th DCA 2012):

> Supporting affidavit, based on information supplied to law enforcement by defendant's roommate, provided probable cause justifying a search warrant; roommate directly approached law enforcement and gave sworn statement regarding defendant's criminal conduct, and roommate's disclosure that he had been molested by defendant nine years earlier, coupled with his observation of defendant repeatedly observing child pornography and bragging about engaging in sex with young boys, supported inference that he was reporting defendant's behavior to protect other children and promote justice.

State v. Gonzalez, 884 So.2d 330 (2d DCA 2004):

> Defendants' daughters, who informed police about cocaine in safe located next to defendants' bed, qualified as "citizen-informants," rather than mere anonymous informants, for purposes of determining whether factual allegations in search warrant affidavit, including hearsay evidence provided by daughters' phone calls to police, provided sufficient probable cause for magistrate to issue warrant; daughters' identities were readily ascertainable because they gave their names and location, and there was no indication they were motivated by anything other than concern for the safety of their parents and others.

Dial v. State, 798 So.2d 880 (Fla. 4th DCA 2001):

> This case basically says that if a family member or someone with a potential grudge against the suspect provides the basis for pc to obtain a warrant, investigative steps need to be taken to confirm her reliability. When a disinterested citizen provides information to the police, there is a presumption of reliability, but when is an ex-girlfriend or disgruntled teenage son, you need to corroborate the testimony. We see these cases when the defendant's alienated wife or girlfriend calls the police and tells them there is child porn on his computer.

State v. Woldridge, 958 So.2d 455 (Fla. 2d DCA 2007):

> Internet service provider's compliance with federal law mandating that it report a subscriber's apparent violation of federal child pornography laws to National Center for Missing and Exploited Children (NCMEC) provided presumption of reliability akin to that afforded citizen informant, for purposes of determining whether probable existed for issuance of residential search warrant arising from provider's reports to NCMEC; provider was a recognized, well-established company that essentially witnessed the crime when it received images of child pornography from defendant subscriber in an attempted e-mail transmission.
>
> Search warrant affidavit relating that officer had received four reports from National Center for Missing and Exploited Children (NCMEC) stating that internet service provider had reported that computer user with specific screen name had attempted to e-mail files containing child pornography provided probable cause to issue warrant; tip came from provider, reliability of tip was presumed because of federal law compelling corporation to report to NCMEC, and provider was acting in manner analogous to that of citizen informant when it forwarded information to NCMEC.
>
> AOL, as required by federal law, provided its business record concerning content of specific e-mails from a specific subscriber to NCMEC for it to forward to law enforcement, and defendant offered no basis for trial or appellate court to conclude that these business records were unreliable.

Delay in Obtaining Warrant after Seizure

U.S. v. Laist, 702 F.3d 608 (11th Cir. 2012):

Government's 25-day delay in obtaining a search warrant after seizing suspect's computer based on probable cause that it contained child pornography was reasonable under Fourth Amendment; although suspect retained a possessory interest in computer, that interest was diminished by his opportunity to download personal and school documents he needed while computer was in government's possession, and government acted diligently in obtaining a warrant, as it began preparing warrant affidavit shortly after suspect revoked his consent to search computer and it included in affidavit a substantial amount of information regarding suspect's conduct.

A temporary warrantless seizure supported by probable cause is reasonable as long as the police diligently obtained a search warrant in a reasonable period of time.

In determining whether a temporary warrantless seizure was reasonable, courts consider the nature and complexity of the law enforcement investigation and whether overriding circumstances arose, necessitating the diversion of law enforcement personnel to another case, the quality of the warrant application and the amount of time such a warrant would be expected to take to prepare, and any other evidence proving or disproving law enforcement's diligence in obtaining the warrant.

Six-day period between government's submission of a warrant application to search suspect's computer for child pornography and a magistrate judge's issuance of warrant was not attributable to government in evaluating reasonableness of its delay in obtaining a warrant after seizing computer; attributing six-day period to government would not have an appreciable deterrent effect, since after submitting application, government's interests aligned with those of suspect, in that both wanted matter resolved promptly.

United States v. Shaw, 2012 U.S. Dist. LEXIS 32624 (N.D. Ga. February 10, 2012):

Defendant conceded his cell phones were properly seized, but the government’s 90 day delay in getting a search warrant for the cell phones were unreasonable and required suppression.

U.S. v. Laist, 2012 WL 6156278 (C.A.11 (Ga.)):

When determining whether a delay in obtaining a search warrant renders a seizure unreasonable under the Fourth Amendment,

courts evaluate the totality of the circumstances presented by each case.

In determining whether a temporary warrantless seizure was reasonable, courts consider the nature and complexity of the law enforcement investigation and whether overriding circumstances arose, necessitating the diversion of law enforcement personnel to another case, the quality of the warrant application and the amount of time such a warrant would be expected to take to prepare, and any other evidence proving or disproving law enforcement's diligence in obtaining the warrant.

Six-day period between government's submission of a warrant application to search suspect's computer for child pornography and a magistrate judge's issuance of warrant was not attributable to government in evaluating reasonableness of its delay in obtaining a warrant after seizing computer; attributing six-day period to government would not have an appreciable deterrent effect, since after submitting application, government's interests aligned with those of suspect, in that both wanted matter resolved promptly.

Government's 25-day delay in obtaining a search warrant after seizing suspect's computer based on probable cause that it contained child pornography was reasonable under Fourth Amendment; although suspect retained a possessory interest in computer, that interest was diminished by his opportunity to download personal and school documents he needed while computer was in government's possession, and government acted diligently in obtaining a warrant, as it began preparing warrant affidavit shortly after suspect revoked his consent to search computer and it included in affidavit a substantial amount of information regarding suspect's conduct.

States v. Stabile, 633 F.3d 219 (3d Cir.2011)

Government's three-month delay in obtaining state search warrant and searching seized hard drives was reasonable, despite defendant's claim that he required the hard drives for work; defendant did not ask for return of hard drives until eighteen months after their initial seizure and delay was due to lead case agent's assignment to Secret Service Detail protecting the President.

U.S. v. Mitchell, 565 F.3d 1347 (11th Cir. 2009)

Twenty-one day delay in obtaining search warrant for single hard

drive seized from desktop computer in home of defendant suspected of receiving and possessing child pornography was unreasonable under all the circumstances; detention constituted a significant interference with defendant's possessory interest that was not eliminated by admissions made by defendant which provided probable cause for seizure, and fact seizing Immigration and Customs Enforcement (ICE) special agent was scheduled to depart in two and one-half days for two-week training program in another state and was the only agent in office trained to conduct forensic examination of computer for child pornography was not compelling justification for delay.

Initial warrantless removal of hard drive from computer in home of defendant suspected of receiving and possessing child pornography did not violate Fourth Amendment.

People v. Shinohara, 375 Ill.App.3d 85, 872 N.E.2d 498 (2007):

Seventy-five day delay between seizure by police of child pornography defendant's computer and issuance of warrant authorizing police to search that computer did not render lawful seizure of defendant's computer unreasonable.

Delay in Forensic Exam after Consent to Search Cell Phone

U.S. v. Butler, 2020 WL 1429827, (M.D. Fla. Mar. 24, 2020)

Federal agents obtained consent to search suspect's cell phone for child pornography on May 2, 2018 and did not begin their forensic examination until June 26, 2018. Court ruled that although the time delay was not an unconstitutional violation, the better practice would be for the agents to obtain a search warrant, especially since it was a cell phone. The court cites various cases discussing delays in conducting searches after consent.

Execution of Warrants

Container: Computer is Just a Container of Evidence:

U.S. v. Giberson, 527 F.3d 882 (9th Cir. 2008):

Search warrant for defendant's residence that described particular documents and records to be seized authorized the seizure of a computer, while waiting to obtain a specific

warrant authorizing the search of the computer's files, where the searching law enforcement agents reasonably believed that documents and records specified in the warrant would be found stored in the computer.

While officers ought to exercise caution when executing the search of a computer, pursuant to a search warrant specifying documents and records, just as they ought to when sifting through documents that may contain personal information, the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement.

Law enforcement officers were not required to limit their search of defendant's computer files pursuant to search warrant authorizing a search for records related to state identification cards, driver's licenses, state seals, and photographs that could be used for fake identification cards, since there was no reasonable way to sort relevant and irrelevant files, and government was not required to rely on defendant's self-labeling of his files.

"Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer."

Discussion: This case has some good language concerning how a computer is just a container that stores the evidence sought and how we do not have to treat it in a special way just because it is technology and contains a larger amount of data. The case also contains a discussion regarding why the police do not have to limit their search to certain types of files. The court notes that files can be mislabeled, etc… so we cannot expect the police to rely on file names or types.

Jackson v. State, 18 So.3d 1016 (Fla. 2009):

Search of a locked safe in a motel room was encompassed in a warrant to search the motel room for several classes of

items, and thus an additional warrant for the safe was not required; all items specified in the warrant, which included documents, bank cards, and receipts, could fit inside the safe and would logically and reasonably be secured in a safe, and thus it was reasonable for the searching officers to search inside the safe for these items.

Delay in Obtaining Warrant After Seizure

People v. Shinohara, 375 Ill.App.3d 85, 872 N.E.2d 498 (2007):

Seventy-five day delay between seizure by police of child pornography defendant's computer and issuance of warrant authorizing police to search that computer did not render lawful seizure of defendant's computer unreasonable.

Experts Accompanying Search

Wade v. State, 544 So.2d 1028 (Fla. 2d DCA 1989):

Use of advisers to identify items encompassed by search warrant was permissible where objects of the search warrant were computer equipment and parts which required identification by persons familiar with the particular parts described in the warrant.

Fact that experts who aided law enforcement officers in identifying computer equipment and parts which were subject of search warrant were employees of the victim did not render the search invalid, despite claim of defendant that the seizure resulted in the hauling away of items which crippled his business.

United States v. Hill, F.Supp (C.D.CA 2004) **Computer**

- Police are free to hire experts to help them conduct a search.

Time for Execution

U.S. v. Veloz, 2015 WL 3540808 (D.Mass)

Ongoing off-site forensic examination of contents of cell phones, thumb drives, and computers seized pursuant to warrant from residence of defendant suspected of being involved in violent kidnapping crew did not implicate defendant's Fourth Amendment or due process rights; although reports reflecting ongoing analysis of seized data were generated approximately 18 months after search of residence, there was no dispute that government copied or attempted to copy data from devices almost immediately after their seizure, government acted reasonably in seeking outside expertise, and there was no allegation that wrongfully seized and later discovered material of exculpatory nature was willfully retained.
Fourth Amendment itself contains no requirements about when a search or seizure is to occur or the duration.

Computer searches are not, and cannot be, subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation, and a greater degree of care in their execution.

U.S. v. Ganias, 755 F.3d 125 (2d Cir. 2014) *rehearing granted*

"Instead, we consider a more limited question: whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. We hold that it does not."

Government's seizure and retention of a mirror image of a defendant's computer hard drive for two-and-a-half years after records covered by a search warrant had been separated was unreasonable under Fourth Amendment, given that seizure and retention included personal records that were beyond scope of original search warrant.

Fourth Amendment does not permit officials executing a warrant for seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations.

Exclusionary rule applied to government's seizure and retention of a mirror image of a defendant's computer hard drive; widespread seizure of files beyond scope of warrant resembled an impermissible general search, government agents were aware that they should have purged non-

responsive data after they completed their search for relevant files, benefits of deterrence were great, and costs of suppression were minimal in a prosecution for the nonviolent offense of tax evasion.

People v. Deprospero, 91 A.D.3d 39, 932 N.Y.S.2d 789, 2011 N.Y. Slip Op. 08421

Mere fact that, following seizure of computer, digital cameras, and other electronic equipment from his home, defendant had already pled guilty to possession of child pornography charge arising out of single pornographic image initially recovered from computer and had demanded that the seized property be returned did not prevent police, prior to returning the seized equipment to defendant, from conducting forensic examination thereof for other contraband, where forensic examination was conducted just about eight months after seizure, and there was no evidence of any bad faith on part of police or district attorney's office, or that defendant was prejudiced by delay; eight-month delay, in connection with large-scale child pornography investigation of defendant and other suspects, was not unreasonable under the Fourth Amendment.

Fourth Amendment did not provide for specific time limit in which a computer seized from defendant's home could undergo a government forensic examination after it was seized pursuant to warrant, but required only that subsequent search of computer occur within reasonable time.

Police who had seized computer, digital cameras, and other electronic equipment from defendant's home pursuant to warranted search had obligation to search this equipment for contraband prior to returning it to him; indeed, returning contraband, such as child pornography, to defendant would constitute a crime.

Once computer, digital cameras, and other electronic equipment was lawfully seized from home of individual suspected of downloading child pornography pursuant to valid search warrant, this individual lacked any legitimate expectation of privacy therein, and police did not have to apply for second warrant prior to performing forensic examination thereof, notwithstanding passage of more than

six months between seizure and forensic examination.

U.S. v. Koch, 625 F.3d 470 (8th Cir. 2010):

> Rule that search warrant not executed within 10 days of issuance no longer was valid was not implicated with regard to police officer's viewing of material on flash drive that had been lawfully seized eight months earlier under valid warrant; although viewing was for purpose other than that which had been listed in warrant, original search warrant had been executed on same day that it had been issued.

United States v. Cameron, 652 F. Supp. 2d 74 (D. Me. 2009)

> After timely execution of warrant authoring search of defendant's residence within ten days of issuance of warrant, continued forensic inspection of computer and discs seized pursuant to warrant for more than ten days after issuance of warrant did not violate Fourth Amendment, rule of criminal procedure requiring that warrant command the officer to execute warrant within specified time no longer than ten days, or condition of warrant itself requiring officers to return results of search to court within ten days, absent showing that the delay in conducting forensic inspection of seized items resulted in lapse of probable cause, that delay prejudiced defendant, or that delay was in bad faith in attempt to circumvent requirements of warrant or the law.

United States v. Mutschelknaus, 564 F. Supp. 2d 1072 (D.N.D. 2008) aff'd, 592 F.3d 826 (8th Cir. 2010)

> Neither the Federal Rules of Criminal Procedure nor the Fourth Amendment provides for a specific time limit in which a computer must undergo a government forensic examination after it has been seized pursuant to a search warrant.
>
> Forensic analysis of defendant's computer and electronic storage media took place within a reasonable time after execution of search warrant and thus did not violate the Fourth Amendment or the Criminal Procedure Rule requiring a search warrant to be executed in no more than ten days after its issuance; forensic analysis was completed within 60 days from when warrant was executed, which was within the period authorized by the search warrant.

U.S. v. Burgess, 576 F.3d 1078 (10th Cir. 2009):

> Forty-four day delay in conducting forensic search of hard drive of computer did not violate the Fourth Amendment; warrant to search was secured prior to hard drive being seized, nothing indicated that officers were not diligent in executing search, probable cause to search was unaffected by delay, and any delay was due to officer's efforts to make sure job was done right.
>
> The Fourth Amendment does not specify that search warrants contain expiration dates.
>
> A violation of the criminal procedural rule requiring an officer to execute a warrant within 10 days alone should not lead to exclusion of evidence unless (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the rule.

State v. Grenning, 142 Wash. App. 518, 174 P.3d 706 (2008) aff'd, 169 Wash. 2d 47, 234 P.3d 169 (2010)

> Search and seizure of defendant's computer hard drives was timely under rule of criminal procedure requiring officer to search person, place, or thing named in search warrant within specified period of time not to exceed 10 days, even though detective found two child pornography photographs more than 10 days after warrant was issued; police entered and searched defendant's residence within 10–day warrant requirement, detective searched information stored on imaged copies of defendant's hard drives, which stored permanent, static, and unchanging data, and due to nature of material seized, passage of time did not affect probable cause.
>
> Delay of police in examining information stored on copies of defendant's computer hard drives beyond 10–day deadline was reasonable, and thus, did not violate Fourth Amendment; detective had to search three hard drives and consult with expert to obtain specialized software in order to complete search, information on hard drives was not transitory, changeable, nor stale when detective reviewed copies, there was a significant amount of information on

hard drives and it was not realistic for detective to review it all in 10 days, probable cause continued to exist throughout detective's search, and police did not act in bad faith in executing warrant.

Fourth Amendment does not provide for a specific time limit in which a computer may undergo forensic examination after it has been seized with a valid search warrant.

People v. Shinohara, 375 Ill.App.3d 85, 872 N.E.2d 498 (2007):

Officer officially executed warrant by completely carrying out directions included in warrant when he made mirror image copy of child pornography defendant's hard drives using special software, and thus, subsequent examination of contents of hard drives 78 days later did not violate statute requiring execution of a search warrant within 96-hour time frame.

Purpose underlying statute requiring execution of search warrant within 96-hour time frame was not violated by any delay in examining hard drive of defendant's computer; record did not reflect that there was any less probable cause to believe there were images of child pornography on defendant's computer on day warrant was issued than on day officer completed his forensic analysis of mirror images of hard drives, defendant did not challenge integrity of evidence of child pornography by arguing evidence was tampered with or altered, and staleness ceased to be concern after evidence was lawfully seized.

A delay in the execution of a search warrant does not violate a defendant's right to be free from an unreasonable search absent a showing of the interim dissipation of probable cause or any prejudice to the defendant.

United States v. Syphers, 296 F.Supp 2d 50 (N.D.N.H 2003)

The court properly extended the amount of time the police had to execute the warrant to 12 months. The extension would have been cleaner if done under oath.

The court recognized the complexity of executing searches of computers and found that the 7 month period was not unreasonable.

The court also briefly discussed the issue of whether superimposing a penis on the mouth of a minor child is child pornography under Ashcroft. The court did not answer the question because the officers got the warrant before the Ashcroft v. Free Speech Opinion.

United States v. Aldahondo F.Supp (D.P.R. 2004)

Furthermore, the affidavit also provided an adequate explanation of the search strategy that requires removal of the computer and media for proper examination and recovery of the evidence it contains. When a search is conducted in a residence, which holds a higher expectation of privacy, an off-site examination of the evidence fosters privacy concerns more efficiently since agents should not be reasonably expected to spend more than a few hours searching for materials on-site nor should risk damaging the evidence because of time constrictions.

United States v. Al-Marri, 230 F.Supp 2d 535 (S.D. NY 2002)

"While seizing the computer for examination at the FBI office may have inconvenienced Al-Marri, the Court acknowledges that current technology does not permit proper on-site examination of computer files. Thus until such technology does become available, a complete seizure of the computer will be necessary, provided that proper safeguards are put in place to prevent problems such as evidence tampering. See Hunter, 13 F. Supp 2d at 583 ('Until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur.')"

United States v. Hernandez, 183 F.Supp. 2d 468 (D.P.R. 2002):

- Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant. In most cases the forensic examination of the computer will take place

at a different location than that where the computer was seized. The same principle applies when a search warrant is performed for documents. The documents are seized within the time frame established in the warrant but examination of these documents may take a longer time, and extensions or additional warrants are not required. The examination of these items at a later date does not make the evidence suppressible.

- In cases where a search warrant directs agents to seize broad categories of records, or even all records, courts have upheld the "carting off" of whole file cabinets containing pounds of unsorted paper, to be searched off-site. The rationale that searches can be executed off-site because of the volume of information has been extended to include computers. These and other cases express the proposition that, because off-site computer searches are reasonable, it may be necessary, by implication, for the return of the warrant to be filed with the court before such off-site searching can be completed. Courts have recognized that the search of computer data involves more preparation than an ordinary search and a greater degree of care in the execution of the warrant; and that the search may involve much more information.

United States v. Habershaw, F.Supp. (Mass.)

- "The execution of the warrant, namely the seizure of the electronic evidence took place well within the ten days allowed. Further forensic analysis of the seized hard drive image does not constitute a second execution of the warrant or a failure to "depart the premises" as defendant claims, any more than would a review of a file cabinet's worth of seized documents.

U.S. v. Triumph Capital Group, Inc., 211 F.R.D 31 (D.Conn 2002)

The purpose of time limitation in criminal procedure rule governing searches is to prevent a stale warrant; delay in executing a warrant beyond the time set forth in the rule is not unreasonable unless, at the time it is executed, probable

cause no longer exists and the defendant demonstrates legal prejudice as a result of the delay.

Special agent was not required to complete forensic examination of computer's hard drive within the time period required by criminal procedure rule for return of the search warrant.

Removing Computer to Search Off-Site

United States v. Hill, (9th Cir. 2006) **Computer**

- Warrant was not overbroad for allowing police to seize all storage media to examine later.
- Police were not required to preview computer disks on site before removing them from home.
- Police were not required to bring equipment to search site that would allow them to preview evidence before removing it from site.
- Police are free to hire experts to help them conduct a search.
- Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." United States v. Hunter, 13 F.Supp.2d 574, 583 (D.Vt.1998). Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
- In child pornography prosecution, although search warrant was overbroad in authorizing a blanket seizure of defendant's computer equipment and files in the absence of an explanatory supporting affidavit, which would have documented the informed endorsement of the neutral magistrate, the exclusionary rule did not require the suppression of pornographic evidence within the scope of the warrant; the officers' wholesale seizure was flawed because they failed to justify it to the magistrate, not because they acted unreasonably or improperly in executing the warrant and the officers were motivated by considerations of practicality rather than by a desire to engage in indiscriminate fishing.

  Discussion: The defendant argued that the police were unreasonable in seizing storage media at defendant's home and taking it back to the lab for analysis because they should have

determined whether each disk contained child pornography prior to seizing it. The court recognized that it is frequently impracticable to do an on-site search because of the complexities of computer searches. The court ruled, however, that the police should specify in the affidavit why they must remove the storage media. The court ruled that the police were in error for not describing the complexities in their warrant, but the evidence was not suppressed because the officers acted in good faith.

U.S. v. Albert, 195 F.Supp. 2d 267 (D.Ma. 2002):

"The First Circuit upheld the off-site search of the computer and computer disks finding that "it was about the narrowest definable search and seizure reasonably likely to obtain the images." *Id.* at 535. As in *Upham*, here the mechanics of searching a hard drive by viewing all of the information it contains cannot readily be accomplished on site. The off-site search was therefore appropriate and constitutional."

Necessity to Attach Affidavit:

State v. Gayle, 573 So.2d 968 (Fla. 5th DCA 1991)

Search warrant which is valid on its face needs no affidavit attached; however, defective warrant can be cured by affidavit which is referenced in warrant and which is physically attached to warrant.
Affidavit or other proof which sets forth facts to establish probable cause for issuance of search warrant must be submitted to magistrate; search warrant itself need not recite or repeat facts recited in affidavit.

Failure to attach affidavit to valid search warrant does not make warrant defective.

Perez v. State, 521 So.2d 262 (Fla.App. 2 Dist.,1988)

Executing officer's failure to attach supporting affidavit to facially valid search warrant did not render warrant defective.

Necessity to Provide Warrant to Subject Before Search

U.S. v. Grubbs, 547 U.S. 90, 126 S.Ct. 1494 (2006)

> Neither the Fourth Amendment nor rule governing issuance of search warrants imposes requirement that the executing officer present the property owner with a copy of the warrant before conducting his search.
>
> Constitution protects property owners not by giving them license to engage the police in a debate over the basis for search warrant, but by interposing, ex ante, the deliberate, impartial judgment of a judicial officer between the citizen and the police, and by providing, ex post, a right to suppress evidence improperly obtained and a cause of action for damages.

State v. Henderson, 253 So. 2d 158, 159 (Fla. Dist. Ct. App. 1971)

> If an original search warrant was duly signed by the proper officer and was read to the defendant in toto before the search was commenced, the act of leaving an unsigned and undated duplicate of the original search warrant is solely an administerial act and not such error as would be prejudicial. State v. Featherstone, Fla.App.1971, 246 So.2d 597. Accordingly, the ruling of the trial court suppressing the evidence is reversed and this cause is hereby remanded to the trial court. This decision assumes that an original search warrant was duly issued by the proper officer pursuant to Officer Hobson's testimony and that said warrant was read to the defendant in toto. The production of the original warrant and the reading of same rests upon and is the burden of the State to prove within the law upon the trial of this cause.

Harden v. State, 433 So.2d 1378 (Fla. 2d DCA 1983):

> We are inclined toward what we perceive to be the majority rule. The failure to serve a proper copy of the search warrant at the time of execution has no effect upon the constitutional imperatives for its issuance and does not diminish the reliability of the evidence seized. The appellant has made no showing of prejudice in the failure to serve him with a complete copy of the search warrant. There is no indication that he asked for the balance of the

warrant or even realized that his copy was incomplete. We do not suggest that the requirement for serving a copy of a search warrant is unimportant, but where, as here, there was no prejudice in the failure to do so, justice would not be served in imposing an exclusionary rule upon the items seized.

Knock and Announce

State v. Herstone, 633 So.2d 110 (Fla. 2d DCA 1994):

Police officers who used deception to gain peaceable entry to premises were not required to comply with "knock and announce" requirement for execution of search warrant; uniformed officer knocked on defendant's door, when defendant answered, officer told him that friend of his was outside in drunken state and that officer needed defendant to identify him, defendant and officer walked to police vehicle where second officer informed defendant that they had search warrant for premises, and defendant and officers then returned to premises and went inside.

Officer can be Affiant Out-of Jurisdiction

State v. Stouffer, 2018 WL 2331855 (Fla.App. 4 Dist., 2018)

Officer can be affiant for search warrant in another county.

The key provision is that the judge must "have the application of some *person for said warrant duly sworn to and subscribed."* F.S. 933.06

United States v. Huntoon, 2018 WL 1474428, (D.Ariz., 2018)

State police obtained a search warrant for defendant's computer in child pornography case. Two years later, the feds brought defendant to trial and asked for a copy of the defendant's computer. Defendant argued that they needed a separate warrant to examine the State's copy. The appellate court ruled that the defendant's right to privacy had already been eliminated by the State search. As long as

the feds only looked at what the State agents viewed, all was good.

U.S. v. Cartier, 543 F.3d 442 (8th Cir. 2008):

The absence of particular search strategy for search of defendant's computer for images of child pornography did not render the search warrant invalid per se, absent showing that defendant was prejudiced by search of unrelated files or that any unrelated files were actually searched.

Morris v. State, 622 So. 2d 67 (4th DCA 1993)

The police obtained a search warrant to search a doctor's office for evidence of Medicaid fraud. The officer directed to execute the warrant waited in the lobby of the office as members of the Auditor General's office collected the evidence. The court ruled that the officer was not sufficiently involved in the execution of the warrant and the evidence was suppressed.

"Under the statute, the officer authorized by the warrant to conduct the search and seize the evidence designated must participate in or supervise the search even where he requires the assistance of others to do so. While the level of supervision and participation may vary depending upon the circumstances, it is absolutely essential that the officer authorized be present when and where the search is conducted and carry out his responsibility to see that the warrant is properly executed and that its authorization is not exceeded. It is not enough that the authorized officer wait in another room while the search is conducted by others."

Expert Search Warrants

United States v. Payne, 341 F.3d 393 (5th Cir. 2003):

Facts: Witness informed police that her bail bondsman had her exchange sex for bond payments and posted naked pictures of her on the Internet. She also said he showed her pictures on his office computer of young girls posing in sexually provocative ways. A trash pull at the defendant's office revealed a few such images. The

police obtained a search warrant to search the defendant's home and computer. The nexus between the offense and the defendant's home was established by the officer's general allegations that people who sexually exploit children often keep mementos at their home. Child pornography was found on his home computer. The defense argued that the evidence should be suppressed because there was no probable cause to believe the requested evidence would be found in the home. All evidence described was at the defendant's place of work.

Holding: "Payne, emphasizing the fact that this was Agent Sutherland's first child sexual exploitation investigation, urges us to disregard the so-called boilerplate language of the affidavit asserting that evidence of child sexual exploitation is often kept in the home of the perpetrator. This generalization stated what Agent Sutherland learned in training and what more experienced officers assisting him had learned in practice. n2 Agent Sutherland's training taught him that people who sexually [*11] exploit children tend to be "collectors" who keep evidence of the exploitation at home, in their vehicles, and at their workplaces. [HN6] Generalizations in an affidavit regarding the likely location of evidence will not undermine the reasonableness of reliance on the warrant. See United States v. Broussard, 80 F.3d 1025, 1034 (5th Cir. 1996). While the generalization alone might be insufficient to render official reliance reasonable, other facts in the affidavit taken together with generalizations founded upon training and experience could support reasonable reliance. See id. at 1034-35."

Discussion: The court only addressed the good faith exception in this case. They reasoned that if the good faith exception applied they did not need to directly address the probable cause issue. With that being said, the court itemized the various aspects of the affidavit that pointed to probable cause.

Cano v. State, 29 Fla. L. Weekly D1619 (Fla. 2d DCA 2004):

In affidavit supporting the warrant, a police officer wrote regarding the characteristics of people who use computers to disseminate child pornography. The evidence would likely have been inadmissible character evidence, but the fact that such evidence was included in the affidavit does not make the warrant illegal. Expert evidence that might not meet a Frye standard may be considered in evaluation whether a warrant establishes probable cause.

Burnett v. State, 28 Fla. L. Weekly D1179 (Fla. 2d DCA 2003):

> Conviction of possession of child pornography based on images on computer and diskettes seized in defendant's bedroom reversed where affidavit in support of search warrant failed to set forth crime-specific facts regarding defendant's probable possession of child pornography and the likelihood that it would be found on the computer and diskettes.
>
> Although affidavit properly stated that videotape seized in prior consensual search of defendant's bedroom substantiated allegations of defendant's lewd or lascivious conduct with children, the videotape corroborated only those initial charges and nothing more.
>
> Affidavit failed to describe a factual link between the video camera and the functioning capability of the computer so that images could be transferred, and omitted any factual averment that the computer was linked to the Internet or that the video camera was compatible with the computer so that images could be downloaded, transferred, or transmitted.
>
> Although affiant averred in general terms her experience in investigations involving crimes against children, affiant failed to describe any personal experience with child pornography from which her conclusions concerning defendant were derived.
>
> Discussion: The suspect videotaped two boys engaged in lewd conduct. During a consent search of the defendant's home, the detective found the videotape containing the alleged lewd conduct. Based on this finding, the detective sought a warrant to search the defendant's home and computer for more child pornography. The detective alleged that based on her expertise, the defendant would have child pornography on his computer.
>
> Even though this case ruled against the State, it is a helpful resource for us because it explains how the affidavit could have been done correctly. The court discussed two basic problems in the detective's affidavit. The first problem concerned her expertise in child pornography investigations. She detailed her expertise in child sex abuse investigation, but did not detail her training and experience in child pornography and the habits of child pornographers. The court implied that she could have remedied this by either elaborating on her specific expertise in child pornography *or* by listing the works of other experts in the field. Since she did neither, the affidavit was deemed insufficient.

The second major concern of the court was the detective's conclusory statement that the computer contained child pornography. The court noted that the detective did not state whether the computer was connected to the Internet or whether it had the capability to connect to the video camera. In conclusion, the affidavit could have been sufficient, but wasn't. The actual language from the detective's affidavit is included in the opinion.

Good Faith Exception

U.S. v. Flanders, 468 F.3d 269 (5th Cir. 2006):

Even if warrant for search of defendant's computer for evidence of child pornography possession was not supported by probable cause, police officers' reliance on warrant was objectively reasonable, and thus, good-faith exception to exclusionary rule applied; although police officer stated in affidavit in support of warrant that he knew that persons who sexually abused children also collected and kept child pornography, affidavit also contained statements of defendant's wife that defendant had taken digital photograph of his naked two-year-old daughter and that defendant used computer to view adult pornography, daughter's statements to forensic interviewer indicating defendant had licked her genitals, and information that defendant communicated on Internet about his sexual contact with daughter.

Language for Search Warrant:

United States v. Campos, 221 F.3d 1143 (10th DCA 2000):

"Additionally, the affidavit presented by an FBI agent in support of the warrant provided an explanation of the ways in which computers facilitate the production, communication, distribution, and storage of child pornography. Moreover, the FBI agent provided an explanation as to why it was not usually feasible to search for particular computer files in a person's home:

Computer storage devices .. can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and

> Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The wide variety of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data.... Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code embedded into the system as "booby trap"), the controlled environment of a laboratory is essential to its complete analysis."

Scope of Warrant: Exceeding

U.S. v. Perez, Slip Copy, 2015 WL 3498734 (E.D.Pa.)

> Agent's use of FTK software to scan and organize files did not exceed scope of search warrant in child pornography case.
>
> Previewing multiple files to see if they contained relevant evidence did not exceed scope of warrant.

U.S. v. Schlingloff, 2012 WL 5378148 (C.D.Ill.)

> Agent exceeded the scope of a search warrant for evidence of passport fraud when he activated a filter that would also seek out known child pornography on the computer and subsequently viewed some of the files that were discovered. Getting a subsequent search warrant to continue looking for child pornography did not cure the problem.

U.S. v. Farlow, 2012 WL 1957990 (C.A.1 (Me.))

> Police officers' search of suspect's computer for evidence of dissemination of indecent materials to minors or endangering welfare of child did not exceed scope of warrant, authorizing search of suspect's home for computers, software, and specifically-listed computer equipment, operational materials, and records or data, even though officers conducted gallery-view search that detected child pornography rather conducting more limited hash-value search, where suspect could have manipulated hash values, and limited hash-value search would not have turned up any chat transcripts or other evidence of enticement of minors.

U.S. v. Koch, 625 F.3d 470 (8th Cir. 2010):

Police officer acted in good faith by opening flash drive file and unexpectedly discovering child pornography eight months after executing valid search warrant for gambling materials, and thus did not exceed scope of warrant, where officer, after seeking advice from county attorney's office, was in process of following court order for disposal of property seized under warrant and checking for any gambling material on flash drive and officer did not prolong viewing but closed drive within just few minutes and obtained new search warrant and then looked at computer and examined bulk of flash drive.

U.S. v. Payton, 573 F.3d 859 (9th Cir. 2009):

Search of suspect's computer exceeded scope of warrant permitting search of his residence for evidence of narcotics sales and did not meet Fourth Amendment standard of reasonableness, and thus evidence obtained from computer was not admissible in suspect's prosecution for possessing child pornography, even though warrant permitted seizure of "[s]ales ledgers showing narcotics transactions" and "[f]inancial records," where warrant did not explicitly authorize search of computer, search produced no evidence of drug sales, and search of computer preceded any attempt to secure computer and seek second warrant.

"Our confidence in our conclusion is buttressed by contemplating the effect of a contrary decision. In order to uphold the search in this case, we would have to rule that, whenever a computer is found in a search for other items, if any of those items were *capable* of being stored in a computer, a search of the computer would be permissible. Such a ruling would eliminate any incentive for officers to seek explicit judicial authorization for searches of computers. But the nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests."

U.S. v. Giberson, 527 F.3d 882 (9th Cir. 2008):

Search warrant for defendant's residence that described particular documents and records to be seized authorized the seizure of a computer, while waiting to obtain a specific warrant authorizing the search of the computer's files, where the searching law enforcement agents reasonably believed that documents and records specified in the warrant would be found stored in the

computer.

While officers ought to exercise caution when executing the search of a computer, pursuant to a search warrant specifying documents and records, just as they ought to when sifting through documents that may contain personal information, the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement.

Law enforcement officers were not required to limit their search of defendant's computer files pursuant to search warrant authorizing a search for records related to state identification cards, driver's licenses, state seals, and photographs that could be used for fake identification cards, since there was no reasonable way to sort relevant and irrelevant files, and government was not required to rely on defendant's self-labeling of his files.

"Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer."

Discussion: This case has some good language concerning how a computer is just a container that stores the evidence sought and how we do not have to treat it in a special way just because it is technology and contains a larger amount of data. The case also contains a discussion regarding why the police do not have to limit their search to certain types of files. The court notes that files can be mislabeled, etc… so we cannot expect the police to rely on file names or types.

U.S. v. Graziano, --- F.Supp.2d ----, 2008 WL 789886 (E.D.N.Y.)

Manner and method of search of arson defendant's computer, seized pursuant to search warrant covering gambling records, and discovery during such search of materials related to arson, was reasonable, despite fact that search was not limited to files and documents related to gambling on their faces, where forensic examiner engaged in cursory review of files and documents, by

opening them, to determine whether they contained evidence of illegal gambling within scope of warrant, and file containing arson reference also contained reference to "rico," within scope of permissible search.

Warrant authorizing search of arson defendant's computers was not constitutionally required to specify search methodology or limit search of computers to certain keywords or terms.

Warrant for search of arson defendant's computer was sufficiently specific, where warrant established probable cause to believe that defendant's home, including any computer therein, would contain evidence of gambling records, and search warrant particularized that it was limited to such gambling records, whether in paper or electronic form.

"Defendant argues that the warrant is facially overbroad and invalid because it did not require a certain search methodology or limit the search of **computers** to certain keywords or terms, the Court finds that argument unpersuasive. There is nothing in the language of the Fourth Amendment, or in the jurisprudence of the Supreme Court or the Second Circuit, that requires such a rule in the context of a search of **computers**."

U.S. v. Triumph Capital Group, Inc**.** 211 F.R.D 31 (D.Conn 2002): **Computer**

Where a search exceeds the scope of a warrant, the general rule is that only the improperly seized evidence will be suppressed; the properly seized evidence remains admissible.

The drastic remedy of blanket suppression of all seized evidence is not justified unless the agent executing the search warrant effected a widespread seizure of items not within the scope of the warrant and did not act in good faith.

Egregious, callous, and reckless conduct in execution of search warrant must be shown to justify blanket suppression of all seized evidence.

Flagrant disregard justifying blanket suppression is found only in extraordinary cases such as those where the government effects a widespread seizure of items clearly not within the scope of a warrant and does not act in good faith, or when the lawful basis of a warrant was a pretext for the otherwise unlawful aspects of a

search.

A search is not rendered invalid merely because agents seize items that are outside the scope of the warrant; the search must actually resemble a general search.

Blanket suppression of all evidence seized in search of computer's hard drive was not justified on ground that search warrant was executed in a manner that resembled a general exploratory search and in flagrant disregard of the warrant; evidence did not establish indiscriminate rummaging through the hard drive or a widespread, grossly excessive seizure of data and documents clearly outside the scope of the warrant.

U.S. v. Adjani, 452 F.3d 1140 (9th Cir. 2006):

Probable cause for search warrant of extortion suspect's residence for instrumentalities of the extortion extended to permit search of computer found in residence, but owned by third-person; agent's were acting pursuant to valid warrant to look for evidence of a computer-based crime, agents searched computers at residence to which suspect had apparent access, and third-person's involvement with suspect was described in search warrant affidavit.

U.S. v. Smith, 459 F.3d 1276 (11th Cir. 2006)

Search of premises and lockbox pursuant to warrant authorizing officers to search for and seize evidence of illicit drug activity was valid, and seizure of pornographic photographs of minor children was legitimately conducted pursuant to plain view doctrine; warrant specifically authorized officers to seize "photographs that would be probative to establish residency," officers, alerted to lockbox by narcotics dog, were justified in searching it for evidence of drugs or photographs, and it was immediately apparent to officers, i.e., they had probable cause to believe, that among what they found in lockbox was evidence of crime of child pornography.

United States v. Gleich F.Supp (2003):

B. THE OFFICERS DID NOT EXCEED THE SCOPE OF THE FIRST SEARCH WARRANT

Gleich contends that the February 6, 2003, search warrant authorized the seizure of only one computer and that the seizure of

three computers grossly exceeded the scope of the search warrant. Gleich also contends that the search warrant did not authorize the examination of the files stored within the computer or on the discs found at his residence. The Government responds that all the computers were covered by the search warrant.

"The requirement that a search warrant describe its objects with particularity is a standard of 'practical accuracy' rather than a hypertechnical one." United States v. Peters, 92 F.3d 768, 769-70 (8th Cir. 1996) (quoting United States v. Lowe, 50 F.3d 604, 607 (8th Cir. 1995)). HN5The wording of a search warrant and the known circumstances giving rise to the search may lead reasonable law enforcement officials to believe that the items seized [*13] were of such an incriminating nature as to constitute contraband or evidence of criminal activity. Walden v. Carmack, 156 F.3d 861, 873 (8th Cir. 1998). "The mere fact that the items seized were not described in the warrant does not justify their suppression." United States v. Golay, 502 F.2d 182, 184 (8th Cir. 1974).

While Agent Pfenning may have anticipated finding only one personal computer in Gleich's home, the Court does not read the search warrant so narrowly as to limit the search and seizure to only one computer. The February 6, 2003, search warrant clearly authorized law enforcement officers to search Gleich's home and personal computer and to seize the items that could contain "Photographs, pictures, visual representations, or videos in any form that include sexual conduct by a minor, as defined by N.D.C.C. 12.1-27.2-01(4)" described in Exhibit A. All three personal computers were found in Gleich's home, and all three computers could have contained the items described in Exhibit A. Thus, the Court finds that the officers did not exceed the scope of the February 6, 2003, search warrant when they seized three personal computers from Gleich's [*14] home. Gleich's other contention that the February 6, 2003, search warrant did not authorize a search of the computer files found on either the computers themselves or the discs found at his residence is without merit. The February 6, 2003, search warrant clearly authorized the search of the computer and the computer files contained within the computer and on the additional discs found at the Gleich residence. Any other interpretation of the search warrant would be nonsensical. Thus, the Court expressly finds that the February 6, 2003, search warrant authorized the forensic examination undertaken by Agent Erickson.

U.S. v. Horn, 187 F.3d 781 (8th Cir. 1999):

Officers did not exceed scope of warrant by seizing defendant's video collection in its entirety for examination elsewhere, since officers could not practically view more than 300 videos at the search site, tapes could contain evidence of material related to defendant's contact with woman in Texas regarding child pornography, and officers could not immediately identify which videos were most likely to fit description of items that they were authorized to seize, especially given postal service official's testimony that individuals sometimes splice segments of child pornography into commercial tapes.

Plain View

Arizona v. Hicks, 107 S.Ct. 1149 (1987):

Officer's actions, in moving stereo equipment in order to locate serial numbers and determine if equipment was stolen, constituted "search," notwithstanding that officer was lawfully present within apartment where equipment was located in plain view. Probable cause was necessary to justify moving equipment to view serial number.

Discussion: Keep this in mind when searching for computer data or images. Opening a file or directory is considered a search and the contents found therein are not in plain view. Probable cause or valid consent must be prior to opening the file or directory.

U.S. v. Stabile, 633 F.3d 219 (3rd Cir. 2011)

List of computer files with lurid names were in plain view for purposes of determining whether seizure of such files was lawful under Fourth Amendment; detective did not violate the Fourth Amendment in highlighting folder containing the files, incriminating character of the files was immediately apparent, and detective had a lawful right of access to the object of the search because he was authorized by a state search warrant to search the hard drive for evidence of defendant's financial crimes.

United States v. Gray, 78 F.Supp.2d 524 (E.D. Virginia, 1999):

Under plain view doctrine, FBI agent's viewing of subdirectories in defendant's computer which turned out to contain suspected child pornography was within scope of search warrant which sought unrelated evidence of "hacking" or unauthorized entry into government agency library, where agent opened subdirectories in

course of systematic search for evidence of hacking, and did not abandon original search upon inadvertent discovery of pornography files in order to begin unauthorized search; agent was entitled to examine each subdirectory, at least briefly, to determine if it was covered by warrant.

Discussion: This case basically allows the investigator or analyst to view every file on a computer. The court recognized that files may be intentionally mislabeled to hide their content and consequently, the investigator is allowed to briefly view each file in order to determine if it is relevant under the warrant.

The main point stressed by the court, however, is that the investigator never abandoned his original search for evidence of hacking. The investigator was systematically viewing the contents of every directory according to procedure. He did not specifically focus on the "Teen" or "Tiny Teen" directories. After completing his search for hacking data, a subsequent warrant was obtained to search for more pornography. The court distinguished this case from United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), where that court held that the investigator impermissibly searched for additional child pornography after he found his first picture while executing a warrant on a narcotics case. The distinction lies in the fact that the investigator in Carey abandoned his original search and shifted his focus to child pornography. In the instant case, the investigator never abandoned his search for hacking material, but continued to give each file a cursory review for relevant evidence. If he happed to view more child pornography, it was legitimately in plain view.

U.S. v. Wong, 334 F.3d 831 (9th Cir. 2003):

Child pornography discovered on defendant's computer during search for evidence linking defendant to his girlfriend's murder, pursuant to warrant, was in plain view; police were lawfully searching for evidence of murder in graphics files that they had legitimately accessed, and where child pornography was located, and incriminating nature of files containing pictures of children as young as age three engaged in sexual acts was immediately apparent.

Misleading or Omitted Facts in Affidavit:

U.S. v. Craighead, (9th Cir. 2008)

Defendant charged with transportation, shipping, and possession of

child pornography was not entitled to an evidentiary hearing on his claim that search warrant affidavit contained false information, absent allegation of false or misleading statement in affidavit; statement in affidavit that two files from defendant's IP address were downloaded by affiant did not suggest that the files were downloaded from defendant's computer and affidavit never stated that such files were found on defendant's computer, affiant did not commit misleading omission by failing to include general knowledge about computer hacking that might have supported theory that defendant might not have downloaded to his own computer the files that affiant downloaded from defendant's IP address, and list of other files available for download from defendant's IP address did not amount to an averment that affiant knew that such files actually existed on defendant's computer.

Case also includes extensive analysis regarding when officers must read Miranda when interviewing defendant during execution of search warrant.

Return and Inventory

US. v. Franklin**,** 2013 WL 4442030 (W.D.Ark.)

Next, the Court finds that, although the search warrant was returned past the time set forth in the warrant, the delay was not unreasonable under the circumstances nor did the delay prejudice Defendant. The Court will not suppress the evidence obtained through the search warrant based only on a non-prejudicial, technical violation of the issuing judge's order, especially where the Government has a reasonable explanation for the delay.

State v. Musselwhite, 402 So.2d 1235 (Fla. 2d DCA 1981):

Absent showing of prejudice, a defect in postseizure procedure does not render execution of warrant illegal; hence, failure to list seized automobile and its contents on return of inventory did not void the warrant.

State v. Featherstone, 246 So.2d 597 (Fla 3rd DCA 1971)

Statute providing that no warrant shall be issued in blank, and that any such warrant shall be returned within ten days after issuance thereof, did not make void, due to subsequent failure of officer to make return thereon, warrant which had been executed; while it was duty of officer serving search warrant to make due return

> when same was served, failure to do so would not have a retroactive effect so as to render void a search that was valid at time it was made where defendant failed to show that he was prejudiced by the late return

Florida Op.Atty.Gen., 1953-54, p.

> The requirement in this section that inventory and receipt of seized property be made is directory and not mandatory, and failure to make such inventory and receipt does not invalidate evidence obtained in an otherwise legal search and seizure. P 711

Probable Cause: See "Probable Cause Chapter"

PROBATION ISSUES

Probation Conditions: No access to Internet

United States v. Sofsky, *** (2d Cir. 2002):

- In holding that defendant's condition of probation denying him access to the Internet was an overly broad restriction, the court held:

> We previously considered a sentencing component that prohibited **access** to a computer or the **Internet** in United States v. Peterson, 248 F.3d 79, 82-84 (2d Cir. 2001). The restriction **[*8]** was imposed as a condition of **probation** for a defendant convicted of larceny because of the defendant's prior state conviction for incest and his accessing of adult pornography on his home computer. Noting that "computers and **Internet access** have become virtually indispensable in the modern world of communications and information gathering," id. at 83, we ruled the condition unreasonable. Appellate courts considering a similar restriction imposed upon defendants convicted of child pornography offenses have reached different conclusions. Compare United States v. White, 244 F.3d 1199, 1205-07 (10th Cir. 2001) (invalidating and requiring modification of restriction imposed on defendant who used Internet to receive child pornography), with United States v. Paul, 274 F.3d 155, No. 00-41299, 2001 WL 1462963, at *11 (5th Cir. Nov. 19, 2001) (upholding restriction imposed on defendant who produced child pornography and used Internet to distribute it), and United States v. Crandon, 173 F.3d 122, 127-28 (3d Cir. 1999) (upholding restriction imposed on defendant who used

Internet to contact 14-year-old girl with whom he had sexual relations **[*9]** and photographed such conduct).

We appreciate the Government's point that permitting Sofsky access to a computer and the Internet after serving his ten-year sentence can facilitate continuation of his electronic receipt of child pornography, but we are more persuaded by the observation in Peterson that "although a defendant might use the telephone to commit fraud, this would not justify a condition of **probation** that includes an absolute bar on the use of telephones." Peterson, 248 F.3d at 83. The same could be said of a prohibition on the use of the mails imposed on a defendant convicted of mail fraud. A total ban on **Internet access** prevents use of e-mail, an increasingly widely used form of communication and, as the Tenth Circuit noted, prevents other commonplace computer uses such as "doing any research, getting a weather forecast, or reading a newspaper online." White, 244 F.3d at 1206. Although the condition prohibiting Sofsky from accessing a computer or the Internet without his probation officer's approval is reasonably related to the purposes of his sentencing, in light of the nature of his offense, we hold that the condition inflicts **[*10]** a greater deprivation on Sofsky's liberty than is reasonably necessary.

The Government contended at oral argument that the restriction must be broad because a restriction limited to accessing pornography would be extremely difficult for the probation officer to enforce without constant monitoring of Sofsky's use of his computer. There are several responses. First, to the extent that even a broad restriction would be enforced by the probation officer, monitoring (presumably unannounced) of Sofsky would be required to check if he was using a computer at all. Second, a more focused restriction, limited to pornography sites and images, can be enforced by unannounced inspections of Sofsky's premises and examination of material stored on his hard drive or removable disks. n4 Cf. United States v. Knights, 534 U.S. 112, 122 S. Ct. 587, 591-93, 151 L. Ed. 2d 497 (2001) (rejecting Fourth Amendment challenge to search, on reasonable suspicion, of probationer's premises). Finally, the Government can check on Sofsky's Internet usage with a sting operation--surreptitiously inviting him to respond to Government placed **Internet** ads for pornography. See White, 244 F.3d at 1201.

United States v. Walser, 275 So.3d 981 (10th Cir. 2001):

> Condition of defendant's child pornography probation sentence specifying that he not access the Internet without prior permission of his probation officer was not overly broad. The court noted, however, that complete denial of access to the Internet may have been too broad.

United States v. Paul, 274 F.3d 155 (5th Cir. 2001):

> Facts: Defendant argued that the condition of his supervised release prohibiting him from having, possessing, or having access to "computers, the Internet, photographic equipment, audio/video equipment, or any item capable of producing a visual image" is unreasonably broad.
>
> Holding: The conditions were reasonably related to his contact and are therefore valid.
>
> Discussion: This opinion cites numerous other opinions on the same topic and is a good reference source.

Probation Conditions: Monitoring Software

United States v. Lifshitz, (2d Cir. 2004)

> Defendant challenged the computer monitoring condition as violative of his Fourth Amendment right to be free of unreasonable searches. Although the Fourth Amendment offered protection against searches of home computers, the "special needs" of the probation system, including rehabilitating defendant and ensuring that he did not inflict further harm on the community by receiving or disseminating child pornography during the probationary period, were sufficient to justify conditioning defendant's probation upon his agreement to submit to computer monitoring. However, the scope of the computer monitoring condition was possibly overbroad. There was little information about what kind of monitoring the probation condition authorized. A brief survey of methods revealed that the varieties of available products and techniques diverged vastly in their breadth, and in their implications for computer users' privacy. And, while the Fourth Amendment's reasonableness inquiry did not require employing the least intrusive means, it was not clear that the monitoring condition as structured ensured the required close and substantial relation. Finally, the efficacy of the condition was not clear.

Particularity Requirements

United States v. Irving, 2018 WL 4681631 (D.Kan., 2018)

> Warrant to search sex offender's social media account was overbroad, and thus invalid, where warrant stated that crime being investigated was alleged violation of Kansas Offender Registry Act requirement that offender register account with law enforcement, yet covered entire time frame that offender had maintained account and encompassed everything in account, including all contact and personal identifying information, all private messages and chat histories, all video history, all activity logs, all Internet Protocol (IP) logs, all friend requests whether accepted or rejected, and all past and present lists of friends.

SOLICITATION OF CHILDREN ONLINE

Charging Attempt When No Real Child Is Involved

U.S. v. Morris, (7th Cir. 2008):

> The case law uniformly holds that the fact that a defendant is mistaken in thinking that the person he is trying to entice is underage is not a defense to a charge of attempted illegal sexual contact with a minor.
>
> It is not a defense to child solicitation charge that victim's mother assumed her identity on line to facilitate a meeting with the suspect.

U.S. v. Hicks, (8th Cir. 2006):

> A defendant may be convicted of attempting to violate statute prohibiting enticement of a minor to engage in sexual activity using the Internet even if the attempt is made towards someone the defendant believes is a minor but who is actually not a minor.
>
> Existence of actual minor victim was not required to convict defendant of travel in interstate commerce with the purpose of engaging in criminal sexual conduct

First Amendment Defense to Soliciting Child

U.S. v. Riccardi, 258 F. Supp. 2d 1212 (Kansas 2003):

> [18 U.S.C. § 2422(b)] only applies to those who "knowingly" [**32] persuade or entice, or attempt to persuade or entice, minors. Thus, it only affects those who intend to target minors: it does not punish those who

inadvertently speak with minors or who...post messages for all internet users, either adults or children, to seek out and read at their discretion. Any limited or incidental effect on speech does not infringe on any constitutionally protected rights of adults. Put another way, the Defendant simply does not have a First Amendment right to attempt to persuade minors to engage in illegal sex acts. Defendant's constitutional challenge is without merit.

Undercover detectives assuming identity of child online

United States v. Meeks, 366 F.3d 705, (9th Cir. 2004):

14-year-old victim gave police permission to assume his Internet identity and engage in instant messages with his online "friends." Subsequently, the police engaged in and captured online communications with the defendant. The court ruled that the police did not unlawfully intercept defendant's communications and he had no expectation of privacy in instant messages.

Wiretaps

State v. Otte, 29 Fla. L. Weekly S549 (Fla. 2004):

In ruling that wiretaps cannot be used in prostitution investigations, the court points out that federal law in wiretaps preempt state law. States are free to place more stringent requirements on governments, but no lesser ones.

Compelling Defendant to produce password:

Varn v. State, 2020 WL 5244807 (Fla.App. 1 Dist., 2020)

Petitioner has no legal right to prevent the State from obtaining his cell phone passcode. He cannot demonstrate irreparable harm as required to obtain certiorari relief, and we dismiss the Petition.

On this limited factual record, we must determine if Petitioner has shown irreparable harm; i.e., whether Petitioner's Fifth Amendment rights survive a foregone conclusion analysis. If the government already knows the existence and location of the information sought, and that the target has access to it, the act of production is not sufficiently testimonial to invoke the Fifth Amendment.

We certify conflict between this decision and State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016).*

We certify to the Florida Supreme Court the following questions of great public importance, and urge the Court to review and resolve them:

Is It a Constitutionally Protected Testimonial Act To Disclose One's Cell Phone Passcode Under State Compulsion?

When Does the Foregone Conclusion Exception Apply To Such Compelled Disclosure?

G.A.Q.L., v. State, 2018 WL 5291918, at *2 (Fla.App. 4 Dist., 2018)

All of these password cases, with the exception of Stahl, have determined that the compelled production of a passcode is more akin to revealing a combination than producing a key. This is so because revealing one's password requires more than just a physical act; instead, it probes into the contents of an individual's mind and therefore implicates the Fifth Amendment. See Kirschner, 823 F. Supp. 2d at 669. The very act of revealing a password asserts a fact: that the defendant knows the password. See Hubbell, 530 U.S. at 43 (stating that the Fifth Amendment applies "to the testimonial aspect of a response to a subpoena seeking discovery" of sources of potentially incriminating information). Thus, being forced to produce a password is testimonial and can violate the Fifth Amendment privilege against compelled self-incrimination.

Additionally, the trial court erred in relying on the foregone conclusion exception, as the requirements of that exception were not met.

State v. Stahl, 206 So.3d 124 (Fla.App. 2 Dist., 2016)

Requiring defendant who was charged with video voyeurism to produce the passcode to unlock his cell phone did not compel defendant to communicate information that had testimonial significance under the Fifth Amendment's protection against self-incrimination; providing the passcode would not be an acknowledgment that the phone contained evidence of video voyeurism, and the state had a warrant to search the phone.

In order for the foregone conclusion exception of the Fifth Amendment privilege against self-incrimination to apply, the State must show with reasonable particularity that, at the time it seeks the act of production, it already knows the evidence sought exists, the evidence is in the possession of the accused, and the evidence is authentic.

State established with reasonable particularity the existence of a cell phone's passcode that defendant did not want to produce, as required under the foregone conclusion exception to the Fifth Amendment's protection against self-incrimination, where the state established that the phone, which was subject of an

unchallenged search warrant, could not be searched without entry of a passcode.

In Re: Boucher (D.Vt. 2007)

Defendant could not be compelled to produce password to encrypted files on his laptop in child pornography investigation.

"*Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" If Boucher does know the password, he would be faced with the forbidden dilemma; incriminate himself, lie under oath, or find himself in contempt of court."*