Digital Child Pornography and the Fourth Amendment ©[1]

by

Thomas K. Clancy[2]

The advent of digital evidence is having a profound impact on Fourth Amendment principles and analysis. Yet to be resolved by the courts is the fundamental question whether locations where digital evidence may be found, ranging from desk top computers, cell phones, to countless other digital devices, are subject to special rules or whether traditional search and seizure rules suffice.[3] There is, however, another fundamental trend influencing the development of Fourth Amendment principles to digital evidence that has not been much noted for its impact: Almost 70 per cent of all reported appellate decisions involving the search or seizure of digital evidence are concerned with the recovery of child pornography. {See accompanying chart}

The alcohol prohibition era had a significant influence on Fourth Amendment analysis in the 1920s and 1930s. The drug wars of the last 50 years have also impacted the structure of search and seizure jurisprudence. Now, during the digital age, governmental investigations designed to locate child pornography are having a similar influence. This article highlights some of the more important aspects of the trends in the case law.

***Analytical Structure of Fourth Amendment Claims*[4]**

The Fourth Amendment is the most implicated and litigated portion of the Constitution. In analyzing any case involving a Fourth Amendment claim, three separate questions must be answered. First, is the Amendment applicable? The applicability question, in turn, is a two–sided inquiry: (a) does the governmental activity–which must be either a search or a seizure–invade (b) an individual interest protected by the Amendment? If the Amendment does not apply, that ends

the inquiry; it does not matter if the governmental actions are reasonable or not. Second, if the Amendment does apply, is it satisfied? If it is found that the Amendment is applicable but not satisfied, a third question must be answered: what is the remedy, if any, for the violation? That third question is *not* a Fourth Amendment issue, given that the Supreme Court has stated that the exclusionary rule is not constitutionally mandated.[5]

***Step #1*. Does the Fourth Amendment apply to Internet Child Pornography Investigations?**

Unless governmental activity that would otherwise be labeled a "search" or "seizure" invades a protected interest, the Amendment does not apply and there is no inquiry into the reasonableness of those activities. Digital child pornography cases have examined both aspects of the applicability question.

Part A: Does the governmental activity constitute a "search"?

Private Searches. The Fourth Amendment is applicable only to governmental activity; it does not regulate private searches and seizures.[6] As a consequence, a rather complex jurisprudence has developed to distinguish between governmental searches and private party searches.[7] Private parties often report their discovery of child pornography to the police.[8] A surprising common situation involves computer repair shops. Child pornographers are unlikely to give up their images once they are collected.[9] As a result, employees of repair shops often discover images when computers are brought in for repair. Courts have consistently held that observations made by those private computer technicians do not implicate the Fourth Amendment.[10] The computer technician then typically calls the police, who often replicate the prior examinations, expand that prior examination by looking for more images, or ask the repair person to look for more images. These three scenarios result in disparate legal results. If the police merely replicate the prior private

search, what the police observe is not a search within the meaning of the Fourth Amendment.[11] The courts have engaged in a confusing analysis, with disparate results, if the police not only replicate the prior search but also look for and find more images.[12] On the other hand, when a repairman copies files based on a state trooper's request, a search within the meaning of the Amendment has occurred.[13] **Part B: Does that activity invade an individual's protected interest?**

If the individual does not have a protected interest, actions that might otherwise be labeled a search or seizure do not implicate the Fourth Amendment. To have a protected interest as to a search, courts employ a two-pronged test, which requires that a person exhibit a subjective expectation of privacy, which must be recognized by society as legitimate.[14] Pursuant to that test, the Supreme Court has created a hierarchy of expectations, with long lists of situations where it has found either no reasonable expectation of privacy or a reduced one.[15] If no reasonable expectation of privacy is found (and no other protected interest is present), the Amendment is inapplicable to regulate the government action.[16] If a court finds a reduced expectation of privacy, the governmental intrusion has been almost uniformly upheld, with the court utilizing a test for reasonableness favorable to the government.[17]

Peer-to-Peer Distribution Schemes. The overwhelming distribution scheme of choice for child pornographers is the use of peer-to-peer networks.[18] A person seeking to trade child pornography can download for free software that permits him to configure his computer to join such networks and share files.[19] One file sharing program is called *Limewire.*

> LimeWire is a file-sharing program that can be downloaded from the internet free of charge; it allows users to search for and share with one another various types of files, including movies and pictures, on the computers of other persons with LimeWire. Once a user downloads the program onto his computer, the user can click on an icon that connects his computer to others on the network. Users can input search terms and receive a list of responsive files available on other computers connected to the network.[20]

Law enforcement is well aware of such networks and task forces and police departments are engaging in operations to identify persons utilizing peer-to-peer technology to trade illicit images. The government agents join such networks, search for files, and determine which constitute child pornography. The caselaw is uniform that persons who put files in a folder that others can access to share on peer-to-peer networks do not have a reasonable expectation of privacy in such files.[21] The same analysis applies to local networks.[22] In response to one claim that the police had invaded his reasonable expectation of privacy, the court stated:

> The crux of Ganoe's argument is that he simply did not know that others would be able to access files stored on his own computer. But he knew he had file-sharing software on his computer; indeed, he admitted that he used it–he says to get music. Moreover, he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network. Ganoe thus opened up his download folder to the world, including Agent Rochford. To argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes.[23]

Once a file is located, there are a few steps that must be taken to identify the computer that holds the file;[24] agents thereafter employ a warrant, consent, or (hopefully) otherwise seek to comply with Fourth Amendment satisfaction standards to search the computer. Government agencies have software tools available to them that permit searches of large numbers of computers on a P2P network and have the ability to catch thousands of offenders.[25] The techniques, used for years, are now being widely exploited by authorities and large numbers of offenders are being identified as a result.

Step #2. <u>If the Amendment applies, is it satisfied?</u>

There have been many Fourth Amendment satisfaction issues litigated in the context of digital child pornography. Highlighted here are two. The concept of probable cause–a familiar but fluid standard for a court to apply[26]–has created some unique difficulties in the computer context.[27]

Once again, the bulk of the case law concerns child pornographers. The courts have been troubled by two nexus questions: 1) as to subscribers of child pornography web sites, the amount of information needed in order to conclude that there is probable cause to search the subscriber's computer; and 2) as to distributors or recipients of child pornography, establishing the location of the computer used to distribute or receive the materials.

There is a split of authority over the strength of the inference that can be drawn as to whether a person has child pornography on his computer based on membership in a child pornography web site. Some courts have indicated that mere membership in a child pornography site is sufficient.[28] Others have rejected that view.[29] To establish probable cause to search, many courts look for additional information–beyond membership in a child pornography site–that substantiates the person's sexual interest in children or in child pornography.[30] That additional information has included such factors as evidence of actual downloading[31]–as opposed to mere viewing,[32] automatic transmissions as part of the site's services,[33] use of suggestive names,[34] expert information on the retention habits of child pornography collectors[35] (which often serves to dispel allegations of staleness[36] and identifies the house as the place where the materials were viewed), and prior convictions involving sex offenses involving children or child pornography.[37]

Another significant question is ascertaining the location of the computer that has distributed or received the child pornography. This difficulty arises because many individuals use computers in a variety of locations, including in an office and at home.[38] Computers accessing the Internet are assigned an Internet Protocol number, which does "*not directly* reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the internet."[39] As a result, "law enforcement officials must conduct research and rely upon the

addresses and data provided by internet providers, . . . as well as billing addresses for those service providers and/or credit card companies."[40]

Some courts will infer that the computer is located in the home from the Internet Protocol address assigned to the user's account[41] and other courts will find probable cause to search the billing address associated with the screen name.[42] Still other courts have rejected the view that a registered screen name is sufficient to establish probable cause to search the subscriber's computer.[43] Instead, it has been sometimes suggested that additional information is needed, such as the fact that the suspect maintained a computer or computer-related equipment at the place to be searched that was capable of transmitting child pornography, the screen name required a particular password, the transmission of child pornography was to a unique Internet or ethernet address assigned to a particular computer at the location to be searched, or the person occupying the place to be searched had an "extreme" interest in young children or had access to Internet sites operated by entities that required those having access to maintain Internet-accessible child pornography.[44] Also relevant to the probable cause determination are the habits of child pornography collectors, which includes a propensity to collect child pornography and maintain the collection at home, and whether the suspect was a pedophile.[45]

Conclusion

Courts are increasingly confronting the problems associated with adapting Fourth Amendment principles to modern technology. Supreme Court jurisprudence, developed to regulate traditional search and seizure practices, presents conceptual problems when applied to the world of cyber-space and electronically stored evidence. Some authorities are reluctant to accept–or outright reject–analogies to physical world searches and seizures. I have concluded elsewhere, however, that

there is nothing "special" in the nature of computer searches that differentiate them in any principled way from other document and container searches.[46] The Supreme Court will have had its first opportunity to address aspects of that question by the time this article appears.[47] That decision does not involve child pornography; nonetheless, in addressing search and seizure claims involving digital evidence, they are most often addressed in that context.

1. © Copyright, Thomas K. Clancy, 2010.

2. Director, National Center for Justice and the Rule of Law, Research Professor, University of Mississippi School of Law. email: tclancy@olemiss.edu

3. *See generally* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005).

4. *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION Ch. 1 (Carolina Academic Press 2008) www.cap-press.com/books/1795.

5. The exclusionary sanction is a judicially created remedy and is not a personal constitutional right. United States v. Leon, 468 U.S. 897, 906 (1984).

6. *See, e.g.,* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

7. Whether a person is acting as an agent of the government "necessarily turns on the degree of the Government's participation in the private party's activities, [which] can only be resolved 'in light of all of the circumstances.'" Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989).

8. Spouses, parents, and others who share joint access to the offender's computer are significant sources. Other common private searches involve hackers. *See* United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003); United States v. Steiger, 318 F.3d 1039, 1042-46 (11th Cir. 2003); Jarrett v. Commonwealth, 594 S.E.2d 295, 301-03 (Va. App. 2004).

9. *E.g.,* Sisson v. State, 903 A.2d 288, 298 (Del. Sup. 2006).

10. *See, e.g.,* State v. Horton, 962 So. 2d 459, 464-66 (La. App. 2007); United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); United States v. Barth, 26 F. Supp. 2d 929, 932-35 (W.D. Tex. 1998). *Cf.* Rogers v. State, 113 S.W.3d 452, 457-48 (Tex. App. 2003) (no reasonable expectation of privacy in computer files that defendant had requested repairman to copy); Commonwealth v. Sodomsky, 939 A.2d 363 (Pa. Sup. Ct. 2007) (person who brought computer to repair shop abandoned any expectation of privacy in child pornography files).

11. *E.g.*, United States v. Grimes, 244 F.3d 375, 377-83 (5th Cir. 2001); People v. Emerson, 766 N.Y.S.2d 482, 486-87 (Monroe County 2003).

12. *See* Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. at 228-44.

13. *Hall*, 142 F.3d at 993. *See also Barth*, 26 F. Supp. 2d at 935-36 (although computer repairman acting in private capacity when he observed first file containing child pornography, after he related his observations to a FBI agent who asked him to copy the entire hard drive, observations of additional files were as government agent).

14. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating that the test "embraces two discrete questions").

15. *See generally* CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION at § 3.3.3.

16. *E.g.*, United States v. Barrows, 481 F.3d 1246 (10th Cir. 2007) (no reasonable expectation of privacy in personal computer brought to work and installed in public space when no precautions taken to shield child pornography files).

17. *E.g.*, People v. Thornburg, 895 N.E.2d 13 (Ill. App. 2008) (agreement to probation condition regarding searches of computer acted to eliminate expectation of privacy in search that uncovered child pornography); State v. Williams, 146 P.3d 481 (Wash. App. 2006) (reduced expectation of privacy in computer due to civil commitment to a special commitment center); United States v. Yuknavich, 419 F.3d 1302, 1309-11 (11th Cir. 2005 (reduced expectation of privacy of probationer justified search of his computer based on reasonable suspicion).

18. Other preferred ways to use the Internet to trade and distribute child pornography include websites designed for that purpose and chat rooms, which are used to establish contacts and followed by transmission or trading of images. *See, e.g.*, United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000).

19. *See, e.g.*, Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 100-01 (2000) (cataloguing reasons for explosion of Internet child pornography).

20. United States v. Ganoe, 538 F.3d 1117, 1119 (9th Cir. 2008).

21. *Id.*; United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008).

22. *See* United States v. King, 509 F.3d 1338, 1342 (11th Cir. 2007) (military base computer network, with the court stating: "The contents of his computer's hard drives were akin to items stored in the unsecured common areas of a multi-unit apartment building or put in a dumpster accessible to the public.").

23. Ganoe, 538 F.3d at 1127.

24. *See, e.g.*, United States v. Craighead, 539 F.3d 1073 (9th Cir. 2008).

25. *E.g.*, United States v. Borowy, __ F.3d __, 2010 WL 537501 (9th Cir. 2010).

26. *E.g.*, Brinegar v. United States, 338 U.S. 160, 175 (1949) (probable cause determinations "are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act").

27. As with other situations, probable cause determinations in the computer context are fact-bound. *See, e.g.*, Williford v. State, 127 S.W.3d 309, 313 (Tex. App. 2004) (probable cause to seize computer based on repairman's viewing of thumbnail picture of two naked boys on bed); Burnett v. State, 848 So. 2d 1170, 1173-75 (Fla. App. 2003) (no probable cause to support warrant to search computer for evidence of child pornography based on initial complaint that suspect had made lewd videotape of two children); State v. Staley, 548 S.E.2d 26, 28-29 (Ga. App. 2001) (although police had probable cause to believe that Staley had molested a specific child, that he had worked as a computer analyst, that he had been previously convicted of molesting a child and taking pictures of that child, and that the affiant detailed that pedophiles stored information relating to having sex with children, there was no nexus between either the crime of molesting that specific child or the propensities of child sex offenders and search of computer in Staley's apartment); Burke v. State, 27 S.W.3d 651, 653-56 (Tex. App. 2000) (fact-bound question whether there was probable cause to issue warrant in child pornography case).

A persistent question concerns the circumstances under which file names establish probable cause to search or seize a computer; a finding of probable cause generally turns on the explicit nature of the names and the surrounding circumstances. *See, e.g.*, State v. Wible, 51 P.3d 830, 833-34 (Wash. App. 2002) (file names "8 year old Rape" and "8 year old Smile" gave context and meaning to repairman's tip that computer contained child pornography).

28. *See* United States v. Gourde, 440 F.3d 1065, 1070-72 (9th Cir. 2006) (en banc) (membership in Internet child pornography site for at least three months was sufficient to establish probable cause of downloading child pornography onto home computer); United States v. Martin, 426 F.3d 83 (2d Cir. 2005), *rehearing en banc denied*, 430 F.3d 73 (2d Cir. 2005); United States v. Wagers, 452 F.3d 534, 540 (6th Cir. 2006) (probable cause existed that suspect's home computer contained child pornography based on membership in child pornography website); U.S. v. Bailey, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003) (holding that "knowingly becoming a computer subscriber to a specialized Internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer"). *Cf.* United States v. Coreas, 419 F.3d 151 (2d Cir. 2005) (affirming on basis of precedent but asserting that mere membership should not be the basis for probable cause), *rehearing en banc denied*, 430 F.3d 73 (2d Cir. 2005).

29. *See* United States v. Perez, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003) (subscription to known child pornography website created a "chance, but not a fair probability, that child pornography would be found").

30. *See, e.g.*, United States v. Froman, 355 F.3d 882, 884-91 (5th Cir. 2004) (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names, "Littlebuttsue" and "Littletitgirly"); State v. Schaefer, 668 N.W.2d 760, 770 (Wis. App. 2003) (because computer files are common way of storing photographs, reasonable inference that computer contained child pornography when suspect actively cultivated friendship of teenage boys by inviting them to use his home computer, used his computer to communicate with others interested in stories about adults sexually assaulting children, and visited Internet sites where child pornography was available for downloading).

31. *Perez*, 247 F. Supp. 2d at 483-84 (rejecting finding of probable cause and noting, *inter alia*, that, unlike other cases where there was evidence of downloading, the affidavit contained "nothing concrete to suggest that Perez had transmitted or received images of child pornography").

32. *See id.* at 483-84 n.12 ("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.'"). *See also* United States v. Zimmerman, 277 F.3d 426, 435 (3rd Cir. 2002) (without evidence that pornography was specifically downloaded and saved to defendant's computer, offending images "may well have been located in cyberspace, not in [the defendant's] home"); United States v. Tucker, 305 F.3d 1193, 1198 (10th Cir. 2002) (upholding conviction for possession of files automatically stored in browser cache because defendant's habit of manually deleting images from cache files established his control over them).

The analysis of federal courts should change because the federal statute has been amended to prohibit mere access with intent to view child pornography images. *See* 18 U.S.C. § 2252A(a)(5)(A). This is to say that possession does not have to be the central inquiry and, for probable cause to search a computer, intentional access with intent to view would be a reasonable conclusion based on membership. *See* Gourde, 440 F.3d at 1070 (membership in child pornography website "manifested his intention and desire to obtain illegal images"). Most states, however, still require possession. *See* Rebecca Michaels, Note, *Criminal Law–The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should be Criminal*, 30 W.N. ENG. L. REV. 817 (2008).

33. *See Perez*, 247 F. Supp. 2d at 485 (asserting that "the agents either had or could have had, before they requested the warrant, all the Yahoo logs, which provided extensive information--whether a subscriber was offered e-mail delivery options; whether he elected a delivery option; whether he uploaded or posted any images; when he subscribed; and whether he unsubscribed"). *Cf. Froman*, 355 F.3d at 884-91 (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names,

"Littlebuttsue" and "Littletitgirly").

34. *E.g.*, United States v. Shields, 458 F.3d 269, 279-80 (3rd Cir. 2006) (maintaining that suggestive email address added to probable cause determination).

35. *See, e.g.*, United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause found in child pornography case when affiant, based on her training and experience, explained that collectors and distributors of child pornography typically store it in their homes); United States v. Cox, 190 F. Supp. 2d 330, 333 (N.D.N.Y. 2002) (recognition of habits of child pornography collectors); State v. Lindgren, 687 N.W.2d 60, 64-65 (Wis. App. 2004) (when defendant took nude photographs of a 14 year old female employee at work, touched her vaginal area, and had allegedly taken pictures of other female employees, and affiant detailed habits and characteristics of child molesters, including, *inter alia*, that they collect sexually explicit materials, rarely dispose of them, and record diaries of their encounters on, *inter alia*, their computers, probable cause existed to search home computer for photographic evidence of underage children of sexually explicit nature); State v. Evers, 815 A.2d 432, 446, 448 (N.J. 2003) (probable cause to believe that pornographic images of children would be retained on computer due to retention habits of child pornographers).

An explanation of child pornography collectors' retention habits was offered in *United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y. 1996):

> Since the [child pornographic] materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

But see United States v. Greathouse, 297 F. Supp. 2d 1264, 1272 (D. Or. 2003) (even though agent indicated in affidavit that child pornography collectors routinely maintain their materials for long periods of time, rejecting that assertion as sufficient because it appeared "to be based upon a generalized sense developed through informal conversations with other agents").

36. Staleness claims are common in child pornography cases but typically rejected due to the nature of digital evidence and the habits of collectors. *E.g.*, United States v. Lemon, 590 F.3d 612 (8th Cir. 2010); United States v. Paull, 551 F.3d 516 (6th Cir. 2009); United States v. Morales-Aldahondo, 524 F.3d 115 (5th Cir. 2008); Mehring v. State, 884 N.E. 2d 371, 377-80 (Ind. App. 2008); State v. Pickard, 631 S.E.2d 203 (N.C. App. 2006); State v. Felix, 942 So. 2d 5, 9-10 (Fla. App. 2006). Even long periods of time between the initial report of the existence of child pornography and the execution of a subsequently issued warrant have not defeated the existence of probable cause. *E.g.*, *Hay*, 231 F.3d at 636 (probable cause that computer in suspect's home contained child pornography was not stale, even though information was six months old, due to affiant's explanation that collectors and distributors rarely if ever dispose of it and store it in secure place); United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause not stale in child pornography case when based on information 10 months old because affiant, based on her training and experience, explained that collectors and distributors of child pornography "rarely if ever" dispose of such material);

Lamb, 945 F. Supp. at 460-61 (based, *inter alia*, on proposition that pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant period of time, five month delay from last transmission of child pornography to issuance of warrant did not render probable cause stale); *Schaefer*, 668 N.W.2d at 767 (information that suspect possessed child pornography in 1998, some of which went back to 1990, not stale based on protracted and continuous nature of habits of preferential child offenders, who rarely dispose of sexually explicit materials); Hause v. Commonwealth, 83 S.W.3d 1, 13-14 (Ky. App. 2002) (based on "hoarding" characteristics of child pornography collectors, information that was 178 days old not stale). *But cf. Zimmerman*, 277 F.3d at 433-34 (probable cause based on viewing of pornographic video file on defendant's computer six months prior to execution of search warrant was stale, absent evidence that defendant had downloaded the video clip and absent evidence of continuous criminal activity); *Greathouse*, 297 F. Supp. 2d at 1272-73 ("Carefully considering all of the factors present in this case, including the limited incriminating evidence, the absence of any evidence of intervening criminal activity, the absence of any evidence that [the suspect] was a pedophile, and the fact that computer equipment becomes obsolete very quickly, I find that the thirteen month delay in this case is simply too long. If a line must be drawn in internet child pornography cases, I find that the line is one year absent evidence of ongoing or continuous criminal activity.").

37. *See, e.g.*, United States v. Wagers, 452 F.3d 534 (6th Cir. 2006); United States v. Fisk, 255 F. Supp. 2d 694, 706 (E.D. Mich. 2003) (when the defendant had prior conviction for unlawful sexual involvement with a minor, had wired money to purveyor of child pornography, and when the purveyor sold that pornography over the Internet, there was probable cause to believe that computer contained child pornography).

38. *See, e.g.*, State v. Evers, 815 A.2d 432, 446 (N.J. 2003) ("Computers are in use in both homes and businesses, and, with the advent of the laptop, in almost every other conceivable place. Business people and students leave their homes with laptops, use them at other locations, and return home with them.").

39. United States v. Wagers, 339 F. Supp. 2d 934 (E.D. Ky. 2004), *aff'd*, 452 F.3d 534 (6th Cir. 2006). Internet protocol (IP) numbers are owned by Internet service providers; each number is unique to each computer while it is online. Terrence Berg, *Practical Issues in Searching and Seizing Computers*, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 27, 37 n.22 (2004). However, IP numbers can be either "dynamic" or "static." A dynamic number, typically used by persons who have dial-up Internet service, changes each time the user goes online: "it is only good for that transaction, and then returns to the pool of numbers after the transaction is over." *Id*. On the other hand, a static IP number, which is more commonly used with cable and DSL connections, is permanently assigned to a customer. *Id*.

40. United States v. Wagers, 339 F. Supp. 2d 934 (E.D. Ky. 2004), *aff'd*, 452 F.3d 534 (6th Cir. 2006).

41. *E.g.*, United States v. Perez, 484 F.3d 735, 739-44 (5th Cir. 2007); State v. Felix, 942 So. 2d 5 (Fla. App. 2006); State v. Brennan, 674 N.W.2d 200 (Minn. App. 2004). *See also* Ellis v. State, 971 A.2d 379, 389 (Md. App. 2009) (finding reasonable inference that defendant used his home

computer from the circumstances); State v. Byne, 972 A.2d 633, 637-42 (R.I. 2009) (in video voyeurism case, analogizing to child pornography cases to find nexus between taking pictures with a digital camera and the home); State v. Samson, 916 A.2d 977, 981-83 (Me. 2007) (finding reasonable nexus between home and digital child pornography pictures taken by defendant).

42. *See, e.g., Evers*, 815 A.2d at 446 ("the billing address of the Internet screen name–a screen name that had e-mailed photographs of child pornography–was the logical place to search for evidence of the identity of the holder of the screen name and evidence of the crime").

43. *See, e.g.,* Taylor v. State, 54 S.W.3d 21 (Tex. App. 2001) (no probable cause to search computer for child pornography in Taylor's home when affidavit merely alleged that one image of child pornography sent over the Internet had been traced to screen name registered to Taylor).

44. *See, e.g., id*. at 25-26 (collecting cases). *See also* United States v. Grant, 218 F.3d 72, 75 (1st Cir. 2000) (because use of password-protected account requires that user know password associated with account, fair probability that person using account is registrant).

45. *See, e.g., Taylor*, 54 S.W.3d at 25-26. *See also* Berg, *supra* note ___, at 42-45 (arguing that there are "good reasons" to follow the *Taylor* court's approach, including the fact that email headers can be forged, that the information given to an ISP regarding the user's billing address does not mean that a computer is present at that address, and that, with current technology, ISPs can determine the phone numbers and times when the account was accessed).

46. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 1 at 196-220.

47. City of Ontario v. Quon, 529 F.3d 892 (9th Cir. 2008), *cert. granted*, 130 S. Ct. 1011 (December 14, 2009) (expectations of privacy of users in records held by a provider of pager services to a police department).