Denver Law Review

Volume 79
Issue 3 *Tenth Circuit Surveys*

Article 5

December 2020

Combating the Illicit Internet: Decisions by the Tenth Circuit to Apply Harsher Sentences and Lessened Search Requirements to Child Pornographers Using Computers

Anton L. Janik Jr.

COMBATING THE ILLICIT INTERNET: DECISIONS BY THE TENTH CIRCUIT TO APPLY HARSHER SENTENCES AND LESSENED SEARCH REQUIREMENTS TO CHILD PORNOGRAPHERS USING COMPUTERS

> *There is no adequate way to measure the damage caused by those who produce and sell child pornography. Child pornographers rob children of their innocence and leave them harmed for life. Society must not tolerate this behavior, and the federal government must have the resolve and the necessary tools to combat it.*
>
> . . . In light of these significant harms, it is essential that those who are caught and convicted for this conduct be punished severely.[1]

With its inexpensive, unlimited and instantaneous transmission characteristics, the Internet has been termed "the most efficient pornography distribution engine ever conceived."[2] About one-fifth of worldwide Internet users regularly visit a commercial pornography site,[3] making the Internet the "primary medium for pornography transmission."[4] Estimates of the annual U.S. sales revenue from child pornography approach one billion dollars.[5]

In 1994, about twenty-three percent of federal child pornography cases involved the use of a computer.[6] In 1995, that number increased by more than one-fifth, to twenty-eight percent.[7] In response to such growth, Congress enacted legislation to stiffen the penalties assessed against child pornographers.[8] The legislation subjects suspected child pornographers to lessened search and seizure requirements and subjects convicted pornographers to increased sentencing terms.[9] If crimes were committed by using the computer, the pornographers may have restrictions on Internet use that reach into their parole terms.[10] The lessened search and sei-

---

1. H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61.

2. Lesli C. Esposito, Note, *Regulating the Internet: The New Battle Against Child Pornography*, 30 CASE W. RES. J. INT'L L. 541, 541 (1998) (quoting Bill Frezza, *Morality and Imagination: Technology Challenges Both*, COMM. WK., Jan. 13, 1997, at 31, 1997 WL 7691238).

3. *See* Kelly M. Doherty, Comment, *www.obscenity.com: An Analysis of Obscenity and Indecency Regulation on the Internet*, 32 AKRON L. REV. 259, 263 (1999).

4. Esposito, *supra* note 2, at 541.

5. *See* HOWARD A. DAVIDSON & GREGORY A. LOKEN, U.S. DEP'T. OF JUSTICE, CHILD PORNOGRAPHY AND PROSTITUTION 1 (1987).

6. *See* U. S. SENTENCING COMM'N, REPORT TO THE CONGRESS: SEX OFFENSES AGAINST CHILDREN, at 30 (1996), http://www.ussc.gov/r_congress/scac.htm (last visited Feb. 18, 2002).

7. *See id.*

8. *See* H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61.

9. *See id.*

10. *See* discussion *infra* Parts I.B. & II.B.

zure standard applies whether authorities discover pornography, or even merely believe it may exist, on the defendant's computer.[11]

During this past year, the Court of Appeals for the Tenth Circuit expanded the definition of "solicitation" of a minor,[12] supported offense-level enhancements for child pornographers who use computers to commit crimes,[13] upheld Internet restrictions on paroled child pornography defendants,[14] and widened the scope of warranted searches to encompass all material on computer hard drives and disks.[15] The change in the court's traditional interpretation is in response to the realization that computers present extraordinarily wide distribution capabilities and, by exploiting a child's fascination with computers, may be effective in enticing minors to engage in pornographic activity.[16]

As presented in several cases that came before the Tenth Circuit in 2000-2001, this survey examines the current movement toward reinterpreting traditional search and seizure requirements, and increasing penalties for defendants convicted of child pornography crimes involving computer usage. Part I examines the legislation behind the increased sentencing and parole penalties, and the Court of Appeals' corresponding interpretation of that legislation. Part II continues that analysis, focusing on the lowered standards applied to both the execution of search warrants, and the search and seizure of computer equipment.

I. PENALTIES INCREASE WHEN A COMPUTER IS USED IN THE SOLICITATION OF MINORS

A. *Legislation that Controls the Crime of Child Pornography*

The federal crimes constituting sex offenses against children fall into three major categories: pornography, transportation, and criminal sexual abuse.[17] This paper focuses on the first category.

Sex offenses against children constitute a small percentage of the total federal criminal sentencings.[18] In 1995, courts sentenced only fifty-eight defendants for committing child pornography crimes, constituting 0.2% of all federal sentencings.[19] That same year, the total number of federal convictions for violations of all child sex crime laws numbered

---

11. *See* discussion *infra* Part II.C.1.a.2.
12. *See* discussion *infra* Part I.C.
13. *See* discussion *infra* Part I.C.1.a.
14. *See* discussion *infra* Part I.D.
15. *See* discussion *infra* Part II.B.1.a.3.
16. *See, e.g.*, United States v. Reaves, 253 F.3d 1201, 1204-05 (10th Cir. 2001) (construing H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61).
17. *See* U. S. SENTENCING COMM'N, *supra* note 6, at 1.
18. *See id.* at 2.
19. *See id.*

209, approximately 0.6% of all federal convictions.[20] However, federal prosecutions account for only a small number of child pornography defendants.[21] In cases involving the rape of a minor, which is one category from which accurate state and federal numbers may be drawn, state courts convicted an estimated 8,662 offenders in 1992.[22] Using this estimated figure, federal convictions constituted only 1.6% of the total nationwide convictions for rape of a minor.[23] These numbers suggest that child sex offenders commit a staggering number of crimes in the United States each year.

Federal law criminalizes the production of child pornography under 18 U.S.C. §§ 2251 and 2252.[24] Section 2251 provides:

> Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, shall be punished . . . if such person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, *including by computer*, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.[25]

In the United States, pornography is "more freely available over the Internet than in other mass communications media."[26] The increasing use of the Internet to purchase, trade, and download pornographic materials subjects many child pornographers to the interstate transport clause of § 2251.[27] Courts may impose sentences ranging from ten years to life imprisonment for violations of § 2251.[28]

In addition to restricting production, federal law also prohibits the interstate transport, receipt, reproduction, and sale of child pornography.[29] Similar to § 2251's provision, § 2252A explicitly provides

---

20. *See id.* (citing fifty-eight sentences for child pornography, six sentences for transportation of a minor, and 145 sentences for criminal sexual abuse).

21. *See id.*

22. *See id.*

23. *See* U. S. SENTENCING COMM'N, *supra* note 6, at 2.

24. *See id.* at 1.

25. 18 U.S.C. § 2251(a) (2000) (emphasis added).

26. Anthony L. Clapes, *The Wages of Sin: Pornography and Internet Providers,* COMPUTER LAW, July 1996, at 1.

27. *See* Esposito, *supra* note 2, at 541 ("the Internet has caused a surge in the production and distribution of child pornography"); Clapes, *supra* note 26, at 1 ("pornography is not rampant on the Internet; it is, however, more freely available over the Internet than in other mass communications media in the United States").

28. *See* 18 U.S.C. § 2251(d).

29. *See* 18 U.S.C. § 2252A (2000).

that interstate transport includes transmission via computer.[30] A violation of § 2252A carries a penalty of up to thirty years of imprisonment.[31]

In 1984, Congress created the United States Sentencing Commission (hereinafter "Sentencing Commission") to develop and maintain uniform sentencing guidelines for use by federal judges.[32] The guidelines established base offense levels for each federal crime.[33] As part of the guidelines, the Sentencing Commission also established sentence-level enhancements, which increase the offense level of the crime committed.[34] Balancing such enhancements against any applicable credits results in a "total 'offense level' number" that "corresponds to a sentencing table which, together with considerations of prior criminal history, sets forth the appropriate sentencing range (in months) that the judge must employ when sentencing an offender."[35] Each year, the Sentencing Commission proposes revisions to its published guidelines, which enter into effect unless Congress acts to modify or block them.[36]

A defendant's use of a computer to produce or solicit child pornography subjects the defendant to sentence enhancement under the U. S. Sentencing Guidelines Manual (hereinafter "Sentencing Guidelines").[37] Similarly, sentence enhancements also apply when the defendant used a computer to transmit child pornography.[38]

B. *Pornography's "Significant Harms" Caused Congress to Call for Increased Sentence Terms*

Federal legislation protecting children from sexual exploitation has existed at least since 1977, when Congress enacted the Protection of Children Against Sexual Exploitation Act of 1977.[39] That law made it illegal to engage a minor in any sexually explicit conduct for the purpose of producing a visual depiction of that conduct, when such depiction would be transported via interstate commerce.[40] Since the 1977 act resulted in only a single conviction, Congress modified the law by passing

---

30. *See* 18 U.S.C. § 2252A(a)(1).
31. *See* 18 U.S.C. § 2252A(b).
32. *See* H.R. REP. NO. 104-90, at 3 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760.
33. *See id.*
34. *See id.*
35. *Id.*
36. *See id.*
37. *See* U.S. SENTENCING GUIDELINES MANUAL § 2G2.1(b)(3)(B) (2001).
38. *See id.* at § 2G2.2(b)(5).
39. Pub. L. No. 95-225, 92 Stat. 7 (1977) (codified as amended at 18 U.S.C. §§ 2251-53 (2000)). *See* Anthony Miranda, *A Survey of Federal Cases Involving the Child Pornography Prevention Act of 1996*, 9 B.U. PUB. INT. L.J. 483, 484 (2000).
40. *See* Miranda, *supra* note 39, at 484.

the Child Protection Act of 1984,[41] itself amended by the Child Sexual Abuse and Pornography Act of 1986.[42]

Congress continued to refine the law by passing the Child Protection and Obscenity Enforcement Act of 1988,[43] which criminalized using a computer "to transport, distribute, or receive child pornography."[44] Later reforms included the Child Protection Restoration and Penalties Enhancement Act of 1990[45] and the Sex Crimes Against Children Prevention Act of 1995,[46] discussed below. Congress next passed the Child Pornography Prevention Act of 1996,[47] which was a turning point because the act regulated content rather than conduct[48] by criminalizing "visual depictions [made by computer] that create the impression that children are involved in sexually explicit acts."[49] Congress recently reformed the law by passing the Protection of Children from Sexual Predators Act of 1998.[50]

In the Sex Crimes Against Children Prevention Act of 1995, Congress increased the penalties for certain sex crimes against children that involved the use of a computer.[51] These changes found their genus in the Family Reinforcement Act, which addressed crimes against children, and Congress' perceived need to control child pornography.[52] Perceiving "significant harms"[53] arising at the nexus between computer use and child pornography, the House of Representatives passed H.R. 1240.[54] In the words of the House Committee on the Judiciary:

> Distributing child pornography through computers is particularly harmful because it can reach an almost limitless audience. Because of its wide dissemination and instantaneous transmission, computer-assisted trafficking is also more difficult for law enforcement officials to investigate and prosecute. Additionally, the increasing use of com-

---

41. Pub. L. No. 98-292, 98 Stat. 204 (1984) (codified as amended at 18 U.S.C. §§ 2251-53).

42. Pub. L. No. 99-628 § 2, 100 Stat. 3510 (1986) (codified as amended at 18 U.S.C. § 2251). *See* Miranda, *supra* note 39, at 484.

43. Pub. L. No. 100-690 § 7511, 102 Stat. 4181 (1988) (codified as amended at 18 U.S.C. §§ 2251A-2252).

44. Miranda, *supra* note 39, at 484.

45. Pub. L. No. 101-647 § 301, 104 Stat. 4789 (1990) (codified as amended in scattered titles of the U.S.C.).

46. Pub. L. No. 104-71, 109 Stat. 774 (1995) (codified as amended at 18 U.S.C. § 2423 (1995); 28 U.S.C. § 994 (1995)).

47. Pub. L. No. 104-208 § 121, 110 Stat. 3009 (1997) (codified as amended in scattered titles of the U.S.C.).

48. *See* Dawn A. Edick, Note, *Regulation of Pornography on the Internet in the United States and the United Kingdom: A Comparative Analysis*, 21 B.C. INT'L & COMP. L. REV. 437, 445 (1998).

49. Miranda, *supra* note 39, at 485.

50. Pub. L. No. 105-314, 112 Stat. 2974 (1998) (codified as amended in scattered titles of the U.S.C.).

51. *See* Pub. L. No. 104-71, 109 Stat. 774.

52. *See* H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61.

53. *Id.* at 4.

54. *See* Pub. L. No. 104-71, 109 Stat. 774.

> puters to transmit child pornography substantially increases the likelihood that this material will be viewed by, and thus harm, children. Finally, the Committee notes with particular concern the fact that pedophiles may use a child's fascination with computer technology as a lure to drag children into sexual relationships.[55]

Essentially, the House Committee not only feared that pornographers would entice children to engage in pornographic acts by merely enabling children to view images, but also that computer usage might increase the overall number of images disseminated due to the ease with which pornographers can copy and transmit material to a virtually unlimited market. In the Sentencing Commission's words: "Persons who transmit the images . . . may be mailing a single photo to a friend, or they may be more similar to a person who opens an adult bookstore in every city in the world."[56] However, § 2G2.1 of the Sentencing Guidelines "does not distinguish between persons who e-mail images to a single voluntary recipient and those who establish a BBS [bulletin board system] and distribute child pornography to large numbers of subscribers."[57]

Finding great potential for significant harm to children, the House concluded "it is essential that those who are caught and convicted for this conduct be punished severely."[58] Thus, H.R. 1240 directed the Sentencing Commission to "increase the base offense level by at least 2 levels for an offense committed under section 2251(c)(1)(A) and 2252(a) of title 18, United States Code, if a computer was used to transmit the notice or advertisement to the intended recipient or to transport or ship the visual depiction."[59]

The Sentencing Commission complied, and on April 30, 1996, submitted to Congress the guidelines that increased those sentences.[60] Increasing the offense level directly resulted in an increase to the sentencing term: in the case of a child pornography producer, the sentence increases from the original range of fifty-seven to seventy-one months, to seventy to eighty-seven months per count; in the case of a child pornography trafficker, the range increases from the original range of eighteen to twenty-four months, to twenty-four to thirty months per count.[61] By

---

55. H.R. REP. NO. 104-90, at 3-4.

56. U. S. SENTENCING COMM'N, *supra* note 6, at 29.

57. *Id.* at 30.

58. H.R. REP. NO. 104-90, at 4.

59. Sex Crimes Against Children Prevention Act of 1995, Pub. L. No. 104-71 § 53, 109 Stat. 774.

60. *See* U. S. SENTENCING COMM'N, *supra* note 6, at i. H.R. 1240 ordered the Sentencing Commission to complete this report within 180 days of the enactment of the Sexual Crimes Against Children Prevention Act of 1995. *See* H.R. REP. NO. 104-90, at 2.

61. *See* U. S. SENTENCING COMM'N, *supra* note 6, at 4 tbl.1.

simply using a computer to commit a child pornography offense, a person increases his or her sentence by roughly twenty-five percent.[62]

C. *The Expanded Definition of "Solicit"*

Taking the House Committee on the Judiciary's concerns as a mandate, the Sentencing Guidelines provide offense-level enhancement if a computer is used to *solicit* participation by a minor in sexually explicit conduct.[63] In *United States v. Reaves*,[64] the Tenth Circuit confronted an issue of first impression: what is the definition of the term "solicit?"[65] Interpreting the House Committee on the Judiciary's "broad concerns," the Court expanded the meaning of solicitation of a minor to include *any* situation in which a computer is used, whether or not that use is directly related to a common notion of "solicitation."[66]

1. Tenth Circuit Cases

a. *United States v. Reaves*[67]

i. Facts

In *Reaves*, the defendant acquired several child pornography images from the Internet.[68] Using his computer, the defendant showed those images to children to entice and lure them into sexual relationships, and to produce sexually explicit materials.[69] The defendant pled guilty to five counts of producing child pornography, and "one count each of interstate transportation, distribution, and possession, of child pornography."[70]

Reasoning that "the computer played an integral part in a solicitation scheme presumably designed to accustom the minors to child pornography and encourage the sexual conduct depicted therein," the United States District Court for the District of Wyoming determined that the defendant's actions constituted solicitation, which thus subjected him to the offense-level enhancer § 2G2.1(b)(3).[71] Following those guidelines, the district court increased the defendant's offense level by two.[72] The defendant appealed, arguing that because he did not directly *ask* or *re-*

62. *See id.* at ii.
63. *See* U.S. SENTENCING GUIDELINES MANUAL § 2G2.1(b)(3)(B) (2001).
64. 253 F.3d 1201 (10th Cir. 2001).
65. *See Reaves*, 253 F.3d at 1202.
66. *Id.* at 1205; *see also* discussion *infra* Part I.C.2.a.2.
67. 253 F.3d 1201 (10th Cir. 2001).
68. *See Reaves*, 253 F.3d at 1203.
69. *See id.*
70. *Id.* at 1202. The defendant's production of pornography violated 18 U.S.C. § 2251(a). *See id.* The defendant's "interstate transportation, distribution, and possession, of child pornography" violated "18 U.S.C. §§ 2252A(a)(1) and (b)(1), (a)(2)(B) and (b)(1), and (a)(5)(B) and (b)(2), respectively." *Id.*
71. *Reaves*, 253 F.3d at 1203.
72. *See id.* at 1202-03.

quest children to participate in creating the pornography, he did not "solicit" minors via his computer, and therefore the offense-level enhancement did not apply.[73]

ii. Decision

Noting that § 2G2.1 provides no definition of "solicit," the Tenth Circuit struggled to determine whether the phrase "if a computer was used to solicit participation" meant "if a computer was used to *directly request* participation," or "if a computer was used to *lure or entice* participation."[74] In order to determine the intent of the Sentencing Commission, the Tenth Circuit turned to the congressional mandate underlying the Sentencing Commission's change to the guidelines.[75]

After considering the House Commission on the Judiciary's statements outlining the reason for the offense-level enhancing statute, the Court noted that "[l]imiting 'solicit' . . . to 'direct requests' . . . solely penalizes *how* a pedophile exploits a child's fascination with computers rather than *if* a pedophile does so—an unacceptable result given Congress's broad concerns."[76] The court concluded that "solicit" was not narrowly limited to situations where a defendant used a computer to directly contact a victim; rather it applied in a more general sense, to situations where a defendant used a computer at all.[77] The Tenth Circuit thus upheld the offense-level enhancement.[78]

2. Other Circuits

a. *United States v. Brown*[79]

Brown represents the only other appellate opinion to address the solicitation definition issue presented in *Reaves*. *Brown* extended the scope of solicitation to include the defendant's use of a computer as a desensitizing tool, which enabled him to obtain minors' cooperation in the creation of pornography.[80]

i. Facts

---

73. *See id.* at 1203.

74. *Id.* at 1204-05. The court applied the version of the offense-level enhancing statute in force at the time of defendant's commission of the crime, which provided for an increased sentence "[i]f a computer was used to solicit participation by or with a minor in sexually explicit conduct for the purpose of producing sexually explicit material." *Id.* at 1202 (quoting U.S. SENTENCING GUIDELINES MANUAL § 2G2.1(b)(3) (1998)).

75. *See Reaves*, 253 F.3d at 1204-05.

76. *Id.*

77. *See id.* at 1205.

78. *See id.*

79. 237 F.3d 625 (6th Cir. 2001).

80. *See Brown*, 237 F.3d at 629.

As part of a worldwide child pornography investigation, the United States Customs Service learned that Internet Relay Chat (hereinafter "IRC") software was being used to exchange child pornography images.[81] During the course of the investigation, British authorities seized a computer belonging to a member of a private IRC group, which used the computer to exchange child pornography.[82] The seized computer revealed several IRC nicknames, including one that U.S. law enforcement officials ultimately tied to the defendant, who officials subsequently arrested.[83]

The defendant pled guilty to three counts of "producing child pornography for transportation in interstate commerce" and one count of "possessing child pornography using materials shipped via interstate commerce," among other charges.[84] The United States District Court for the Western District of Michigan determined the defendant "allowed his victims unmonitored access to the computer wherein they observed that other children were being filmed and sexually abused by adults."[85] Finding the defendant thus used his computer to solicit the children's participation in the production of pornography, the district court applied § 2G2.1(b)(3) and sentenced the defendant to a 405-month term of imprisonment.[86]

ii. Decision

On appeal, the defendant argued that § 2G2.1(b)(3)'s sentence enhancement did not apply because he did not use a computer to *solicit* minors' participation in the creation of pornography.[87] The defendant interpreted "solicit" to require that he "specifically ask minors [via his computer] to engage in sexually-explicit conduct."[88] The Sixth Circuit disagreed, determining that Congress did not intend such a narrow definition of the term "solicit."[89] In a short analysis, the Court held that allowing children to view child pornography gave them the "impression that this is acceptable conduct," which aided in the defendant's ability to use those children to produce child pornography.[90] The Sixth Circuit con-

---

81. *See id.* at 626-27. IRC allows users to communicate without using their real names. *See* ORIN S. KERR, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 91 (2001), http://www.usdoj.gov/criminal/cybercrime/searchmanual.pdf (Feb. 16, 2001).

82. *See Brown*, 237 F.3d at 627.

83. *See id.*

84. *Id.* at 626. The defendant's production of child pornography violated 18 U.S.C. § 2251(a). *See Brown*, 237 F.3d at 626. The defendant's possession of child pornography violated 18 U.S.C. § 2252(a)(4)(B). *See Brown*, 237 F.3d at 626.

85. *Brown*, 237 F.3d at 628.

86. *See id.* at 626.

87. *See id.* at 628.

88. *Id.*

89. *See id.* at 628-29 (construing H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61).

90. *See id.* at 629.

cluded that because the defendant used his computer "to desensitize his victims to deviant sexual activity, he was using it to solicit participation" in the creation of child pornography.[91]

3. Analysis

As the Tenth Circuit noted, § 2G2.1(b)(3) provides no express definition of the term "solicit."[92] In both of the above cases, the appellate courts deduced the meaning of the term by using the House Committee on the Judiciary's statements regarding the dangers of computer usage in association with child pornography.[93] Both the Tenth Circuit and the Sixth Circuit interpreted the broad concerns outlined by the House Committee on the Judiciary as requiring a defendant's mere use of a computer in connection with child pornography to suffice as solicitation.[94] The common notion of solicitation cannot be strictly applied because, as Congress recognized, the dangers found at the nexus between computers and child pornography are very high—so high that there may be no way to adequately measure the damages.[95]

The Tenth Circuit's expansive interpretation of the term "solicit" comports with the only other appellate opinion on this issue. It remains to be seen whether this expansive view will become the court's standard interpretation.

D. *A Defendant's Use of a Computer May Prompt the Court to Institute Post-Sentence Parole Requirements*

Child pornography, coupled with computer use, may result in penalty increases that reach beyond sentencing. In some circumstances, this coupling can affect a defendant's parole term when a court mandates compliance with special conditions. In the cases below, the Tenth Circuit permitted parole-phase Internet restrictions on convicted child pornographers, provided courts narrowly construe such restrictions.

1. Tenth Circuit Cases

a. *United States v. White*[96]

i. Facts

Responding to an Internet advertisement posted as part of a United States Customs Service sting operation, the defendant ordered three

91. *Brown*, 237 F.3d at 629.
92. *See* United States v. Reaves, 253 F.3d 1201, 1204 (10th Cir. 2001).
93. *See Brown*, 237 F.3d at 628-29; *Reaves*, 253 F.3d at 1204-05.
94. *See Brown*, 237 F.3d at 629; *Reaves*, 253 F.3d at 1205.
95. *See* H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61.
96. 244 F.3d 1199 (10th Cir. 2001).

videotapes advertised as containing child pornography.[97] United States Customs officers made a controlled delivery, which triggered the defendant's arrest.[98] A federal grand jury indicted the defendant for violating a federal statute that prohibits a person from receiving child pornography, among other charges.[99] The defendant pled guilty and served a two-year sentence.[100]

One week after serving out his sentence, the defendant violated a requirement of his supervised release by consuming alcohol.[101] After a second such violation, the government then filed a petition to revoke the defendant's supervised release.[102] In a subsequent hearing, the United States District Court for the District of New Mexico sentenced the defendant to six months incarceration followed by a two-year period of supervised release.[103] The court imposed five special conditions upon the supervised release.[104] One of these conditions prevented the defendant from possessing sexually explicit material and any computer with access to the Internet.[105] The defendant challenged this special condition by arguing that a "plea to a single count of receiving child pornography which he ordered over the Internet . . . is not 'reasonably related' to prohibiting him from all access to the Internet."[106] The defendant further argued that this "special condition [wa]s 'greater than necessary' in the equation balancing protection of the public with the goals of sentencing."[107]

ii. Decision

The Tenth Circuit held that while a federal statute[108] permitted the district court to exercise discretion in imposing a term of supervised release, the district court is limited by the requirement that it "shall impose a sentence sufficient, but not greater than necessary."[109] The court held that the special condition preventing the defendant from owning a computer with Internet access potentially is both too narrow and overbroad.[110] The court found the condition potentially too narrow because the terms

97. *See White*, 244 F.3d at 1201.

98. *See id.*

99. *See id.* (noting the grand jury indicted the defendant for violating 18 U.S.C. § 2252(a)(2)(A), among other statutes).

100. *See id.*

101. *See id.*

102. *See id.*

103. *See White*, 244 F.3d at 1201.

104. *See id.*

105. *See id.* The provision in question provided that the defendant "shall not possess erotica, or any other sexually explicit material, and shall not possess a computer with Internet access throughout his period of supervised release." *Id.*

106. *White*, 244 F.3d at 1201-02, 1205.

107. *Id.*

108. 18 U.S.C. § 3583(a) (2001).

109. *White*, 244 F.3d at 1204 (quoting 18 U.S.C. § 3553(a)).

110. *See id.* at 1206. The relevant portion of the condition provided that the defendant "shall not possess a computer with Internet access throughout his period of supervised release." *Id.*

of the condition were too indeterminate and, thus, the condition did not bar the defendant from *accessing* to the Internet, but simply from *owning* a computer with such access.[111] The court found the condition potentially too broad because the district court could have intended for the word "possess" to restrict all of the defendant's Internet and computer usage, even usage unrelated to the defendant's underlying crime.[112] From that viewpoint, the sentence was "greater than necessary."[113]

The Tenth Circuit determined that instead, the district court should have limited the condition to *use* of the Internet, as opposed to *possession* of a computer with an Internet connection, as many alternative means existed by which the defendant could have accessed the Internet without owning a computer.[114] The court thus found the restriction "neither reasoned nor reasonable" and remanded the case for clarification on the condition prohibiting the defendant from owning a computer with Internet access.[115]

Although restrictive, the Tenth Circuit's decision is not as strict as the Third Circuit's decision in *United States v. Crandon*,[116] below, where the Third Circuit supported the total ban on a defendant's possession of, procurement of, purchase of, or other access to any form of computer network, including networks operating outside the Internet.[117]

2. Other Circuits

a. *United States v. Crandon*[118]

i. Facts

The defendant solicited a minor via e-mail, then traveled to her location and "engaged in sexual relations with her."[119] The defendant took forty-eight photographs of the minor.[120] Two of the photographs portrayed sexually explicit activity, including one photograph of the defendant and the minor participating in oral sex.[121] The defendant mailed the film to a Seattle film developer and received the developed pictures by

111. *See id.* at 1205.
112. *See id.* at 1206.
113. *See id.* (quoting 18 U.S.C. § 3553(a)).
114. *See id.* at 1206-07.
115. *White*, 244 F.3d at 1207 (holding that "any condition limiting [the defendant's] use of a computer or access to the Internet must reflect these realities and permit reasonable monitoring by a probation officer. The purpose of the special condition must be articulated and enforceable as defined. As presently written, the special condition is neither reasoned nor reasonable.").
116. 173 F.3d 122 (3d Cir. 1999).
117. *See Crandon*, 173 F.3d at 125.
118. 173 F.3d 122 (3d Cir. 1999).
119. *Id.*
120. *See id.*
121. *See id.*

return mail.[122] After his return to New Jersey, the defendant continued to contact the minor.[123] The defendant again traveled to the minor's location, and this time he picked her up and began to return home.[124] Soon after their departure from the minor's home, the defendant discovered the police were looking for him.[125] The defendant sent the minor home on a bus and then returned to his home state.[126] The police later arrested the defendant and seized his cache of pornographic photographs.[127]

The defendant pled guilty to receiving child pornography in violation of a federal statute.[128] The United States District Court for the District of New Jersey sentenced the defendant to seventy-eight months of imprisonment and three years of supervised release.[129] The terms of the defendant's parole "included a special condition directing that [the defendant] not 'possess, procure, purchase or otherwise obtain access to any form of computer network, bulletin board, Internet, or exchange format involving computers unless specifically approved by the United States Probation Office.'"[130] The defendant appealed on the basis that the special condition "unnecessarily infringe[d] upon his liberty interests and b[ore] no logical relation to his offense."[131]

ii. Decision

The Third Circuit held that because the defendant "used the Internet as a means to develop an illegal sexual relationship with a young girl over a period of several months[,] . . . the condition of release limiting [the defendant's] Internet access is related to the dual aims of deterring him from recidivism and protecting the public."[132] As such, the Third Circuit upheld the restriction on Internet use as a reasonable limitation, noting that "[a] sentencing judge is given wide discretion in imposing supervised release."[133]

---

122. *See id.*
123. *See id.*
124. *See Crandon*, 173 F.3d at 125.
125. *See id.*
126. *See id.*
127. *See id.*
128. *See id.* (noting the defendant pled guilty to violating 18 U.S.C. § 2252(a)(2)).
129. *See id.*
130. *Crandon*, 173 F.3d at 125.
131. *Id.* at 127.
132. *Id.* at 127-28.
133. *Id.* at 127. *See generally* 18 U.S.C. § 3583(d). The court read 18 U.S.C. § 3583(d) to hold that

> a District Court may order any appropriate condition to the extent it:
>
> > (1) is reasonably related to certain factors, including (a) the nature and circumstances of the offense and the history and characteristics of the defendant, (b) deterring further criminal conduct by the defendant, or (c) protecting the public from further criminal conduct by the defendant; [and] (2) involves no greater deprivation of liberty than is reasonably necessary for the purposes of deterrence and protection of the public.

The court further held that even though this special restriction "may hamper his employment opportunities upon release," and infringe upon the defendant's First Amendment rights, "the restrictions . . . are permissible because the special condition is narrowly tailored and is directly related to deterring [the defendant] and protecting the public."[134]

3. Analysis

The Tenth Circuit strictly adhered to Congress's expressed intent. Not only will a defendant be subjected to an increased term of incarceration, but when that defendant returns to society upon rehabilitation, his parole restrictions may legally include restrictions upon Internet use.[135] The Third Circuit took that notion farther, expressly comparing the relative harm to a defendant's constitutional rights with the risk of public harm, and determined that a total ban on Internet use is permissible, provided that the restriction remains narrowly construed towards averting that harm.[136]

After determining that Internet restrictions are proper, the Tenth Circuit discussed the technical means by which effective control of Internet use could occur.[137] One method is to install a database-centered software program specifically designed to restrict access to pornographic sites.[138] The mayor of Boston, Massachusetts, Thomas Menino, required the Boston Public Library to install such software "on every computer accessible to children."[139] The program, CyberPatrol, prevents access to web sites listed in its database of objectionable web sites.[140] An alternative means of preventing access to pornographic web sites is to employ a program that scans the target site for objectionable words and blocks web sites containing these objectionable words.[141]

While useful, neither restriction method is perfect: in the case of a database restriction method, someone must continually update the database to afford protection from an expanding number of Internet sites.[142] In the case of objectionable word scanning, such software may restrict access in an overbroad fashion.[143] For example, such a program might

---

Crandon, 173 F.3d at 127 (alteration in original).

134. *See Crandon*, 173 F.3d at 128.

135. *See* United States v. White, 244 F.3d 1199, 1207 (10th Cir. 2001).

136. *See Crandon*, 173 F.3d at 127.

137. *See White*, 244 F.3d at 1206 (noting the availability of filtering software capable of monitoring the defendant's Internet usage).

138. *See id.*

139. Edick, *supra* note 48, at 449.

140. *See id.*

141. *See id.*

142. *See White*, 244 F.3d at 1206.

143. *See* Edick, *supra* note 48, at 449-50.

restrict access to "medical and educational information on 'breast' cancer and 'Middlesex, England.'"[144]

II. LESSENED SEARCH AND SEIZURE REQUIREMENTS APPLY WHEN COMPUTERS ARE INVOLVED IN CHILD PORNOGRAPHY INVESTIGATIONS

While the previous section focused on the penalties applicable to a defendant who used a computer when committing a child pornography crime, this section analyzes the pre-trial effects upon search and seizure requirements when the defendant's commission of the crime involved a computer. As above, the defendant's use of a computer changes the way courts view and treat such a defendant.

A. *Background*

The Fourth Amendment to the Constitution provides for freedom from unreasonable search and seizure.[145] The United States Supreme Court has held that the Fourth Amendment's protections are only available upon the showing of a reasonable expectation of privacy.[146] The "reasonable expectation" determination requires both that a defendant have "an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[147]

Before officers may conduct a search, they must establish probable cause and must ensure the search warrant describes with particularity the property to be seized.[148] Probable cause is established when "given the totality of the circumstances, 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'"[149] On the issue of particularity, the Tenth Circuit has held that "[t]he Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings."[150] The reason for the particularity requirement is to leave the officer serving the warrant no discretion,

---

144. *Id.* at 450.

145. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U. S. CONST. amend. IV.

146. *See* Katz v. United States, 389 U.S. 347, 351 (1967), *accord* Minnesota v. Olson, 495 U.S. 91, 95-96 (1990).

147. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

148. *See* U. S. CONST. amend. IV.

149. United States v. Simpson, 152 F.3d 1241, 1246 (10th Cir. 1998) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

150. United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999).

thereby preventing general searches.[151] A warrant's description qualifies as sufficiently particular if it "enables the searcher to reasonably ascertain and identify the things authorized to be seized."[152]

When computers are involved, several issues complicate the particularity requirement: the ability of a computer to store large quantities of data, the computer's ability to hide data,[153] and the fact that a file's title need bear no relation to that file's content.[154] These issues may require law enforcement officials to seize a computer and remove it from a location in order to search the computer's contents.[155]

According to the U.S. Department of Justice, two potential seizure options exist, and the option selected by law enforcement officials depends upon the role of the computer in the underlying crime:

> If the hardware is itself evidence, an instrumentality, contraband, or a fruit of crime, agents will usually plan to seize the hardware and search its contents off-site. If the hardware is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible.[156]

When a defendant uses a computer in the transmission of child pornography, the government considers the computer an instrumentality of the crime.[157] As such, seizure of the entire computer is the usual practice.[158] Rule 41 of the Federal Rules of Criminal Procedure comports with this assessment.[159] In a case where seizure of the computer itself becomes

---

151. *See* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible, and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

152. United States v. Wolfenbarger, 696 F.2d 750, 752 (10th Cir. 1982).

153. According to the U.S. Department of Justice:

> [f]iles may be stored on a floppy diskette, on a hidden directory in a suspect's laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly tilted, stored in unusual file formats, or commingled with millions of unrelated, innocuous, and even statutorily protected files.

KERR, *supra* note 80, at 29. *See also* Erickson v. Comm'r of Internal Revenue, 937 F.2d 1548, 1554 (10th Cir. 1991) (noting that drug trafficking activity is often concealed or masked by deceptive records).

154. *See* Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 263 (2000).

155. *See* KERR, *supra* note 81, at 31.

156. *Id.*

157. *See id.; see also* Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (holding that computer equipment used to display and distribute pornographic images constitutes an instrumentality of the crime).

158. *See* KERR, *supra* note 81, at 32. When the instrumentality is not a single computer, but instead is a network, the impossibilities of seizure are obvious. In such a case, "agents will want to take a more nuanced approach to obtain the evidence they need." *Id.*

159. The rule provides:

> A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits

necessary, the Tenth Circuit requires both that the search warrant adequately describe the hardware and that the hardware seized by law enforcement officials fits within the warrant's description.[160]

B. *What Standard Applies to the Search and Seizure of Evidence Contained In Computer Hard Drives?*

1. Tenth Circuit Cases

a. *United States v. Campos*[161]

i. Facts

In *Campos*, a jury found the defendant violated a federal statute that prohibits the transmission of child pornography in interstate commerce when the defendant e-mailed pornographic images over the Internet.[162] The recipient of the images notified the FBI and gave agents copies of the e-mailed images.[163] FBI agents determined that the defendant sent the images.[164] The agents received a warrant enabling them to search the defendant's home and computer for those images.[165] The FBI found and seized the defendant's computer.[166] In examining the computer's hard drive, agents located the two pornographic images sent over the Internet, plus six more pornographic images containing children.[167] At trial, the defendant motioned to suppress the images.[168] The United States District Court for the Northern District of Oklahoma denied that motion.[169] Subsequently, a jury convicted the defendant, and the court sentenced the defendant to thirty-seven months of incarceration.[170]

ii. Decision

On appeal, the defendant argued that the search was overbroad, as agents "had grounds to search only for the two images that had been sent."[171] The Tenth Circuit disagreed, finding the warrant within permissible bounds because the warrant specified that it covered "items relating

---

of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense; or (4) person for whose arrest there is probable cause, or who is unlawfully restrained.

FED. R. CRIM. P. 41(b).

160. *See Davis*, 111 F.3d at 1478.

161. 221 F.3d 1143 (10th Cir. 2000).

162. *See Campos*, 221 F.3d at 1145 (noting the court convicted the defendant for violating 18 U.S.C. § 2252(a)(1)).

163. *See id.*

164. *See id.*

165. *See id.*

166. *See id.* at 1145-46.

167. *See id.* at 1146.

168. *See Campos*, 221 F.3d at 1146.

169. *See id.*

170. *See id.*

171. *Id.*

to child pornography."[172] The court held that although the warrant permitted agents to seize anything related to child pornography, the warrant did not authorize "an unfocused inspection of all of [the defendant's] property."[173]

The court reiterated testimony given by an FBI agent during the district court proceeding, in which the agent stated that due to the ability to conceal evidence on a computer, "all the stored data [must be examined] to determine whether it is included in the warrant."[174] The court agreed with this assessment, distinguishing this situation from its decision in *United States v. Carey*,[175] below, by stating that "the officers here did not expand the scope of their search in a manner not authorized by the warrant."[176] Rather, the search warrant in *Campos* specified the exact type of material the agents found: child pornography.[177] Thus, the court upheld the agents' search of all files on the computer hard drive.[178]

2. Analysis

The Tenth Circuit held that in order to determine which computer files fall under the scope of the search warrant, FBI agents could examine all the data stored upon the computer's hard drive.[179] Interestingly, the court noted that a computer search is constrained to information only on that hardware and does not constitute the authorization of "an unfocused inspection of all [the defendant's] property."[180]

Despite the broad search allowed in *Campos*, the court's opinion did note several restrictions on the scope of a computer search.[181] First, when an investigator finds intermingled documents, those "containing both relevant and irrelevant information," the investigator should seal those documents and await approval of a magistrate before proceeding.[182] Second, the court pointed out that its holding does not permit an officer to conduct a generalized search, where the discovery of the pornographic images is collateral to the reason for the initial search.[183] In that case, it is

172. *Id.*
173. *Id.*
174. *See Campos*, 221 F.3d at 1146.
175. 172 F.3d 1268 (10th Cir. 1999).
176. *Campos*, 221 F.3d at 1148.
177. *See id.* at 1147.
178. *See id.*
179. *See id.*
180. *Id.* at 1148.
181. *See id.*
182. *Campos*, 221 F.3d at 1148.
183. *See id.; see also* discussion *infra* Part II.D.1.b. (discussing the court of appeals' approach to an argument alleging a generalized search).

improper for law enforcement officials to delve into every file on a defendant's computer.[184]

C. *What Constitutes a "Fair Probability" that the Search of a Residence Will Uncover Material Evidence?*

The search and seizure issues associated with finding the location of a particular pornographic image are not limited to the search of computer hard drives but extend to the search of residences.[185] Where the only indication of a file's origination is the Internet e-mail address of the sender, does that provide probable cause that those images will be located at the sender's home? The Tenth Circuit determined that it does provide probable cause, holding in *United States v. Cervini*,[186] below, that a simple e-mail header provided officers with probable cause to search for pornographic images within the sender's home.[187]

1. Tenth Circuit Cases

a. *United States v. Cervini*[188]

i. Facts

In this case, the defendant posted on an Internet newsgroup web site two pornographic pictures containing children.[189] The e-mail header from the posting contained an Internet protocol address that allowed investigators to subsequently link the photos to the defendant.[190] The FBI obtained a search warrant and executed a search at the defendant's residence.[191]

Authorities indicted the defendant for "knowingly transporting and shipping child pornography in interstate commerce," in violation of federal statute.[192] In addition, authorities also indicted the defendant for "knowingly possessing an image of child pornography that was produced using materials shipped and transported in interstate commerce," also in violation of federal statute.[193]

---

184. *Compare Campos*, 221 F.3d at 1147 (inadvertent discovery of items related to child pornography during search for drug-related evidence), *with* United States v. Carey, 172 F.3d 1268, 1271 (10th Cir. 1999) (discovery of items related to child pornography pursuant to a warrant permitting a search for such items).

185. *See* United States v. Cervini, 16 Fed.Appx. 865, 867 (10th Cir. 2001).

186. 16 Fed.Appx. at 865.

187. *See id.* at 866-67.

188. 16 Fed. Appx. 865 (10th Cir. 2001).

189. *See id.*

190. *See id.* at 867.

191. *See id.*

192. *Id.* (noting authorities indicted the defendant for violating 18 U.S.C. § 2252A(a)(1)).

193. *Id.* (noting authorities indicted the defendant for violating 18 U.S.C. § 2252A(a)(5)(B)).

The defendant motioned to suppress all evidence obtained from the search of his home.[194] The defendant argued that "the affidavit in support of the warrant provided insufficient probable cause that evidence of criminal activity would be found at his residence."[195] The United States District Court for the Western District of Oklahoma denied the defendant's motion.[196]

ii. Decision

Upon review, the Tenth Circuit stated that a search warrant must only "demonstrate a 'fair probability' that a search of [the] residence would uncover evidence connecting [the defendant] to the pornographic postings."[197] The court held that the e-mail header gave officers sufficient probable cause, constituting a fair probability that officers would find contraband or other criminal evidence at the sender's residence.[198] Even if other locations existed where such images could be found, the Tenth Circuit found no requirement for the district court to "eliminate all other possible conclusions which could be derived from the alleged facts" when authorizing a search warrant.[199] The court noted that "the totality of the facts enable a reasonable person to draw the common-sense conclusion that evidence of the crime would be found at [the defendant's] residence."[200]

Under *United States v. Charbonneau*,[201] below, the United States District Court for the Southern District of Ohio determined that even an illegal search of a residence does not require suppression of seized evidence because had a legal search occurred, officers would have inevitably discovered the evidence.[202]

2. Other Jurisdictions

a. *United States v. Charbonneau*[203]

i. Facts

In *Charbonneau*, an FBI agent investigating child pornography on the Internet posed as a pedophile and monitored two private America OnLine chat rooms titled "Boys" and "Preteen."[204] Chat room members

194. *See Cervini*, 16 Fed.Appx. at 867.
195. *Id.*
196. *See id.*
197. *Id.* at 868 (quoting United States v. Simpson, 152 F.3d 1241, 1246 (10th Cir. 2000)).
198. *See id.*
199. *Id.*
200. *Cervini*, 16 Fed.Appx. at 868.
201. 979 F. Supp. 1177 (S.D. Ohio 1997).
202. *See* discussion *infra* Part II.C.2.
203. 979 F. Supp. 1177 (S.D. Ohio 1997).
204. *See Charbonneau*, 979 F. Supp. at 1179.

exchanged graphic child pornography image files.[205] The federal agent recorded the typed conversations between chat room users.[206] Chat room users e-mailed the agent pornographic images of children.[207]

The agent identified one sender, a chat room member, by his screen name.[208] Using a search warrant, the FBI identified the defendant as the sender.[209] Agents obtained a search warrant for the defendant's address.[210] The agents did not execute that search warrant.[211] Instead, the agents entered the residence after obtaining a signed consent form from the defendant's wife.[212] The agents seized two computers and several computer disks that contained child pornography.[213]

ii. Decision

The defendant motioned to suppress both the chat room conversations and the physical evidence seized from his home as a result of those conversations.[214] The defendant argued that both his freedom of speech and reasonable expectation of privacy protected his chat room conversations.[215] Finding the freedom of speech claim to be "[in]adequately supported by case law," the United States District Court for the Southern District of Ohio dismissed that claim as meritless.[216]

As to the reasonable expectation of privacy claim, the court reasoned that, like a letter, an e-mail message is protected while in the *process* of transmission.[217] However, once a recipient opens that e-mail, the expectation of privacy dissipates.[218] Making an interesting point, the court stated, "a sender of e-mail runs the risk that he is sending the message to an undercover agent."[219] Basing its decision on *Hoffa v. United States*,[220] the district court determined that no expectation of privacy exists where "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[221] In that case, the "letter" is opened, and the recipient may reveal the contents to anyone. The court noted that this rule of law applies to forwarded e-mail messages as well,

---

205. *See id.*
206. *See id.*
207. *See id.*
208. *See id.*
209. *See id.*
210. *See Charbonneau*, 979 F. Supp. at 1179.
211. *See id.* at 1180.
212. *See id.*
213. *See id.*
214. *See id.* at 1183.
215. *See id.*
216. *Charbonneau*, 979 F. Supp. at 1184.
217. *See id.*
218. *See id.*
219. *Id.*
220. 385 U.S. 293 (1966).
221. *Charbonneau*, 979 F. Supp. at 1184-85 (quoting *Hoffa*, 385 U.S. at 302).

stating that "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."[222] The court applied this reasoning to chat room transmissions, finding that "[m]essages sent to the public at large in [a] 'chat room' . . . lose any semblance of privacy."[223]

On the question of illegal search and seizure, the court determined that while the search of the defendant's home was illegal, the evidence seized was admissible under the doctrine of inevitable discovery.[224] The court determined that the agents had a valid search warrant, that absent the permission to enter, the agents would have done so anyway, and that, "the items seized would have been inevitably discovered through the execution of the search warrant."[225] The court thus denied the defendant's motions to suppress the physical evidence and statements.[226]

3. Analysis

While the Tenth Circuit has yet to rule on the issue of the expectation of privacy in e-mail communications, both the United States District Court for the Southern District of Ohio and the Sixth Circuit Court of Appeals have done so. The court in *Charbonneau* held that the Fourth Amendment does not protect e-mail messages sent to an undercover federal agent: "an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received."[227] The Sixth Circuit concurred with the latter assessment, holding that "the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter."[228] Similarly, the Court of Appeals for the Armed Forces has ruled that no expectation of privacy exists if a user forwards that original e-mail message to another person.[229]

Although no expectation of privacy exists for a received e-mail message, while an e-mail message is in transmission the sender does have an expectation of privacy.[230] The Court of Appeals for the Armed Forces has held that "the transmitter of an e-mail message enjoys a rea-

---

222. *Id.* at 1185.

223. *Id.* (quoting United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996)).

224. *See id.* at 1187. The court found the search illegal because officers obtained the consent to search through coercion. *See id.* at 1186. Among other coercive acts, the FBI agents told the defendant's wife that if she did not consent to the search, the agents would break down the front door to access their home. *See id.*

225. *Id.* at 1186-87.

226. *See id.* at 1187 (although the court granted one of the defendant's motions, the court denied both motions discussed herein).

227. *Charbonneau*, 979 F. Supp. at 1184.

228. *See* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (quoting United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995)).

229. *See* United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996).

230. *See id.* at 418.

sonable expectation that police officials will not intercept the transmission."[231]

D. *Seizure Rules When Police Discover Child Pornography While Executing a Warrant Issued for Another Purpose*

While the above cases dealt with probable cause issues surrounding the search of a computer used in connection with child pornography crimes, this section focuses on the seizure standard applied when child pornography materials are discovered during a search authorized for other purposes. Police only need to demonstrate a fair probability that child pornography is located at a defendant's residence in order to receive a search warrant to search that home.[232] In the cases below, the Tenth Circuit extended the fair probability standard to include the situation where police view possible child pornography while conducting a search for other items.[233]

1. Tenth Circuit Cases

a. *United States v. Wolfe*[234]

i. Facts

While executing a search warrant for counterfeiting evidence, which resulted in the seizure of the defendant's computer and several disks, Secret Service agents noticed three items of possible child pornography in the defendant's residence.[235] The agents chose not to seize those items.[236] After interviewing an accomplice, the agents, alerted to the possibility that the defendant was involved in child pornography, sought another search warrant.[237]

Once issued, that second search warrant permitted the agents to search the defendant's computer hard drive and the previously seized disks for evidence of child pornography.[238] The agents discovered an "extensive" number of child pornography images.[239] The government charged the defendant with possession of child pornography.[240]

At trial, the defendant asserted that the affidavit submitted in support of the second warrant was insufficient as a matter of law to establish probable cause that the defendant possessed child pornography on his

---

231. *Id.*
232. *See* United States v. Rabe, 848 F.2d 994, 997 (9th Cir. 1988).
233. *See* discussion *infra* Part II.D.3.
234. No. 00-5045, 2000 WL 1862667 (10th Cir. Dec. 20, 2000).
235. *See Wolfe*, 2000 WL 1862667, at *1.
236. *See id.*
237. *See id.*
238. *See id.* at *2.
239. *Id.*
240. *See id.* (prosecutors charged the defendant with violating 18 U.S.C. § 2252 (2000)).

computer, and thus the seized images were the result of an illegal search.[241] The government argued that the affidavit supporting the warrant was sufficient to support a probable cause finding, based both on the accomplice's statements that he had seen child pornography images on the defendant's computer, and that the defendant told the accomplice he downloaded those pictures onto his computer.[242] The United States District Court for the District of Oklahoma agreed, denying the defendant's motion to exclude that evidence.[243]

ii. Decision

The Tenth Circuit determined that "the evidence presented to the magistrate judge . . . established a fair probability that a search of [the defendant's] computer would reveal contraband within the meaning of 18 U.S.C. §§2252, 2256, such that the magistrate had a 'substantial basis' to determine that probable cause existed to issue the second search warrant."[244] Namely, the three items of possible child pornography that the agents observed in the defendant's home, plus the accomplice's statement that he had seen an image of a nude child on the defendant's computer monitor, and that the defendant told the accomplice he had more pictures on his computer, together established "a 'fair probability' that evidence of possession of child pornography would be found on the hard drive of [the defendant's] personal computer" or disks.[245]

Obtaining a second search warrant is required; in *United States v. Carey*,[246] below, the Tenth Circuit suppressed child pornography images seized collateral to an original search warrant where, unlike here, authorities did not seek a second search warrant.[247]

b. *United States v. Carey*[248]

i. Facts

During his arrest, the defendant, a cocaine dealer, consented to a search of his apartment.[249] The defendant also consented in writing to the removal of any property under his control, "if said property shall be essential in the proof of the commission of any crime in violation of the Laws of the United States."[250] As a result of that search, the police seized two computers under the belief that the computers "would either be sub-

241. *See Wolfe*, 2000 WL 1862667, at *2.
242. *See id.* at *1-*2.
243. *See id.* at *2.
244. *Id.* at *3.
245. *Id.* at *4.
246. 172 F.3d 1268 (10th Cir. 1999).
247. *See Carey*, 172 F.3d at 1271, 1276.
248. 172 F.3d 1268 (10th Cir. 1999).
249. *See id.* at 1270.
250. *Id.*

ject to forfeiture or [provide] evidence of [the defendant's] drug dealing."[251]

The police obtained a warrant to search "the [two] computers for 'names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'"[252] In the course of that warrant's execution, the police discovered a large number of "files with sexually suggestive titles and the label 'JPG.'"[253] The police copied those files to a floppy disk and opened them on another computer.[254] The police discovered numerous images containing child pornography.[255]

The defendant "was charged with . . . possessing a computer hard drive that contained three or more images of child pornography produced with materials shipped in interstate commerce."[256] The defendant moved to suppress the seized evidence, arguing that the police seized the hard drive as a result of an illegal "general, warrantless search,"[257] and that "files not pertaining to the sale or distribution of controlled substances were opened and searched, and [therefore] . . . should have been suppressed."[258] The United States District Court for the District of Kansas denied that motion to suppress.[259]

ii. Decision

On appeal, the defendant argued that despite the clear specificity of the warrant, the detective searched files that were outside the scope of the search warrant.[260] The government counter-argued that the plain view doctrine permitted the file discovery.[261] Under the plain view doctrine,

> [a] police officer may properly seize evidence of a crime without a warrant if:
>
> (1) the officer was lawfully in a position from which to view the object seized in plain view; (2) the object's incriminating character was immediately apparent -- i.e., the officer had probable cause to believe

---

251. *Id.*

252. *Id.*

253. *Id.* "JPG" is a code appended to a file's name (a "filename extension"), which designates that the file has been compressed by a method developed by the Joint Photographic Experts Group. *See* Joint Photographic Experts Group, *at* http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Joint+Photographic+Experts+Group (Sept. 11, 2000). JPG is one of a number of compression schemes used to reduce the size of digital images for easy electronic transmission. *Id.*

254. *See Carey*, 172 F.3d at 1271.

255. *See id.*

256. *Id.* at 1270 (noting that prosecutors charged the defendant with violation of 18 U.S.C. § 2252A(a)(5)(B)).

257. *Id.*

258. *Id.* at 1272.

259. *See id.* at 1271.

260. *See Carey*, 172 F.3d at 1272.

261. *See id.*

> the object was contraband or evidence of a crime; and (3) the officer had a lawful right of access to the object itself.[262]

The Tenth Circuit did not agree that the plain view doctrine applied, reasoning that while the detective did not expect to find child pornography upon opening the first image file, after that point he had probable cause to suspect that the rest of the image files contained child pornography.[263] However, the detective improperly, and illegally, continued his search.[264] "When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant."[265] He knew he would find additional pornographic images.[266] Therefore, the files were not "inadvertently discovered"; they were illegally seized.[267] Following reasoning set out by the United States Supreme Court in *Coolidge v. New Hampshire*, where the Supreme Court determined that "the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges,"[268] the Court of Appeals for the Tenth Circuit suppressed those files, stating that "closed files . . . [are] not in plain view."[269]

The Tenth Circuit disagreed with the government's argument that the defendant's consent to search his apartment implicitly included his computer files' contents.[270] Because the police had the computers in their custody, their search needed to proceed more cautiously.[271] The Tenth Circuit concluded that the police "exceeded the scope of the warrant" and should have used a more narrowly tailored method to search the drive.[272] The court suggested several less intrusive methods, including "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[273] Although the court based its decision only on the facts at issue, it implied that when the police remove a computer from a defendant's home pursuant to a valid search warrant, the subsequent search of that computer must not expand into a general search.[274]

A situation where the computer remains in the defendant's control is distinguishable from this case, where authorities removed the computer because "no 'exigent circumstance or practical reason [permitted] offi-

---

262. *Id.* (citing United States v. Soussi, 29 F.3d 565, 570 (10th Cir. 1994)).
263. *See id.* at 1273.
264. *See id.*
265. *Id.* at 1274.
266. *See Carey*, 172 F.3d at 1274.
267. *Id.* at 1273.
268. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).
269. *Carey*, 172 F.3d at 1272-73.
270. *See id.* at 1274.
271. *See id.* at 1276.
272. *Id.*
273. *Id.*
274. *See id.* at 1273.

cers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant.'"[275] The Court of Appeals for the Tenth Circuit suggested that had the computers remained in the defendant's apartment, the detectives permissibly could have searched each file or proceeded in a less circumspect manner.[276] Courts likely would distinguish this situation from the situation where detectives search for child pornography under a warrant.[277] In that case, the detectives could search each file.[278] The United States District Court for the Eastern District of Virginia, below, failed to base its decision on a warrant's scope; when searching for specific information, irrespective of the underlying crime, the search of a computer may include all of its files.[279]

2. Other Jurisdictions

a. *United States v. Gray*[280]

i. Facts

Pursuant to a warrant, FBI agents conducted a search at the defendant's home for information relating to computer intrusions at the National Library of Medicine.[281] The agents seized four computers and copied their hard drives onto CD-ROMs.[282] Following the FBI's Computer Analysis and Response Team practices, an agent opened and briefly reviewed each file in the directories and subdirectories, both to aid in the discovery of warrant-specified material and to determine how many files would fit on each CD-ROM.[283] The agent opened approximately eighty percent of the files on each hard drive.[284]

During that process, the agent discovered a folder entitled "Tiny Teen."[285] He opened the folder "because it was the next [one] listed and he was opening all of the [folders] as part of his routine search for the items listed in the warrant."[286] While the agent knew that the files he was searching for were likely text files, he opened "picture files because computer files can be misleadingly labeled, particularly if the owner of

275. *Carey*, 172 F.3d at 1275-76 (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 107 (1994)).

276. *See id.*

277. *See supra* text accompanying note 184.

278. *See supra* text accompanying notes 183-84.

279. *See* United States v. Gray, 78 F. Supp. 2d 524, 528-29 (E.D. Va. 1999).

280. 78 F. Supp. 2d 524.

281. *See Gray*, 78 F. Supp. 2d at 526.

282. *See id.*

283. *See id.* The Computer Analysis and Response Team is an FBI unit specializing in the forensic examination of computers. *See FBI Laboratory: Computer Analysis and Response Team*, *at* http://www.fbi.gov/hq/lab/org/cart.htm (last visited Feb. 18, 2002).

284. *See Gray*, 78 F. Supp. 2d at 527.

285. *See id.*

286. *Id.*

those files is trying to conceal illegal materials."[287] The agent discovered pornographic pictures, some of which he thought contained images of minors.[288] The agent obtained a second search warrant that authorized a search of the defendant's computer files for evidence of child pornography.[289] The defendant sought to suppress all the images discovered on the computer, contending that the search of the folders "was beyond the scope of the [original search] warrant."[290]

ii. Decision

The United States District Court for the Eastern District of Virginia disagreed.[291] While holding that a search warrant must be particular to be executable, the court noted that

> [i]n some searches, however, it is not immediately apparent whether or not an object is within the scope of a search warrant; in such cases, an officer must examine the object simply to determine whether or not it is one that he is authorized to seize. . . . As a result, in any search for records or documents, "innocuous records must be examined to determine whether they fall into the category of those papers covered by the search warrant."[292]

The court held that an agent, acting under the authorization of a search warrant "to search a home or office for documents containing certain specific information [is] entitled to examine all files located at the site to look for the specified information."[293] Thus, the district court determined that the law permitted the agents to look at each file.[294] In addition, the court held that if, in the course of that search,

> an agent sees, in plain view, evidence of criminal activity other than that for which she is searching, this does not constitute an unreasonable search under the Fourth Amendment, for "[v]iewing an article that is already in plain view does not involve an invasion of privacy."[295]

The court thus permitted seizure of those pornographic pictures under the "plain view" exception and held that the investigator's search and seizure of the images contained in the "Tiny Teen" folder "was not beyond the scope of the search warrant."[296]

---

287. *Id.* at 527 n.5. *See also supra* note 153.
288. *See Gray*, 78 F. Supp. 2d at 527.
289. *See id.* at 527-28.
290. *Id.* at 528.
291. *See id.* at 531.
292. *Id.* at 528 (quoting United States v. Kufrovich, 997 F. Supp. 246, 264 (D. Conn. 1997)).
293. *Id.* at 528.
294. *See Gray*, 78 F. Supp. 2d at 531.
295. *Id.* at 528 (quoting United States v. Jackson, 131 F.3d 1105, 1108 (4th Cir. 1997)).
296. *Id.* at 528-29.

3. Analysis

In the conclusion of *Carey*, the Tenth Circuit stated:

> [The detective's] seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search, and the district court erred by refusing to suppress it. Having reached that conclusion, however, we are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.[297]

Foreshadowing the situation in *United States v. Campos*,[298] Justice Baldock's concurrence stated, "if the record showed that [the agent] had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would be required."[299] The distinction here is that had the agent continued to find evidence of child pornography collaterally, while remaining within the scope of his original search warrant, that collateral discovery of pornography would have been admissible.[300] Where, as here, the detective exceeded the scope of the search warrant, the court found the evidence inadmissible.[301]

When authorities conduct a warranted search in a child pornography case, authorities must open and examine each file, to counter the "hiding" issues.[302] That search may turn up additional evidence of child pornography that the Court would find permissible.[303] The Court places a restriction upon this search when authorities find the pornographic material collateral to an investigation.[304] In that case, the investigator must stop and obtain a search warrant before proceeding.[305] The United States District Court for the Eastern District of Virginia, however, sees this issue differently and, in *Gray*, permitted the type of search disallowed by the Tenth Circuit.[306]

III. CONCLUSION

During this past year, the Tenth Circuit made several changes in how it interprets and applies the law concerning child pornography. The

---

297. United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999).

298. 221 F.3d 1143 (10th Cir. 2000).

299. *Carey*, 172 F.3d at 1277 (Baldock, J., concurring). *Cf.* discussion *supra* Parts II.B.2. and II.B.3.

300. *See Carey*, 172 F.3d at 1276-77 (Baldock, J., concurring). *Cf.* discussion *supra* Parts II.B.2. and II.B.3.

301. *See Carey*, 172 F.3d at 1276.

302. *See* KERR, *supra* note 81, at 29.

303. *See* United States v. Gray, 78 F. Supp. 2d 524, 527 n.5, 531 (E.D. Va. 1999).

304. *See Carey*, 172 F.3d at 1277 (Baldock, J., concurring).

305. *See id.*

306. *See Gray*, 78 F. Supp. 2d at 530-31.

Court made these changes in response to concerns Congress expressed when enacting the Sex Crimes Against Children Prevention Act.[307] The essence of Congress' worry was that the nexus of child pornography and computers may produce particularly harmful effects. Not only might children be enticed to engage in pornographic activity by merely viewing pornographic images but, due to the ease with which a computer allows people to copy and disseminate images over a virtually limitless market, a computer's use may increase the overall number of images disseminated.[308] In response to Congress' concerns, the Tenth Circuit expanded its interpretation of solicitation of a minor by computer, supported sentence-level enhancements for child pornography defendants who used computers to commit their crimes, expanded traditional search and seizure standards by employing a fair probability standard to determine the appropriateness of complete search of a computer, and supported Internet-use restrictions on paroled child pornographers.

While Congress' concerns are legitimate, the changes wrought by the Court of Appeals' new interpretations are worrisome. Although we no longer live in a society where "an eye for an eye" is our basis for determining punishment, we must strike a proper balance between actual harm and its subsequent punishment. Perceived harm alone should not form that basis. However, according to the Sentencing Commission, such perceived harm may do just that.[309] "[T]he federal cases sentenced to date typically do not involve the type of computer use that would result in either wide dissemination or a likelihood that the material will be viewed by children."[310] The Sentencing Commission made that statement in early 1996, when the Sentencing Commission examined each of the 423 cases involving sex offenses against minors that came before the federal courts during 1994 and 1995.[311] These cases were likely the same cases Congress had in mind when stating its reasoning for enacting the Sex Crimes Against Children Prevention Act. Congress' fears thus may be unfounded, or at minimum, unrepresentative of the entire body of child pornography defendants using computers.

The changes brought about by the Sex Crimes Against Children Prevention Act have materially affected defendants' rights and sentencing. At least two circuit courts, the Tenth Circuit and the Sixth Circuit, have relied upon Congress' concerns when interpreting child pornography laws. If Congress' underlying fears are either unfounded or unrepresentative of the whole, then the Sixth and Tenth circuits have expanded laws and limited rights based upon faulty or misguided policy. Applying

---

307. Pub. L. No. 104-71, 109 Stat. 774 (1995) (codified as amended at 18 U.S.C. § 2423; 28 U.S.C. § 994).

308. *See* H.R. REP. NO. 104-90, at 3-4 (1995), *reprinted in* 1996 U.S.C.C.A.N. 759, 760-61.

309. *See* U. S. SENTENCING COMM'N, *supra* note 6, at i.

310. *Id.*

311. *See id.*

such inroads to all child pornographers using computers may therefore be excessive, overreaching, and out of balance with the harm caused by such computer use.

When the actual effect of that law abridges fundamental rights, as here, Congress should reassess the law. While Congress has powerful reasons to diminish a sex offender's rights, fear of the possible should not become the basis for decision-making. Congress should reassess its reasoning behind the passage of the Sex Crimes Against Children Prevention Act, in light of the act's effect upon current case law. If Congress finds its concerns currently founded, the changes should remain. Otherwise, Congress and the courts should limit the application of the Sex Crimes Against Children Prevention Act to situations where a defendant *actually* used a computer to entice minors to engage in pornographic activity or to disseminate images containing child pornography.

Anton L. Janik, Jr.[*]

---

* J.D. Candidate 2003, University of Denver College of Law.