"One Click, You're Guilty": A Troubling Precedent for Internet Child Pornography and the Fourth Amendment

Eric R. Diez

Follow this and additional works at: http://scholarship.law.edu/lawreview

Recommended Citation
Available at: http://scholarship.law.edu/lawreview/vol55/iss3/9
COMMENTS

"ONE CLICK, YOU’RE GUILTY":1 A TROUBLING PRECEDENT FOR INTERNET CHILD PORNOGRAPHY AND THE FOURTH AMENDMENT

Eric R. Diez

“Child pornography is so repulsive a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules. If they do so, however, they endanger the freedom of all of us.”2

The explosive growth of the Internet has fueled an astounding surge in online child pornography.3 An industry once confined to underground mail-order catalogs and the bold attempts of individuals to produce and share homemade child pornography4 has evolved into vast online communities; chat rooms; and the instantaneous, electronic publication of child pornography.5 Today's law enforcement agencies and judges

2. United States v. Coreas, 419 F.3d 151, 151 (2d Cir. 2005).
4. Silberman, supra note 1, at 157. At one point, the child pornography industry was driven so far underground that practically “the only publishers of child-porn magazines left in the US were law enforcement agencies, who used them as bait in sting operations.” Id. The government was limited to targeting parents who used their own children to manufacture pornographic videos rather than those who obtained the material elsewhere and merely “possessed” it. Id.
5. PHILIP JENKINS, BEYOND TOLERANCE 39-40 (2001) (explaining that adult stores were driven out of business when child pornography was criminalized, but “private mail-order suppliers” remained); see also STEPHEN T. HOLMES & RONALD M. HOLMES, SEX CRIMES 128-30 (2d ed. 2002) (noting that Internet chat rooms and bulletin boards have allowed pedophiles to interact amongst themselves and with children anonymously and easily). With the invention of the web browser enabling graphical navigation of the
face a new threat that is testing their ability to adhere to traditional Fourth Amendment principles in an increasingly technological society.\(^6\)

In 1995, the FBI formed its Innocent Images National Initiative (IINI) specifically to combat Internet child pornography.\(^7\) Six years later, it conducted an enormous nationwide child pornography sting operation.\(^8\) FBI Agent Geoff Binney, while searching for web sites that contained child pornography, subscribed to a suspicious Yahoo! e-group\(^9\) called Internet in the 1990s, "[i]mages that once were accessible to only a self-selecting few were now a search engine away from any casual netsurfer." Silberman, supra note 1, at 157.

\(^6\) See JENKINS, supra note 5, at 16 ("[A] sizable technological gap exists between criminals and law enforcement, to the advantage of the lawbreakers."). Judge Rakoff, a district judge sitting by designation for the Second Circuit Court of Appeals, best highlighted the legal dilemma that law enforcement officials now face: "Child pornography is so repulsive a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules." Coreas, 419 F.3d at 151.

\(^7\) Fed. Bureau of Investigation, Innocent Images National Initiative, http://www.fbi.gov/publications/innocent.htm (last revised Jan. 24, 2006). One of the missions of the IINI is to "[e]stablish a law enforcement presence on the Internet as a deterrent to subjects that exploit children." FED. BUREAU OF INVESTIGATION, U.S. DEPT OF JUSTICE, INVESTIGATING CRIMES AGAINST CHILDREN, http://www.fbi.gov/hq/cid/cac/bicac.pdf (last visited Mar. 11, 2006). The IINI conducts undercover operations in "each of the FBI's 56 field offices." Id. Undercover agents within IINI typically use fictitious names to engage suspected pedophiles in online chat or e-mail conversations. Id. The agents frequently pose as minors to try and set up meetings with adults with whom they have interacted online. Silberman, supra note 1, at 128.

\(^8\) Press Release, Fed. Bureau of Investigation, Innocent Images: Operation Candyman: Phase I (Mar. 18, 2002) (on file with the Catholic University Law Review), available at http://www.criminology.fsu.edu/transcrime/articles/FBI%20-%20Operation%20Candyman.htm (last visited Mar. 29, 2006). As of March 18, 2002, the FBI claims: FBI Houston is coordinating a Nationwide enforcement action against certain individuals who have been associated with Egroup, Candyman. To date, 231 searches have been executed, 86 individuals have been charges [sic] in over 26 states, 27 of these individuals admitted to the prior molestation of over 36 children. Many more arrests are anticipated during the week of 03/18/2002 and coming months. Id.

\(^9\) Silberman, supra note 1, at 128. An e-group is an interactive community that is topically organized according to the group creator's interests, for example "Business and Finance" or "Cultures and Community." JENKINS, supra note 5, at 59; cf. Yahoo! Groups Homepage, http://groups.yahoo.com (last visited Nov. 22, 2005) (highlighting Yahoo! Groups' description and topical directory). An e-group may also be called a Yahoo! Group, group, or Egroup; the terms are used interchangeably by various sources and for purposes of this Comment. A potential member generally finds a group by searching the e-groups site using keywords, or by browsing through the topical directory. See Yahoo! Help—Groups, http://help.yahoo.com/help/us/groups/groups-19.html (last visited Mar. 11, 2006). Generally, there is no cost to join, no credit card or personal information required, and most e-groups use a similar template that includes standard interactive features such as a message board, chat room, file uploads, polls, and other customizable sections as the creator determines. Cf. id. Many e-groups function similarly to a listserv, where members can post an e-mail message that is sent to all members of the group who elect to receive
"Candyman." While joining, the group provided Agent Binney with three ways to access content on the site: 

1. Agent Binney elected to receive e-mails automatically, and soon began receiving e-mails with images containing child pornography from the e-group's members. Agent Binney was a member of Candyman for just over one month before Yahoo! shut the group down.

Agent Binney subpoenaed a list of Candyman members from Yahoo!, and Yahoo! provided the e-mail addresses of all 3397 members. Without obtaining any individualized download statistics, and even such e-mails. Cf. Coreas, 419 F.3d at 152 (discussing the e-mail options available to Agent Binney upon joining Candyman). The e-mails can contain file attachments such as images. See United States v. Martin, 426 F.3d 68, 70 (2d Cir. 2005). A person joins a group most commonly by simply clicking a button on the site. Yahoo! Help—Groups, supra (noting that joining by clicking the button in the group is the preferred method of subscribing, but joining by sending a blank e-mail to a specified e-mail address, or joining by invitation is also possible). When joining via the button on the group site, the site presents each member with the option of receiving e-mails or not receiving e-mails from the group. See id.

10. Coreas, 419 F.3d at 152 (stating that the e-group contained a welcome splash screen that read: "This group is for People who love kids. You can post any type of messages you like too or any type of pics and vids you like too. P.S. IF WE ALL WORK TOGETHER WE WILL HAVE THE BEST GROUP ON THE NET.")

11. Id. If one selected option (1), to receive all e-mails automatically, e-mails sent out to the group also contained image attachments, but one who selected option (2) or (3) received no attachments at all. See id.

12. See id. (noting that from the time Agent Binney joined until the Candyman group shut down, Agent Binney "received 498 e-mail messages" containing 105 images of child pornography).

13. Id. Agent Binney joined the site on January 2, 2001, and Candyman shut down on February 6, 2001. Id. Agent Binney requested that Yahoo! keep the site open to membership, but Yahoo! did not respond and shut the site down. United States v. Froman, 355 F.3d 882, 886 & n.2 (5th Cir. 2004).

14. See Coreas, 419 F.3d at 152; Froman, 355 F.3d at 886. Based on the e-mail addresses of the members turned over by Yahoo!, Agent Binney subpoenaed the internet service provider (ISP) records for "[g]roup members' names, addresses, phone numbers, and any other identifying information," but not information pertaining to the members' downloading (or lack thereof) of child pornography. Froman, 355 F.3d at 886.

15. Cf. Coreas, 419 F.3d at 153 (mentioning that "the Government had no knowledge of what [defendant] had received—even though . . . this was information it could readily have obtained from Yahoo if it had sought to do so"); United States v. Perez, 247 F. Supp. 2d 459, 485 (S.D.N.Y. 2003) (stating that it was possible for the government to obtain "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").
though eighty-five percent of the members elected not to receive the e-mail communications that Agent Binney had subscribed to, law enforcement officers obtained and executed search warrants for hundreds of Candyman members and other e-groups implicated by the operation. It later came to light that Agent Binney made several false statements on his search warrant affidavit.

The federal circuit courts are just beginning to issue decisions in the aftermath of the Candyman and similar sting operations. The courts face two important issues: (1) whether membership to a web site that contains child pornography, without more individualized evidence of possession of child pornography, is enough to constitute probable cause to search a defendant’s home; and (2) whether probable cause exists to search a defendant’s home after redacting the false statements from

16. Coreas, 419 F.3d at 154; Perez, 247 F. Supp. 2d at 467-68 (indicating that the “vast majority” of subscribers opted out of receiving automatic e-mails); see also United States v. Kumen, 323 F. Supp. 2d 390, 392 (E.D.N.Y. 2004).

17. Coreas, 419 F.3d at 152; see also United States v. Martin, 426 F.3d 68, 70-72 (2d Cir. 2005) (identifying “Candyman,” “girls12-16,” and “shangri_la” as the three groups implicated by Agent Binney’s investigation). Local FBI offices used Agent Binney’s statements as a foundation to prosecute other e-group defendants. See Froman, 355 F.3d at 886 (noting that local FBI field offices used the original Binney affidavit as a template to “fill the gaps in the affidavit with the suspect specific information” for other search warrant applications); United States v. Coye, No. 02-CR-732 (FB), 2004 U.S. Dist. LEXIS 14979, at *1-2 (E.D.N.Y. Aug. 4, 2004) (order denying motion for reconsideration) (mentioning that Agent Binney’s “affidavit underlies all of the search warrants and subsequent prosecutions in the Candyman cases”).

18. Coreas, 419 F.3d at 152-53 (stating that Agent Binney falsely claimed that (1) “he had joined Candyman by sending an e-mail message to the group’s moderator, a step he asserted was required of all new subscribers” and (2) “all Candyman members automatically received all messages and files sent to the group by other members”). In reality, members could join by clicking a single “join” button and would not be able to view the content within the site until after doing so. Id. at 153; see also United States v. Strauser, 247 F. Supp. 2d 1135, 1145 (E.D. Mo. 2003) (noting that a person could have subscribed without knowing what content existed beyond the welcome screen).

19. See Martin, 426 F.3d at 70-71 (detailing two e-groups in addition to Candyman, “girls12-16” and “shangri_la,” which Agent Binney’s investigation also encompassed).

20. See Coreas, 419 F.3d at 155. Due to the sheer number of pending Candyman and Binney-related appeals, this Comment will limit itself to discussion of free e-group cases, but the debate over the probable cause determination easily translates to the realm of paid subscription web sites. See United States v. Gourde, 382 F.3d 1003, 1005, 1008 (9th Cir. 2004), reh’g granted, 416 F.3d 961 (9th Cir. 2005) (noting that the defendant subscribed using his credit card to a “mixed” site containing “both legal adult pornography and illegal child pornography”). Gourde suppressed the evidence obtained during the search for lack of probable cause, but the Ninth Circuit recently ordered that the case be reheard en banc. See Gourde, 416 F.3d at 961.
Agent Binney's affidavit. There is a trend toward upholding these convictions, but district and circuit courts have issued harsh dissents.

This Comment examines the difficulty that circuit courts have experienced adjudicating the cases resulting from Agent Binney's affidavit, namely, how to determine whether probable cause exists to support the search of a house of a suspected member of a child pornography web site or e-group. First, this Comment introduces the case law surrounding Fourth Amendment searches and the probable cause requirement. Second, this Comment discusses the current split of authority in determining if probable cause exists to search the home of an alleged member of a child pornography web site, and the consequences of false statements made by an officer in the affidavit for the search warrant. Third, this Comment argues that, under current Supreme Court precedent, membership to an e-group found to contain child pornography, without more evidence of actual possession, is not sufficient to find probable cause to search the home of the member. Fourth, this Comment analyzes the varied factors that courts have found important in determining probable cause in e-group cases, and incorporates them into a new test for determining when probable cause exists to search the home of a member of an e-group that contains child pornography.

I. CHANGING TIMES BRING ABOUT STRICTER PUNISHMENTS FOR CHILD PORNOGRAPHERS

A. Statutory Law Prohibiting Child Pornography

Since 1977, Congress has passed numerous laws of increasing severity that define and regulate child pornography. Motivated by its findings

21. See Coreas, 419 F.3d at 155; infra Part I.B.2.b.ii.
22. See infra Part I.B.3; infra notes 87, 89 and accompanying text.
that child pornography was a "highly organized, multi-million-dollar industry" prevalent within the country, and that victims included large numbers of "runaway and homeless youth," Congress raised the age of a child for the purposes of defining child pornography from sixteen to eighteen via the Child Protection Act of 1984. With the advent of the personal computer in the 1980s, Congress passed the Child Protection and Obscenity Enforcement Act of 1988, which made it illegal to use a computer to transport, distribute, or receive visual depictions of child pornography. After computer software became a recognized media for digitally altering images to "convey the impression" of child pornography, Congress passed the Child Pornography Prevention Act of 1996 (CPPA). The CPPA was aimed at banning virtual child pornography, or the digital creation of images that resemble, but are not, child pornography. To date, 18 U.S.C. § 2256 defines "child pornography" as "any visual depiction . . . of sexually explicit conduct" involving a minor. Downloading child pornography from the Internet falls within § 2252A(a)(5)(B), which punishes the knowing possession of "any . . . material that contains an image of child pornography." Most of the Candyman and other e-group prosecutions have been grounded on this provision. Despite laws bestowing tougher penalties and definitions
broadening their scope, child pornography is now a billion dollar industry that legislators are still struggling to remedy.31

B. The Probable Cause to Search Requirement

1. Probable Cause to Search a Person's House and Personal Effects Is a Requirement That Is Embedded in the Roots of Fourth Amendment Jurisprudence

The English common law practice of issuing broad general warrants and writs of assistance was the impetus behind the drafting of the Fourth Amendment of the U.S. Constitution.32 The Fourth Amendment expressly forbids "unreasonable searches" of "persons, houses, papers, and effects."33 Supreme Court jurisprudence has developed this principle to protect a person's "actual . . . expectation of privacy" that "society is prepared to recognize as 'reasonable.'"34 Thus, the home and the objects within it are historically, textually, and judicially presumed to be places where one has a reasonable expectation of privacy.35

The Fourth Amendment further states that "no Warrants shall issue, but upon probable cause."36 Before an officer may search an area where


32. See Steagald v. United States, 451 U.S. 204, 220 (1981) (citing Payton v. New York, 445 U.S. 573, 608-09 (1980) (White, J., dissenting)); Boyd v. United States, 116 U.S. 616, 624-29 (1886) (quoting James Otis in his portrayal of the writs of assistance as "'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book'"'). Justice Stevens has also proclaimed that "indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." Payton, 445 U.S. at 583.

33. U.S. CONST. amend. IV; see also Perez, 247 F. Supp. 2d at 461 ("[T]he potential for unreasonable intrusions into the home—the chief concern of the drafters of the Fourth Amendment— is great.").

34. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Justice Harlan's concurrence, which has become the standard inquiry to determine if a search has occurred, also stressed that "a man's home is, for most purposes, a place where he expects privacy." Id. at 361.

35. But cf. id. at 351 (majority opinion) (qualifying that the Fourth Amendment protects "people, not places"). Although courts presume that a person has a reasonable expectation of privacy in a person's home, the Supreme Court has also stated that "[w]hat a person knowingly exposes to the public, even in his own home . . . is not a subject of Fourth Amendment protection." Id.

36. U.S. CONST. amend. IV.
one has a reasonable expectation of privacy, the officer must determine that probable cause exists to justify the intrusion and obtain a search warrant. Probable cause supports a search warrant when "the facts and circumstances within an officer's personal knowledge . . . are sufficient in themselves to warrant a person of reasonable caution in the belief that . . . a specifically described item subject to seizure will be found in the place to be searched." It requires a magistrate to conduct a fact-intensive inquiry on a case-by-case basis and use common sense judgment to determine if there is a "fair probability" that probable cause exists to support the search of a place described in the officer's affidavit. The standard has long required that the officer applying for the warrant have more than a bare suspicion, but does not demand enough evidence to condemn the accused. While the probable cause determination is objective, a magistrate may consider an officer's personal observations, experience, 

37. See Katz, 389 U.S. at 361 (Harlan, J., concurring) ("[T]he invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant."); see also Illinois v. Gates, 462 U.S. 213, 276 (1983) (Brennan, J., dissenting) (citing Nathanson v. United States, 290 U.S. 41, 46-47 (1933)). The Nathanson Court held that "[u]nder the Fourth Amendment, an officer may not properly issue a warrant to search a private dwelling unless he can find probable cause therefor from facts or circumstances presented to him under oath or affirmation. Mere affirmation of belief or suspicion is not enough." Nathanson, 290 U.S. at 47.


40. Gates, 462 U.S. at 238. Since law enforcement officers are "engaged in the often competitive enterprise of ferreting out crime," the magistrate must be neutral and detached. Id. at 240 (quoting Johnson v. United States, 333 U.S. 10, 13-14 (1948)).


42. Brinegar, 338 U.S. at 175 (asserting that the probabilities involved with a probable cause determination include the "factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act"); see also DRESSLER, supra note 38, § 9.02[B] (stating that the "officer's subjective belief, no matter how sincere, that she has sufficient cause to . . . conduct a search does not in itself constitute probable cause").
and training in evaluating whether probable cause is present. Courts presume affidavits to be trustworthy because they are submitted under oath, and an officer's personal observation of what he attests to reinforces his basis of knowledge.

2. Limits of the Probable Cause Determination

a. Individualized Suspicion and Probable Cause Determinations Based on "Mere Propinquity"

Although an officer is afforded some latitude to rely on his experience when applying for a search warrant, there are limits to this freedom. Justice Ginsburg broadly stated in *Chandler v. Miller* that the Fourth Amendment "generally bars officials from undertaking a search or seizure absent individualized suspicion." While some searches may be upheld without individualized suspicion, those occur only in "certain
limited circumstances," not relevant to a search of a home for evidence of child pornography.\(^4\)

In 1979, the Supreme Court in *Ybarra v. Illinois*\(^5\) held that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."\(^5\) The *Ybarra* rule withstands scrutiny and has justified a finding of lack of probable cause even in the following scenarios: where an affidavit alleged that a group had a "reputation for violence, property destruction and sabotage";\(^5\) where a group of officers was alleged to have stolen money and items from suspects;\(^5\) and where a warrant authorized the search and seizure of "indicia of membership in or association with the Hell's Angels [Motorcycle Club]," which was suspected of racketeering activity.\(^5\)

An exception to the mere propinquity rule occurs when the individual has continuously remained a member of a "wholly illegitimate" organization where "membership itself necessarily implies criminal conduct."\(^5\) However, *United States v. Brown* refused to declare a group

---

49. Id. (quoting Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 668 (1989)) (listing fixed border patrol checkpoints, sobriety checkpoints, and administrative inspections of "closely regulated" businesses as the only searches not requiring particularized suspicion). *Chandler* examined the constitutionality of a Georgia statute that required candidates for certain state offices to pass a suspicionless drug test. Id. While the facts in *Chandler* are of a different subject matter from those in child pornography cases, Justice Ginsburg phrased her sentence broadly enough to encompass searches of a defendant's home and personal effects in internet child pornography cases. Cf id. (interpreting the Fourth Amendment broadly insofar as it "generally bars officials from undertaking a search or seizure absent individualized suspicion").


51. Id. at 91 (citing Sibron v. New York, 392 U.S. 40, 62-63 (1968)).

52. See Mendocino Envtl. Ctr. v. Mendocino County, 192 F.3d 1283, 1294-95 (9th Cir. 1999) (finding that "information about a group's reputation is legally insufficient to support probable cause that a member of that group is involved in criminal activities"); see also LAFAVE, * supra* note 39, § 3.6(c), at 307-10.

53. See United States v. Brown, 951 F.2d 999, 1000 (9th Cir. 1991).

54. United States v. Rubio, 727 F.2d 786, 790, 794 (9th Cir. 1983). *Brown* also cited *Rubio*, reiterating that "proof of mere membership in the Hell's Angels [motorcycle club], without a link to actual criminal activity, was insufficient to support a finding of probable cause." *Brown*, 951 F.2d at 1002 (citing *Rubio*, 727 F.2d at 793). Instead, the *Rubio* court required, and failed to find, a "nexus" between the member's association with the group and the alleged criminal activity. *See Rubio*, 727 F.2d at 794 ("The facts in the affidavits are limited to the establishment of association with the enterprise.").

55. *Brown*, 951 F.2d at 1003 (""If such a large portion of the subject organization's activities are illegitimate so that the enterprise could be considered, in effect, wholly illegitimate, then there would certainly be cause to believe that evidence of a suspect's association with that enterprise would aid in a . . . conviction." (second alteration in original) (quoting *Rubio*, 727 F.2d at 793)); see also 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 3.6(c), at 336 (4th ed. 2004) ("Continuous membership in a group which has
wholly illegitimate where only some of the members participated in the illicit activity. Thus, organizations where only some of the members participate in the illicit activity in question do not meet the wholly illegitimate standard; searches of those members must arise from suspicion individualized to the particular member.

Several courts in recent e-group child pornography cases have cited or relied on either Chandler or Ybarra to different ends. One Fourth Circuit case arising from the FBI e-group sting operations avoided the "mere membership" issue by finding probable cause based on other facts and circumstances particular to the defendant. Other courts have evaded the Ybarra rule entirely (over dissent, in United States v. Martin). In those cases, rather than examining the composition of the group and the ratio of illicit to legitimate activity within, the courts have tethered a probable cause finding to the e-group's explicit welcome message and the notice such a message provides to potential members.

---

56. See Brown, 951 F.2d at 1003 ("The fact that the Government had information that [the group's legitimate responsibilities were] accompanied by thefts on the part of some of the team members did not transform this law enforcement unit into a 'wholly illegitimate' enterprise." (emphasis added)).

57. See Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person."). Ybarra further states that particularized suspicion may not be "avoided by simply pointing to the fact that coincidentally there exists probable cause to search ... the premises where the person may happen to be." Id. Ybarra reiterated the Gates proposition that the Fourteenth Amendment protects "the 'legitimate expectations of privacy' of persons, not places." Id.

58. See, e.g., United States v. Coreas, 419 F.3d 151, 156-57 (2d Cir. 2005) (expressing frustration at a Second Circuit panel's failure to follow the "well settled" precedent of Ybarra); United States v. Froman, 355 F.3d 882, 889-91 (5th Cir. 2004) (referencing Chandler but still finding probable cause); United States v. Kunen, 323 F. Supp. 2d 390, 400 (E.D.N.Y. 2004) ("Even if, arguendo, a 'majority' of Candyman members are more likely than not to have child pornography on their computers at any given time, that does not, standing alone, cause the entire membership to be fair game for search warrants."); United States v. Perez, 247 F. Supp. 2d 459, 482 n.10 (S.D.N.Y. 2003) (agreeing with the government's concession that "mere membership ... in the Ku Klux Klan would not constitute probable cause to search an individual's home for evidence of civil rights violations"). The Kunen court further stated that "the primary focus for probable cause ... must be on the individual, as an individual, rather than as a member of a group." Kunen, 323 F. Supp. 2d at 400-01.

59. United States v. Ramsburg, 114 F. App'x 78, 81-82 (4th Cir. 2004) (per curiam) (noting that "another e-mail address registered to [defendant] had transmitted an image of child pornography to an agent several years earlier").

60. 426 F.3d 68, 81-82 (2d Cir. 2005) (Pooler, J., dissenting).

61. See id. at 75 (majority opinion). The girls12-16 welcome message stated: Hi all, This group is for all those ho [sic] appreciate the young female in here [sic] finest form. Watching her develop and grow is like poetry in motion [sic], to an
An issue related to the mere membership rule that has given courts pause in e-group cases is the labeling of all members of the e-group in question as “collectors” of child pornography. In his affidavit, Agent Binney included an extensive discussion about “the characteristics of child-pornography collectors,” stating that they “rarely, if ever, destroy [their illicit collections].” Judge Pooler’s dissent in *United States v.*
Martin\textsuperscript{64} and the panel in United States v. Coreas\textsuperscript{65} both address the fact that a defendant's mere association with a group that subsequently is found to contain child pornography does not make the defendant a "collector" by implication.\textsuperscript{66} The United States v. Strauser\textsuperscript{67} Court was also hesitant to classify its defendant as a collector based on the mere joining of a group by the click of a button on a web site.\textsuperscript{68} In contrast, the Martin majority did not address whether the members of the web site actually had a proclivity to collect child pornography, but merely accepted it to be true in concert with the totality of the circumstances, which implied that the overriding purpose of the site was illicit.\textsuperscript{69}

\textsuperscript{64} 426 F.3d 68 (2d Cir. 2005).
\textsuperscript{65} 419 F.3d at 151 (2d Cir. 2005).
\textsuperscript{66} See Martin, 426 F.3d at 82 (Pooler, J., dissenting) ("The majority exaggerates the relevance of the corrected affidavit's descriptions of 'child pornography collectors'... by improperly inferring that all subscribers to the E-group are collectors of illegal visual depictions."); Coreas, 419 F.3d at 156 ("[T]he only evidence [that the defendant is a collector of child pornography] in the excised affidavit is his mere act of responding affirmatively to the invitation to join Candyman."); see also Strauser, 247 F. Supp. 2d at 1137 ("Other than the fact that Strauser had subscribed to Candyman on December 26, 2000, and had not 'unsubscribed' as of February 6, 2001, however, there was nothing to indicate that he was a 'collector or distributor of child pornography.'").
\textsuperscript{67} 247 F. Supp. 2d at 1135.
\textsuperscript{68} Id. at 1144 (rejecting the government's argument that "only persons interested in child pornography would subscribe and not 'unsubscribe,'" and that such persons are tantamount to collectors). The Strauser court theorized that, given the ease of subscription, one could accidentally stumble upon the material. Id.
\textsuperscript{69} Martin, 426 F.3d at 75 ("[T]he affidavit... described the characteristics and proclivities of child-pornography collectors, specifically how they tend to collect such material, store it, and rarely destroy or discard it." (emphasis added) (citation omitted)). Martin refrained from any discussion as to whether the defendant was actually a collector. See id. at 79 (Pooler, J., dissenting) (accusing the majority of making inferential leaps when it concluded that Martin was a collector of child pornography).
b. Knowingly or Recklessly Making False Statements in the Affidavit and the Leon Good Faith Exception

i. A Franks Hearing Is Required To Determine Whether a False Statement Was Made Knowingly or in Reckless Disregard for the Truth

A false statement in an affidavit can have grim exclusionary consequences for a government's case-in-chief. However, the Supreme Court of the United States provides one exception where the evidence may still be admissible as proof of guilt. Under the "Leon good faith exception," evidence derived from a defective warrant is still admissible for proof of guilt if the officer reasonably relied on the warrant. Notwithstanding this good faith exception, the Court listed four exceptions to the good faith exception where the Court will not defer to the judgment of the magistrate. The first exception (and the only one relevant to the sting operations in question) is where the issuing magistrate relies on false information provided by the officer knowingly or in reckless disregard for the truth. This exception evolved from the Supreme Court's concerns in Franks v. Delaware, where the Court held that an officer's false statements in an affidavit can be fatal to a warrant if they were made knowingly or in "reckless disregard for the truth." Under the two-pronged Franks v. Delaware approach, the defendant

---

70. See Franks v. Delaware, 438 U.S. 154, 155-56 (1978) (holding that a consequence of an offending warrant may be suppression of the fruits of the search).

71. United States v. Leon, 468 U.S. 897, 922 (1984); DRESSLER, supra note 38, §§ 21.06[A][1], 21.06[A][3][a] (noting that originally, evidence obtained in cases where the warrant was invalid for lack of probable cause would only be admissible for impeachment purposes).

72. United States v. Taylor, 119 F.3d 625, 629 (8th Cir. 1997); see also DRESSLER, supra note 38, § 21.06[A][1].

73. Leon, 468 U.S. at 922. Leon makes clear that the standard is objective. Id. at 919.

74. Id. at 914-15, 923. Professor Dressler describes these scenarios as ones where "a reasonably well-trained officer would not rely on a warrant." DRESSLER, supra note 38, § 21.06[A][3][a], at 404.

75. See Leon, 468 U.S. at 914.


77. Id. at 155-56. Most circuits use a subjective approach to determine if an affiant made a statement in reckless disregard for the truth, inquiring whether the affiant "entertained serious doubts as to the truth" of the statements. United States v. Kunen, 323 F. Supp. 2d 390, 395 (E.D.N.Y. 2004) (quoting United States v. Schmitz, 181 F.3d 981, 987 (8th Cir. 1999)); accord United States v. Cican, 63 F. App'x 832, 835 (6th Cir. 2003); United States v. Ranney, 298 F.3d 74, 78 (1st Cir. 2002); United States v. Williams, 737 F.2d 594, 602 (7th Cir. 1984); United States v. Davis, 617 F.2d 677, 694 (D.C. Cir. 1979). The Second Circuit has not addressed the issue. Kunen, 323 F. Supp. 2d at 395.

must first “make[] a substantial preliminary showing” that the false statements were made knowingly or in “reckless disregard for the truth.” If the defendant meets both prongs, the court must grant the defendant a Franks hearing to determine if the defendant’s allegations are true. At the hearing, the defendant must show by a preponderance of the evidence that the affiant made false statements knowingly or in reckless disregard for the truth. If the defendant is successful, the court will redact the false statement(s) from the record and determine if probable cause exists based on the corrected affidavit. If, after this analysis is complete, the court finds there is no probable cause, “the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.”

ii. Courts Disagree on the Threat Posed by False Statements to a Probable Cause Determination in E-group Child Pornography Cases

Agent Binney made several false statements on his affidavit, namely, that each member “automatically received every e-mail message and file transmitted to the Candyman Egroup by any Candyman Egroup member.” Two schools of thought have emerged in response to the discovery of these false statements. Most courts are finding that probable cause existed with mere membership in the e-group, valid search warrant can demand an evidentiary hearing to determine if there has in fact been government misconduct”); United States v. Fairchild, 122 F.3d 605, 610 (8th Cir. 1997).

79. Franks, 438 U.S. at 155; accord Fairchild, 122 F.3d at 610; Owen, 621 F. Supp. at 1504. The allegation may not be conclusory and “must be supported by more than a mere desire to cross-examine.” United States v. Levasseur, 619 F. Supp. 775, 778 (E.D.N.Y. 1985); see also LAFAVE, supra note 39, § 4.4(b), at 488 & n.27 (citing a digest of cases holding that “[a]llegations of negligence or innocent mistake are insufficient”).

80. See Franks, 438 U.S. at 156; Fairchild, 122 F.3d at 610; Owen, 621 F. Supp. at 1504.

81. Franks, 438 U.S. at 156; Owen, 621 F. Supp. at 1504. An “allegation of perjury or reckless disregard” for the truth may be substantiated at the hearing. Levasseur, 619 F. Supp. at 778.

82. Franks, 438 U.S. at 156.

83. Id.

84. Id.

85. United States v. Perez, 247 F. Supp. 2d 459, 462 (S.D.N.Y. 2003); accord United States v. Coreas, 419 F.3d 151, 153 (2d Cir. 2005); United States v. Strauser, 247 F. Supp. 2d 1135, 1141 (E.D. Mo. 2003). Agent Binney also misrepresented the method by which he joined the e-group in his affidavit, stating that he joined by “sending an e-mail” to the group’s moderator; in actuality, server records later indicated that he clicked a “join” button. Coreas, 419 F.3d at 152-53.

86. See infra notes 87, 89 and accompanying text.
notwithstanding the redaction of Agent Binney’s false statements. Martin held that even without the false statements, facts supported the probable cause determination because “common sense” and the totality of the circumstances indicated that being a member of the e-group implied usage of the site.

However, the other school of thought, adopted by a smattering of district courts around the country, is that there was no probable cause after redacting the false statements. After a rehearing, the Eastern District of Missouri in Strauser found that Agent Binney’s false statements were recklessly made, and without that information there was no probable cause to issue a warrant. The Strauser court emphasized that after the false information was redacted, “the only information regarding [the defendant was] that an email account registered to [the defendant] subscribed to Candyman on December 26, 2000, and was still a member on February 6, 2001, when the site was shut down, and that the same email account had [a sexually suggestive] screen name.”

A major concern for Judge Perry was that Agent Binney had to have seen the screen prompting him to select a mode of receiving e-group postings at least seven times before he applied for a search warrant. Therefore, the

87. See, e.g., United States v. Martin, 426 F.3d 68, 74-75 (2d Cir. 2005); United States v. Schmidt, 373 F.3d 100, 103 (2d Cir. 2004) (per curiam) (stating in dicta that “we would be inclined to agree with the majority of courts to have decided this precise issue that, even excluding the misstatements, the affidavit demonstrated probable cause to search”); United States v. Froman, 355 F.3d 882, 891 (5th Cir. 2004); United States v. Hutto, 84 F. App’x 6, 8 (10th Cir. 2003); United States v. Shields, No. 4:CR-01-0384, 2004 U.S. Dist. LEXIS 7090, at *24 (M.D. Pa. Apr. 14, 2004) (amended order denying motion to suppress evidence); United States v. Bailey, 272 F. Supp. 2d 822, 837 (D. Neb. 2003).

88. Martin, 426 F.3d at 74-75 (2d Cir. 2005).

89. See, e.g., United States v. Kunen, 323 F. Supp. 2d 390, 400-01 (E.D.N.Y. 2004) (finding no probable cause for one of the four defendants in the case “absent the erroneous information about all members receiving all e-mails”); Strauser, 247 F. Supp. 2d at 1143-44; Perez, 247 F. Supp. 2d at 486.

90. Strauser, 247 F. Supp. 2d at 1136.

91. Id. at 1144.

92. Id. at 1143. Judge Perry found that Agent Binney exceeded the level of mere negligence when he made the statements, thus meeting the first prong of the Franks test. Id. at 1142. Judge Perry elaborated:

[T]he only information available to [Agent Binney] contradicted [the assumption that all subscribers received automatic e-mails]: he had to click on a screen that required him to specify whether or not he wanted all emails, so it is clearly unreasonable to assume that everyone else had done what he did and asked to receive all emails. Indeed, based on what he knew about child pornographers, he should have considered it more likely that most subscribers would not have wanted all the emails to be automatically sent . . . .

. . . Based on all the evidence before me, which I have extensively reviewed multiple times, . . . I find that Binney was reckless because he had obvious reasons to doubt the accuracy of the information he provided.
Court concluded that Agent Binney's false statements regarding each member having received the same e-mails he did were made recklessly. The Court then found that after these statements were redacted, the affidavit could not support probable cause. The Court declared the warrant invalid and suppressed the evidence derived from the search.

Judge Chin in the Southern District of New York agreed. In *United States v. Perez*, Judge Chin conducted a lengthy and technical analysis of Agent Binney's testimony in another Candyman case to determine if Agent Binney made the statements knowingly or in reckless disregard for the truth. Regarding the false statements, the court held that "the agents acted with reckless disregard for the truth when they erroneously represented . . . that all Candyman members automatically received every e-mail transmitted to the Candyman Egroup and that every Candyman member automatically received images of child pornography transmitted to the group." Judge Chin noted that after the court redacted the false statements, the affidavit contained no particularized evidence indicating that Perez had actually received visual depictions of child pornography. The only particularized information was: (1) that the defendant's e-mail address was used to join Candyman, (2) that the e-mail address was registered to defendant's name, and (3) that the defendant resided at the premises listed on the warrant. Moreover, the site was not "wholly illegitimate," so, under *United States v. Rubio*, mere membership to the group was not enough to constitute probable cause. Thus, the court suppressed the fruits of the Perez search.

*Id.* (citation omitted).

93. *Id.* at 1145.
94. *Id.* at 1136.
97. *Id.* at 469-71. Judge Chin pointed out that Yahoo! server logs disproved Agent Binney's belief that all Candyman members received the e-mails he did, yet Agent Binney testified several times that he based the statements made in his affidavit on his "'experience in the site.'" *Id.* at 469-70.
98. *Id.* at 480. The court concluded that "the agents had serious doubt as to the truth of the statements or, at a minimum, they had obvious reasons to doubt their veracity." *Id.* at 479.
99. See *id.* at 483 ("[T]he affidavit contains nothing concrete to suggest that Perez had transmitted or received images of child pornography.").
100. *Id.* at 471.
101. 727 F.2d 786 (9th Cir. 1984).
102. *Perez*, 247 F. Supp. 2d at 482. The court noted that "the site offered protected activities: polls and surveys; links to other sites; and a 'chat' section for real time conversations." *Id.* at 481.
103. *Id.* at 486.
3. Dissension Among the Ranks of the Second Circuit

Within weeks of each other, two separate panels of the Second Circuit presiding over e-group cases issued decisions with different probable cause findings. Martin and Coreas contained sharply different analyses and conclusions of fact and law, but Coreas ultimately affirmed the defendant’s conviction under circuit rules on stare decisis. Nevertheless, given the sheer number of e-group cases resulting from Agent Binney’s sting operation, the central debate within the Second Circuit is likely to spread to other circuits encountering the same issue and has already translated to paid subscription venues for child pornography.

a. Martin Finds Probable Cause Based on Mere Membership to an E-group

In Martin, the court affirmed the conviction of a member of “girls12-16,” another e-group discovered by Agent Binney. The court listed seven facts that supported a finding of probable cause: (1) the graphic welcome message implied that the site’s “essential purpose was to trade child pornography”; (2) the officer’s affidavit extensively detailed “the modus operandi of those who use computers for collecting and distributing child pornography”; (3) collectors of child pornography “tend to collect such material, store it, and rarely destroy or discard it”; (4) an “illicit purpose could be inferred from the website’s technological features”; (5) all members had access to child pornography and child erotica on the site; (6) “the affidavit established a nexus between the member and the website”; and (7) the defendant “joined [the e-group]

104. See United States v. Martin, 426 F.3d 68 (2d Cir. 2005); United States v. Coreas, 419 F.3d 151 (2d Cir. 2005).
105. Compare Martin, 426 F.3d at 74-76 (analyzing seven facts and concluding that the corrected affidavit still supported probable cause), with Coreas, 419 F.3d at 156-57 (“In a case argued a few weeks before this one and decided earlier this month, a divided panel of this Court appeared to reach different conclusions from those set forth above.”).
106. See Coreas, 419 F.3d at 159 (concluding that “since the Martin case was heard first, we are compelled, under established rules of this circuit, to affirm Coreas’ conviction”).
107. See supra note 20.
108. Martin, 426 F.3d at 70, 78.
109. Id. at 75; see also supra note 61.
110. Martin, 426 F.3d at 75.
111. Id.
112. Id. (specifying “files, messages, polls, e-mail, links, polls [sic], chat, and membership lists” as those features “that facilitated the trading of child pornography”).
113. Id.
114. Id. The nexus referred to by the court was that the defendant lived at the physical address associated with the e-mail address used to join the e-group. Id.
voluntarily and never cancelled his membership."\textsuperscript{115} Relying on the above facts as proof that the defendant "more than likely" downloaded images of child pornography, the Second Circuit affirmed Martin's conviction.\textsuperscript{116}

Judge Pooler issued a strident dissent.\textsuperscript{117} Pooler argued that focusing on "group probabilities runs counter to the well-settled notion that probable cause must be based on particularized facts."\textsuperscript{118} Moreover, she accused the majority of making "inferential leaps" that began with the corrected affidavit's lack of individualized suspicion towards the defendant, and ended with the allegation that the defendant was a collector of child pornography.\textsuperscript{119} Pooler concluded that without individualized evidence of illegal conduct in the affidavit, there was no probable cause to support the search warrant.\textsuperscript{120}

\textit{b. The Second Circuit Was Compelled to Follow Martin Precedent by Stare Decisis, but Otherwise Would Not Have Found Probable Cause in Coreas}

Several weeks after the Second Circuit decided Martin, it dealt with another Candyman defendant under a different panel of judges.\textsuperscript{121} The court expressed regret that the circuit's rules on stare decisis forced it to affirm the conviction.\textsuperscript{122} Unlike Martin, who was a member of the girls12-16 e-group, the defendant in Coreas was a member of the Candyman e-group.\textsuperscript{123} Judge Rakoff devoted a substantial portion of the panel's opinion to the probable cause determination, and concluded there was none.\textsuperscript{124} Coreas emphasized several key facts that Martin did

\begin{itemize}
\item \textsuperscript{115} \textit{Id.}
\item \textsuperscript{116} \textit{Id.} at 75, 78. \textit{Martin} reached this conclusion easily and agreed with \textit{Froman} that it was "‘common sense’ that one who ‘voluntarily joins’ a child-pornography group and ‘remains a member of the group . . . without cancelling his subscription . . . would download such pornography from the website and have it in his possession.’” \textit{Id.} at 75 (quoting United States v. \textit{Froman}, 355 F.3d 882, 890-91 (5th Cir. 2004)).
\item \textsuperscript{117} \textit{Martin}, 426 F.3d at 78-83 (Pooler, J., dissenting).
\item \textsuperscript{118} \textit{Id.} at 81-82.
\item \textsuperscript{119} \textit{See id.} at 79.
\item \textsuperscript{120} \textit{Id.} at 78.
\item \textsuperscript{121} United States v. \textit{Coreas}, 419 F.3d 151, 152 (2d Cir. 2005); \textit{see also} United States v. \textit{Coreas}, 426 F.3d 615, 617 (2d Cir. 2005) (per curiam) (denying Coreas' petition for rehearing and asserting that the panel "believe[d] that \textit{Martin I} was wrongly decided" but that it was forced "to affirm Coreas' conviction").
\item \textsuperscript{122} \textit{See Coreas}, 419 F.3d at 159 ("[S]ince the \textit{Martin} case was heard first, we are compelled, under established rules of this circuit, to affirm Coreas' conviction.").
\item \textsuperscript{123} \textit{Id.} at 152.
\item \textsuperscript{124} \textit{Id.} at 156-57. Judge Rakoff proclaimed that "[t]he notion that, by th[е] act of clicking a button, [the defendant] provided probable cause for the police to enter his
not. First, it stressed that the government presented no evidence that Coreas himself was a collector of child pornography.125 Thus, Rakoff deemed the background information126 in the Martin affidavit insufficient for establishing probable cause.127 Second, Coreas joined the e-group simply by clicking on a single button on his web browser: too trivial an act to justify the issuance of hundreds of other members’ search warrants.128 Third, despite its ability to subpoena server records from Yahoo!, the government failed to seek individualized evidence (for example, the e-mail addresses of those members who elected to receive automatic e-mails from the Candyman group) implicating Coreas or any of the other defendants before the government applied for the search warrant.129 Finally, Coreas found it material that e-groups contain protected First Amendment activity such as discussion boards, chat, and polls.130 Coreas ultimately affirmed the conviction under the circuit’s stare decisis rule, but the disparity of emphasis each panel placed on different facts and factors within virtually identical cases illustrates the need for guidance in this arena.131 Since Martin and Coreas are both binding precedent, and because the Second Circuit refused to rehear either case, it is likely that any future cases in the Second Circuit’s jurisdiction will hold that probable cause exists to search the home of a person identified in similar investigations.132 However, this issue will become increasingly important because of the sting operation’s national scope and the possibility that defendants in district and circuit courts in private dwelling and rummage through various of his personal effects seems utterly repellent to core purposes of the Fourth Amendment.” Id. at 156.

125. Id.
126. See supra text accompanying notes 110-11.
127. Coreas, 419 F.3d at 156.
128. Id. at 158. The Martin rule, which would find probable cause to search the home of a defendant who joins a child pornography focused e-group “out of curiosity or even from sheer inadvertence,” focuses on the “primary purpose” of the group, rather than the actions of the defendant to be searched. Id. This, Judge Rakoff feared, “might tend to dilute the First Amendment’s protection against guilt by association and diminish the Fourth Amendment’s focus on particularity and on protection of the privacy of the individual to be searched.” Id.
129. Id.
130. See id. at 156-57 (stating that what was absent from the “Martin majority’s analysis of the welcome messages of both websites [was lack of any genuine] recognition to their invitation to members to simply exchange views”).
131. See infra Part III.C.
132. United States v. Coreas, 426 F.3d 615, 617 (2d Cir. 2005) (per curiam) (denying Coreas’ petition for rehearing); see also United States v. Martin, 426 F.3d 83, 89 (2d Cir. 2005) (denying Martin’s petition for rehearing).
other jurisdictions may rely on, as persuasive authority, the favorable rationales and outcomes in cases like Strauser, Perez, and Kunen.\footnote{133}

II. CONTRASTING APPROACHES TO THE PROBABLE CAUSE DETERMINATION

A. Courts Finding Probable Cause Based on Mere Membership Ignore the Individualized Suspicion Requirement

The Martin court reached its finding of probable cause by considering three factors: (1) whether the “overriding, if not the sole, purpose of the . . . e-group [is] illicit”; (2) whether the e-mail address of the e-group member is “linked” to the defendant’s residence; and (3) whether “collectors of child pornography overwhelmingly use the internet . . . to distribute and hoard” child pornography.\footnote{134} The court concluded there was probable cause after finding the seven facts outlined above in Part I.B.3.a. of this Comment.\footnote{135}

However, the Martin majority claimed that the “girls12-16’s illicit purpose could be inferred from the website’s technological features (files, messages, polls, e-mail, links, polls [sic], chat, and membership lists) that facilitated the trading of child pornography.”\footnote{136} In reality, many e-groups, having a sinister purpose or otherwise, contain the same template-driven features with little variation.\footnote{137} Moreover, Judge


134. Martin, 426 F.3d at 74.
135. See supra Part I.B.3.a.
136. Martin, 426 F.3d at 75.
137. See id. at 71 n.3. (inferring that the girls12-16 and shangri_la e-groups contained substantially similar features as Candyman); see also, e.g., Yahoo! Groups Homepage, http://groups.yahoo.com (last visited Mar. 13, 2006). Yahoo!’s Groups Homepage contains a quadrant called “Features at a Glance,” which boasts the availability of message archives, photos, a calendar system to coordinate events, polls, and a links feature. Id. The author also verified the template design by creating a test group, and discovered that these features are enabled by default. See Law and the Candyman Sting Operation, http://groups.yahoo.com/group/lawandcandyman/ (last visited Mar. 13, 2006).}
Pooler’s dissent noted that textual features like chat rooms, message postings, or polls are not illicit because the statutory definition of child pornography only prohibits “visual depictions.” Also, while the girls12-16 welcome message was explicit, Agent Binney received 193 e-mail messages during the two weeks he was a member of the group. Of the 193 e-mails, only fourteen contained images of child pornography. Over half of the e-mails contained only text, which falls outside of the scope of the statutory definition of child pornography and into the realm of constitutionally protected speech. Thus, the conclusion that the “overriding purpose” of the site was illicit was unfounded.

Judge Pooler’s dissent in Martin called the majority's new precedent “dangerous.” She was particularly troubled that the court did not remand for a Franks hearing to decide whether Agent Binney made his false statement (that all members of the e-group received the illicit images) knowingly or recklessly. Instead, the majority concluded that Martin’s membership alone was sufficient to find probable cause even after redacting Agent Binney's false statements. In fact, it would not have been difficult for Agent Binney to subpoena Yahoo!’s server logs and it would have quickly demonstrated whether Martin actually downloaded child pornography.

---

138. Martin, 426 F.3d at 80 (Pooler, J., dissenting) (commenting that 18 U.S.C. § 2252(A) requires the illicit content to be a “visual depiction” and that features such as polls, chat, and posting messages, are all text-based); see also 18 U.S.C. § 2252(a)(1)-(3) (2000); 18 U.S.C.A. § 2256(8) (West Supp. 2005); supra text accompanying note 28.

139. See supra note 61.

140. Martin, 426 F.3d at 80 (Pooler, J., dissenting).

141. Id.

142. See id. at 80-81 (“Subscribers could have engaged in protected, non-criminal activities, such as answering survey questions or chatting.”) (quoting United States v. Perez, 247 F. Supp. 2d 459, 483 (S.D.N.Y. 2003)).

143. Id. at 80. The mixture of legal and illegal content, combined with the fact that eighty-three percent of the members opted out of receiving e-mails automatically, is consistent with Brown, which required an organization be found wholly illegitimate before suspicion may be based on mere membership to a group. See supra notes 55-57 and accompanying text.

144. Martin, 426 F.3d at 78 (Pooler, J., dissenting).

145. See id. (“Martin satisfies the second prong of Franks v. Delaware, because he has demonstrated by a preponderance of the evidence that Agent Binney’s ‘false statement [in the original affidavit] is necessary to the finding of probable cause.’” (alteration in original) (quoting Franks v. Delaware, 438 U.S. 154, 156 (1978))).

146. Id.

147. See Perez, 247 F. Supp. 2d at 485 (stating that it was possible for the government to obtain “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”); accord Martin, 426 F.3d at 89-90 (Pooler, J., dissenting) (objecting that “[r]quiring particularized evidence will not hamper government enforcement of laws
Agent Binney’s affidavit discussed how “collectors of child pornography” utilize computers and the Internet. However, the dissent pointed out the majority’s “erroneous inference.” If one concedes that non-collectors may be erroneously lumped in a group with collectors of child pornography, other statements in the affidavit become less plausible. For example, Agent Binney stated that “collectors tend to maintain their illicit collections and . . . rarely, if ever, destroy them.” This statement serves two ends. First, it establishes a broader pool of defendants than if individualized suspicion supported the affidavit. Second, it hopes to overcome a staleness of evidence challenge. While it is true that a collector of child pornography tends to hoard material, the same is not likely true of a casual surfer who stumbles upon such a site and is shocked by the material. If the likelihood that the member against child pornography. This is especially true in this case, since the government could easily have obtained information about a particular subscriber by obtaining the user’s email preferences from Yahoo! or monitoring use of the group.”; United States v. Coreas, 419 F.3d 151, 153 (2d Cir. 2005) (mentioning that “the Government had no knowledge of what [defendant] received—even though . . . this was information it could readily have obtained from Yahoo if it had sought to do so”).

148. Martin, 426 F.3d at 74. The affidavit contained discussion of the “characteristics of child-pornography collectors,” along with Agent Binney’s experience as an FBI agent. Id. at 72.

149. Id. at 82 (Pooler, J., dissenting). Judge Pooler further reasoned that [i]t is an inferential fallacy of ancient standing to conclude that, because members of group A (collectors of illegal visual depictions) are likely to be members of group B (subscribers to specified E-groups) then group B is entirely, or even largely composed of, members of group A. Such reasoning would lead us to conclude that if collectors of illegal visual depictions tend to be men, then men are likely to be collectors of illegal visual depictions. Id.

150. Id. at 72 (majority opinion).

151. See Silberman, supra note 1 (quoting Agent Binney as saying that “[i]t takes a lot of time to cultivate someone in a chat room”). Agent Binney also conceded that the FBI “wanted to work smarter” and that he investigated Candyman in order to “cast a wider net.” Id. One unnamed FBI agent stated that “[e]ven my friends can’t believe there’s a federal offense that’s so easy to commit. One click, you’re guilty.” Id.

152. See United States v. Ramsburg, 114 F. App’x 78, 82 (4th Cir. 2004) (“[F]indings of staleness become less appropriate when the instrumentalities of the alleged illegality tend to be retained.”).

153. See JENKINS, supra note 5, at 99 (profiling collectors of child pornography as “pack rats” with “large collections of images often intricately organized and cataloged”).

154. See United States v. Lacy, 119 F.3d 742, 745-46 (9th Cir. 1997) (stating that a court evaluates staleness “in light of the particular facts of the case” and that evidence is not stale if the court finds sufficient grounds to believe “based on a continuing pattern or other good reasons, that the items to be seized are still on the premises”). Since law enforcement officials did not arrest the vast majority of those searched, it raises the question how many were actual collectors, and how many were casual surfers? See Jon
is a collector decreases, so too does the level of suspicion that there is evidence of child pornography on a casual surfer's computer months or even a year later.\textsuperscript{153}

B. A Finding of Probable Cause That Is Based on Group Probabilities Is Overly Broad and Will Support Searches in Innocuous Situations

1. Hypothetical Scenarios Demonstrate a Pervasive Threat to Law Abiding Citizens

Notwithstanding the Supreme Court precedent in \textit{Ybarra} vitiating probable cause based on a person's "mere propinquity," an individualized suspicion requirement is vital to sound public policy because it reduces the "mischief" law enforcement might use to justify searches for large numbers of people.\textsuperscript{156} To demonstrate the dangers

Carroll, \textit{Operation Candyman Gets Sticky}, S.F. CHRON., Mar. 11, 2003, at D8 (reporting that "most of the people in the 700 homes searched were not even consumers of child pornography").


156. \textit{See} United States v. Kunen, 323 F. Supp. 2d 390, 401 (E.D.N.Y. 2004); \textit{cf} JENKINS, \textit{supra} note 5, at 159-61. A strong individualized suspicion requirement protects against overly broad searches or the use of methods like "trap sites," which could be created by law enforcement entities that contain copious amounts of child pornography to attract child pornographers. \textit{See id}. Once the visitors are attracted to the site, knowingly downloading even one image would be sufficient to violate federal child pornography laws. \textit{See} \textit{18 U.S.C. § 2252(a)(2)} (2000) (prohibiting the transfer of "any visual depiction"); JENKINS, \textit{supra} note 5, at 159. Given the simple and fleeting nature of an e-group, it is not difficult to imagine scenarios in which sites with legal pornographic content slowly morph into sites featuring illegal child pornography. \textit{See infra} notes 204-05 and accompanying text. Under Martin's test for probable cause, consider a scenario where a law enforcement officer creates an e-group with an innocuous welcome message that initially contains legal adult pornography attracting many members. \textit{See supra} note 154 (mentioning the shangri_la group and many other sites containing child pornography offer no hint of the contents within). As time progresses, the officer may gradually upload more illegal child pornography, increasing the ratio of child pornography on the site until the overriding purpose of the site becomes the distribution of child pornography. Under Martin, the government would have probable cause to search the homes and personal effects of every member—even those who only visited once when the content was legal, and, shocked by the content, closed their web browsers without unsubscribing to the e-group. \textit{See United States v. Strauser}, 247 F. Supp. 2d 1135, 1145 (E.D. Mo. 2003). While one may argue that entrapment is an affirmative defense to such actions, the existence of probable cause is a collateral issue to the entrapment defense. \textit{See} Bruce Hay, \textit{Sting Operations, Undercover Agents, and Entrapment}, 70 MO. L. REV. 387, 399 n.28 (2005) (noting that some have advocated that sting operations require probable cause, but that this has been rejected by most jurisdictions); Maura F.J. Whelan, \textit{Comment, Lead Us Not into (Unwarranted) Temptation: A Proposal To Replace the Entrapment Defense with a Reasonable-Suspicion Requirement}, 133 U. PA. L. REV. 1193, 1195 & n.14 (1985). Thus, by
involved with upholding a group probabilities (mere propinquity) precedent, Judge Hurley in *United States v. Kunen* presents an insightful hypothetical fact pattern that combines the recidivist nature of a pedophile with the broad powers of a group probabilities regime. The hypothetical illustrates the potential breadth of government searches by assuming a fictional scientific study has concluded that "a majority' of incarcerated pedophiles will return to their criminal ways within the first year following their release from prison." Thus, instead of members of a web site containing child pornography, the group in question becomes "pedophiles out of jail for over a year." Next, assume that "such individuals invariably take one or more items of personal property from their victims and stash those items in their, the pedophiles’ residences." Judge Hurley reasons that if group probability is the sole factor for determining probable cause, any random member is more likely than not to return to criminal conduct. Thus, without law enforcement having any individualized suspicion, any random member of the group remains subject to a future search even after release from prison. Judge Hurley stated that "[e]ven if, arguendo, a ‘majority’ of Candyman members are more likely than not to have child pornography on their computers at any given time, that does not, standing alone, cause the entire membership to be fair game for search warrants."

2. Casual Surfers Will Become Suspected Child Pornographers Based on the Actions of Others

Because only members may view an e-group's content, a probable cause determination based on group probabilities could subject a casual surfer to an intrusive governmental search. The chain of events might

the time the defendant raises an entrapment defense, the defendant will have already suffered damage to his reputation, character, and self-esteem as a result of the search. See infra note 165.

158. Id. at 401.
159. Id.
160. Id.
161. Id.
162. Id.
163. Id.; see also United States v. Strauser, 247 F. Supp. 2d 1135, 1144 (E.D. Mo. 2003) (providing another example of mischief that may result in the context of membership to a subscription magazine advocating legalization of drugs). Judge Perry stated that upholding a search based on group probabilities "is the equivalent of saying if someone subscribes to a drug legalization organization or newsletter, then there is probable cause to believe that person possesses drugs." Id.
164. Kunen, 323 F. Supp. 2d at 400.
165. See Strauser, 247 F. Supp. 2d at 1145 ("[A] person could have clicked on the subscribe button, still not knowing what was on the site, specified the ‘no mail’ option, and
occur like this: First, the potential member stumbles upon an e-group while surfing—perhaps by browsing the e-group's topical directory for a wholly unrelated topic, searching for a group in an innocuous area of interest, or clicking a link in an e-mail.\(^6\) Second, he may not read the welcome message, or he may find it interesting, but not illegal, since no visual depictions have been presented or even suggested yet.\(^7\) He clicks the "join" button and selects the option to receive "no e-mails."\(^8\) Next, the member enters the e-group, accesses the message board and instantly downloads several illicit images. The content shocks him, and he immediately closes his browser and deletes the images from his browser cache.\(^9\) The member never returns to the site and never unsubscribes.\(^10\) Courts finding probable cause based on mere membership risk subjecting this person to a search of his home and personal effects.\(^11\) Such a scenario highlights the pervasive reach of the Second Circuit's new

---

\(^6\) Cf. United States v. Martin, 426 F.3d 68, 71 (2d Cir. 2005) (mentioning that "the shangri-la e-group welcome message simply announced, 'Hardcore Only'"). To avoid detection by law enforcement, many groups and sites containing child pornography maintain innocuous-sounding names known only to those within the subculture, such as "Maestro," "hel-lo," "ll-series," "Tiny Americans," and "KX." JENKINS, supra note 5, at 61-65. However, using innocuous names to trick surfers into visiting pornographic sites also occurs with sites that do not contain child pornography. See Declan McCullagh, *Use Misleading Domain Name, Go to Jail?*, CNET NEWS.COM, Mar. 26, 2003, http://news.com.com/2100-1028_3-994201.html?tag=st.util.print (reporting that the web domain "whitehouse.com" was a web site devoted to pornography, and not one associated with the residence of the President of the United States). In 2003, the site was the target of a proposal in the House of Representatives to criminalize misleading domain names that deceived persons into viewing obscene material or sites harmful to minors. See *Truth in Domain Names Act*, Pub. L. No. 108-21, 117 Stat. 686 (2003) (codified at 18 U.S.C.A. § 2252B (West Supp. 2005)); McCullagh, supra.

\(^7\) See supra note 165.

\(^8\) See supra note 11 and accompanying text.

\(^9\) In Internet Explorer and other web browsers, the cache, or temporary internet files, consists of files automatically downloaded from each visited site that are stored on a computer's hard drive to speed up browsing. Microsoft.com, How To Delete the Contents of the Temporary Internet Files Folder, http://support.microsoft.com/default.aspx?scid=kb;en-us;260897 (last visited Mar. 13, 2006).

\(^10\) See Strauser, 247 F. Supp. 2d at 1145. Judge Perry described a similar sequence of events in her opinion, hypothetically stating that "[a] person could . . . have seen the child pornography on the site, been shocked, and immediately left the site, never to return, not even to search for and find the method of 'unsubscribing.'" *Id.*

\(^11\) See United States v. Coreas, 419 F.3d 151, 158 (2d Cir. 2005) (holding that the *Martin* rule would find probable cause to search the home of a defendant who joins an e-group whose primary purpose is to distribute child pornography "out of curiosity or even from sheer inadvertence").
Pornography and the Fourth Amendment

precedent; thus Judges Rakoff and Pooler have proclaimed Martin to be wrongly decided,\(^7\) and dangerous precedent.\(^7\)

### III. COURTS THAT FIND PROBABLE CAUSE TO SEARCH A HOME OR COMPUTER IN “MERE MEMBERSHIP” CASES SET A DANGEROUS PRECEDENT REQUIRING FURTHER GUIDANCE

#### A. Technology, the Government, and the Fourth Amendment—A Volatile Combination

Law enforcement agencies, politicians, judges, and juries are not experts in the complex technologies used by child pornographers.\(^1\) Lawmakers have demonstrated a fundamental misunderstanding of how the Internet works and the methods of child pornography distribution.\(^1\)

\(^1\) See id. at 159; United States v. Martin, 426 F.3d 68, 78 (2d Cir. 2005) (Pooler, J., dissenting).

\(^7\) See Martin, 426 F.3d at 78 (Pooler, J., dissenting).

\(^1\) See JENKINS, supra note 5, at 215 (“[L]aw enforcement agencies and their political masters have . . . a very poor idea of the organization and mechanisms of the child porn subculture, and above all, of its critical institutions such as the newsgroups and bulletin boards.”); Donald E. Shelton, Teaching Technology to Judges, JUDGES’ J., Winter 2001, at 42, 42 (writing that “many judges are not computer literate” and adding that some “even pride themselves on their lack of technological skills and wear it like a badge of honor”); Silberman, supra note 1 (commenting that one judge presiding over a Candyman case asked in the middle of the hearing, “[w]hat are GIF files?”). Shelton is a presiding judge in a Washtenaw County trial court in Ann Arbor, Michigan. Id.

\(^1\) See JENKINS, supra note 5, at 16. Jenkins comments that the testimony at a 1997 Senate hearing on the Proliferation of Child Pornography on the Internet was “at best rudimentary, at worst simply inaccurate,” id. at 16, when Senator Judd Gregg presented information asserting that “[c]urrently, the avenue for distribution of sexually exploitative material is through chat rooms,” Proliferation of Child Pornography on the Internet: Hearing Before the Subcomm. on Commerce, Justice, and State, the Judiciary, and Related Agencies of the S. Comm. on Appropriations, 105th Cong. 2 (1997) (statement of Sen. Judd Gregg) (quoting JUDD GREGG, CHILD PORNOGRAPHY AND THE INTERNET: WHAT EVERY PARENT, TEACHER, AND CHILD SHOULD KNOW). Senator Gregg continued, “In these chat rooms, the offenders speak freely about their desire to trade pictures.” Id. at 3 (quoting JUDD GREGG, CHILD PORNOGRAPHY AND THE INTERNET: WHAT EVERY PARENT, TEACHER, AND CHILD SHOULD KNOW). In actuality, exchange of child pornography via chat rooms is rare. See JENKINS, supra note 5, at 16. Instead, child pornographers generally confine the exchange to Internet Usenet newsgroups, communities such as Yahoo! Groups or MSN Groups, web-based bulletin boards, and closed groups. Id. at 59. If public web sites ever contain child pornography, their operators give them innocuous names, and visitors flood them very quickly, forcing them to shut down and move to another host. Id. at 69. Jenkins explains that child pornographers sometimes use keywords such as “soccer” and “volleyball,” terms that a server administrator is unlikely to ban. Id. Thus, as Senator Gregg’s testimony reflects, law enforcement and politicians have historically “had a very poor idea of the organization and mechanisms of the child porn subculture, and . . . its critical institutions such as newsgroups and bulletin boards.” Id. at 215; see also Silberman, supra note 1 (recounting the testimony of Agent Kristen Sheldon, Agent Binney’s successor in the investigation,
Furthermore, in an ever-evolving technological world, government bureaucracy and legislatures tend to be reactive to, and thus, two steps behind, net-savvy child pornographers.\(^{176}\) For example, child pornographers routinely use protective measures such as anonymous proxy servers to eliminate “digital fingerprints” in cyberspace.\(^ {177}\) The use of such tools are instinctive to all but the novice child pornographer, yet have perplexed government personnel such as former FBI director Louis Freeh.\(^{178}\) Increasing reliance on technology to “get tough on all pedophiles” could simultaneously amplify this flaw and encourage the

\begin{quote}
during one Candyman case as she imprecisely described the mechanics of an IP address). Sheldon testified that an IP address is “in very simple terms, a Social Security number. Only one person at one specific time can have that number.” Id. To illustrate Sheldon’s error, Silberman clarified that “an IP address identifies a computer, rather than a person, and may not even consistently map to a particular machine in networks that use dynamic IP addressing.” Id.
\end{quote}


Governments are still reacting to, and legislating about, technology that has largely come and gone. While the mention of Napster will still evoke strong responses from many in the public policy sphere, it has long since been replaced by new models of file sharing technology such as Grouper, Kazaa, and BitTorrent. By the time legislation can address a specific issue or problem it has often already been solved by the market or replaced by a newer version. It would be the same exercise in futility if governments were to pass laws regulating the use of blank audio cassettes or Betamax machines.

\begin{quote}
Id. (footnotes omitted); see also JENKINS, supra note 5, at 48 (averring that many “veteran” child pornographers have been exchanging material since the dawn of the first personal computer). It is common for habitual offenders to casually reminisce about technical details like “PDP-11 mainframes” and “300 baud modem[s],” which may baffle a judge or a police officer who has only attended a short training course on the Internet. Id.
\end{quote}

177. See JENKINS, supra note 5, at 12 (“[T]he technical issues involved [with Internet child pornography] can . . . seem forbidding to a non-specialist.”). Jenkins specifically mentions “proxies” and “anonymizers.” Id.; see also Thomas J. Fitzgerald, A Trail of Cookies? Cover Your Tracks, N.Y. TIMES, Mar. 27, 2003, at G6 (discussing methods that the general public may use to conceal their identities online, including a subscription proxy service called “anonymizer.com”).

178. See JENKINS, supra note 5, at 160-61 (noting that former FBI director Louis Freeh testified to a Senate panel on computer hacking of government web sites that “perpetrators . . . [falsify their Internet addresses], ‘meaning that the address that appeared on the target’s log was not the true address of the system that sent the messages’”). The “bemused legislators” needed the practice explained to them, whereas such a precaution is instinctive to veteran computer users. Id. More recently and related to Internet child pornography, FBI agents within the Cyber Division testified in Perez that “they did not understand the material” that Yahoo! provided in response to Agent Binney’s subpoena. United States v. Perez, 247 F. Supp. 2d 459, 485 (S.D.N.Y 2003).
overzealousness of law enforcement that Judge Rakas in Coreas, and the Framers, feared. 179

B. A Mere Membership Precedent Thwarts Researchers and Watchdog Organizations

The incriminating nature of merely possessing child pornography already poses a difficult obstacle for researchers who study the techniques used to obtain child pornography and the nature of those bold enough to commit the crime. 180 Finding probable cause based on mere membership to a web site or e-group that contains child pornography will

179. See United States v. Coreas, 419 F.3d 151, 151 (2d Cir. 2005) (noting the danger of overzealousness); JENKINS, supra note 5, at 218-21 (arguing that the solution to the pervasiveness of child pornography is not "get tough" campaigns and stricter punishments, which have already been tried over the decades, but increasing public awareness of the crime); Spence, supra note 176, at 411-14 (stating that Internet legislative efforts are littered with "spectacular failures" and that "[t]he problems inherent in regulating technology are only exacerbated when combined with sexually explicit content, another source of constant difficulty and struggle"). Jenkins also notes that impressive child porn ring sting operations, some with international cooperation, have occurred without the use of widespread technology. See JENKINS, supra note 5, at 214.

180. See JENKINS, supra note 5, at 17-22. Jenkins devotes an entire section of his book to his unique research methodologies which involved disabling images within his web browser and relying on textual Internet newsgroup postings where other viewers discussed the contents of the images (which Jenkins had blocked). Id. Jenkins resorted to this mode of research, which fell "far short of the kind of direct observation that would normally be demanded in reporting such a study" so that he would not violate child pornography laws. Id. at 22. Jenkins stated simply, "[i]n the context of computers, one violates the law not only by storing such an image on a hard disk but merely by downloading it." Id. at 18; see also Emily D. Goldberg, Note, How the Overtturn of the Child Pornography Prevention Act Under Ashcroft v. Free Speech Coalition Contributes to the Protection of Children, 10 CARDOZO WOMEN'S L.J. 175, 187 (2003) ("Some scholars have called for a... research privilege to allow for the study... of child pornography."). Goldberg argues that the lack of a research privilege forces society to get information on child pornography from either law enforcement (the government) or law breakers (pedophiles themselves). Id. Thus, the result is a "vacuum of neutral information." Id. Finally, in 2000, the Fourth Circuit affirmed the conviction of journalist Lawrence Charles Matthews of six counts of transmitting child pornography and nine counts of receiving child pornography. United States v. Matthews, 209 F.3d 338, 339-40 (4th Cir. 2000). Matthews, "a journalist with thirty-one years of experience and the winner of the George Foster Peabody Broadcasting award," was researching for an article he was writing "on the Internet and law enforcement efforts to police it." Amy Tridgell, Note, Newsgathering and Child Pornography Research: The Case of Lawrence Charles Matthews, 33 COLUM. J.L. & SOC. PROBS. 343, 343 (2000). Matthews entered Internet chat rooms that child pornography traders frequented. Id. Upon identifying himself as a journalist, the users of the chat room all exited the room. Id. Next, in an effort to earn the trust of the child pornographers, he pretended to be one and actually received and transmitted images of child pornography. Id. at 343-44. Consequently, FBI agents raided his house, and he was arrested, tried, and convicted. Id. at 344-45.
have a deterrent effect on researchers and watchdog organizations with legitimate concerns for the well-being of children in mind.  

To help combat child pornography, the FBI has obtained the cooperation of other government organizations like the U.S. Postal Service and the U.S. Customs Service. Moreover, because of the overwhelming presence of Internet child pornography and "the general failure of law enforcement to deal with [child pornography]" on its own, private companies and grassroots groups have formed with the goal of removing child pornography from the web. These private organizations have proven to be far more effective than government entities at doing so. Since child pornography today circulates through e-groups and newsgroups, it follows that one would need to be a subscriber or actively download the content of such media in order to detect violations and report them. If courts continue to find probable cause to search based on mere membership alone, this could have dire public policy implications by punishing, and thus deterring, the civilian assistance that has proven to be so crucial in the effort against child pornography. Organizations that assist the FBI by seeking out child

181. See JENKINS, supra note 5, at 10 (asserting that few "academic or journalistic American accounts . . . ha[ve] appeared since [the early 1980s] because . . . the ferocious legal prohibitions on viewing child porn images have had the effect of virtually banning research").


183. JENKINS, supra note 5, at 165.

184. Id.; see also The WatchDog, http://groups.yahoo.com/group/The_WatchDog (last visited Mar. 14, 2006) (stating as its mission "to seek out [and report] all Yahoo groups and member profiles, internet websites, and all violators of internet obscenity laws, including child sexual exploitation").

185. JENKINS, supra note 5, at 165 ("Activism by private enterprise [results in] . . . finally . . . anti-porn activists who genuinely scare the subculture."). Jenkins hypothesizes that the "ongoing threat posed by technologically sophisticated activists is far more effective than the sporadic danger posed by traditionally conceived police purges." Id. at 166. In addition to being an effective supplement to government enforcement, Jenkins also states that private activism can deter the spread of child pornography on its own. Id.

186. See supra note 9. The Yahoo! Groups site is free and open to anyone who clicks the "Join" button, but without joining, the user only sees a welcome screen and can only view a skeletal template menu of the group without any functional hyperlinks that delve further into the group's image content. See Yahoo! Help—Groups, http://help.yahoo.com/help/us/groups/groups-20.html (last visited Mar. 14, 2006) (explaining that a nonmember may only view messages if "a group has a public archive"). Unless the moderator changes the default setup, a nonmember cannot view image content. See, e.g., Law and the Candyman Sting Operation, supra note 137 (showing the chat, files, photos, polls, links, and member list sections as not viewable until one joins).

187. See supra notes 180, 185 and accompanying text. Removing researchers from the equation isolates society from objective, academic information from scholars and
pornography and reporting it to authorities could suddenly become suspect entities.\textsuperscript{188} Law enforcement agencies issued hundreds of intrusive search warrants for Candyman’s members.\textsuperscript{189} While certainly some of those members will have committed crimes that § 2252 seeks to preclude, other members could be concerned parents, legitimate academic or legal researchers, or members of watchdog organizations.\textsuperscript{190} Regardless of the outcome, a single FBI search is an invasion of privacy that frequently stirs local news headlines, and results in a permanently stained reputation.\textsuperscript{191} Courts should be reluctant to implement such a broad policy.\textsuperscript{192}

C. A New Test for Probable Cause That Requires Individualized Suspicion Is Needed in Internet Child Pornography Cases

The reasons described above suggest that courts need a new test for determining probable cause in the realm of Internet child pornography.\textsuperscript{193} First, courts have examined a host of factors when making a probable cause determination related to the search of the home of a member of an e-group containing child pornography.\textsuperscript{194} Second, a test that requires some evidence of the web site’s illicit functionality in concert with the defendant’s own illicit actions would be helpful.\textsuperscript{195} The author is

---

\textsuperscript{188} Cf. JENKINS, supra note 5, at 19 (“I share the general reluctance [with other researchers] to risk legal consequences.”). Similar to the suspicion that has befallen researchers, watchdog organizations may meet a similar fate.

\textsuperscript{189} See supra note 8.

\textsuperscript{190} See supra note 165; see also Sherry F. Colb, The Qualitative Dimension of Fourth Amendment “Reasonableness,” 98 COLUM. L. REV. 1642, 1720 (1998) (asserting that a home search authorized without individualized suspicion is disproportionately intrusive).

\textsuperscript{191} See Martin, 426 F.3d at 83 (Pooler, J., dissenting) (expressing dismay that the government would find, when a concerned parent or researcher joins such a site, “sufficient information to obtain a search warrant to enter his home”).

\textsuperscript{192} See Martin, 426 F.3d at 83 (Pooler, J., dissenting) (expressing dismay that the government would find, when a concerned parent or researcher joins such a site, “sufficient information to obtain a search warrant to enter his home”).

\textsuperscript{193} See supra Part I.B.3.

\textsuperscript{194} See, e.g., supra text accompanying note 134 (listing the three Martin factors: illicit purpose (as indicated by the site’s welcome message and “technological features”); the defendant’s e-mail address linked to the web site; and the proclivities of collectors); see also United States v. Kunen, 323 F. Supp. 2d 390, 392 (E.D.N.Y. 2004) (failing to find probable cause where the “vast majority” of the group opted out of receiving the automatic e-mails that contained child pornography); United States v. Perez, 247 F. Supp. 2d 459, 483 (S.D.N.Y. 2003) (looking for any particularized evidence that defendant actually possessed the illicit material).

\textsuperscript{195} See supra note 128 (discussing Judge Rakoff’s fear of relying strictly on the "purpose" of the site for the probable cause determination). The prevalence of unsecure wireless networks that can penetrate neighboring walls could also raise doubt as to the identity of a single computer user, and underscores the need for individualized suspicion
The goal is to construct a two-pronged test that considers the totality of circumstances relating to (1) the web site, and (2) the defendant. The test aims to ensure that enough individualized suspicion exists to substantiate a finding of probable cause to search the home of such a suspect. Within the confines of this framework, courts would have discretion to determine what facts are more relevant than others on a case-by-case basis. In accordance with Franks, if the agent made false statements in the application for a search warrant, the court’s analysis would occur after the court redacted any knowingly or recklessly made statements from the affidavit.

1. The Overriding Purpose of the Site

To find probable cause to search the house of a member of a site that contains child pornography, the first inquiry must be whether the overriding purpose of the site is to produce or distribute visual depictions of child pornography. Because probable cause is based on the totality of the circumstances and requires a “fair probability,” judging a site solely by its welcome message or a few circulated e-mail postings by

---


197. This test combines the factors that Martin, Coreas, and various district court cases have emphasized. See supra Parts I.B.2.b.ii, I.B.3.

198. See Chandler v. Miller, 520 U.S. 305, 308 (1997) (explaining that the Fourth Amendment allows searches not grounded on individualized suspicion only in “certain limited circumstances” such as fixed border patrol checkpoints, sobriety checkpoints, and administrative inspections).

199. See, e.g., United States v. Ramsburg, 114 F. App’x 78, 79-80 (4th Cir. 2004) (per curiam). The court factored into its probable cause determination that an individual with the same online moniker as defendant, “OriolesGuy,” had e-mailed an illicit image to an officer during an undercover sting operation several years before. Id. This fact combined with the defendant’s membership to Candyman and his use of the same moniker strengthened Ramsburg’s probable cause finding. Id. at 81-82.


201. Cf. United States v. Martin, 426 F.3d 68, 74 (2d Cir. 2005) (stressing that the overriding purpose of the site was illicit).
individual members does not meet this standard. Rather, a determination of the "overriding purpose" of the site must consider both the form and functionality of the site, and the individual member's participation or activity on the site.

The ratio of total materials posted to the site versus materials posted that contain child pornography objectively measures the overriding purpose of the site. However, visual depictions of child erotica, textual message postings, polls, and chat rooms cannot tilt the scales in favor of finding probable cause because such materials are not illicit. While opponents of this view may argue that "innocent behavior frequently will provide the basis for a showing of probable cause," the necessary degree of suspicion, for example, when a person casually stumbles upon a site, is simply not present. Because one may come into possession of child pornography and child erotica accidentally, and because of the statutory requirement that one "knowingly" possess the illicit material, judges should construe materials falling outside the scope of the statutory definition of "child pornography" as collateral to those factors that contribute to a finding of probable cause. Furthermore, increased prevalence of legal materials on a site dilute a finding that the overriding purpose of the site is to distribute visual depictions of child pornography. The welcome message or any other singular attribute about the site must not be determinative for these reasons.

202. Cf. id. at 86 (noting that the welcome message was "an integral component of [the court's] probable cause determination").

203. This is a combination of the Martin dissent and Chandler holdings. See Chandler, 520 U.S. at 308; Martin, 426 F.3d at 80 (Pooler, J., dissenting) (discussing the scope of 18 U.S.C. § 2252A and functions of an e-group that do not fall within the ambit of "visual depictions"); supra note 49 and accompanying text.

204. Cf. Martin, 426 F.3d at 80-81 (Pooler, J., dissenting).

205. Id. Notwithstanding the legal nature of child erotica, the Second Circuit has also taken the evidentiary stance that possession of child erotica generally is irrelevant to the crime of trading child pornography. Id. at 81 ("Not only is it legal to trade textual depictions and child erotica under the relevant statute, but this Court has also indicated that, as a general matter, possession of child erotica is not relevant to the crime of trading illegal visual depictions."); see also United States v. Harvey, 991 F.2d 981, 994-95 (2d Cir. 1993).


207. See supra note 166 (noting that group names often intentionally sound innocuous to evade law enforcement). Thus, a finding of probable cause based on the group name alone is inaccurate, at best.

208. 18 U.S.C. § 2252A(a)(5)(B) (2000) (requiring the mental state of "knowingly" possessing child pornography); see also supra text accompanying note 29.

209. See Martin, 426 F.3d at 81 (Pooler, J., dissenting).

210. See id. ("In light of the fact that less than 8 percent of e-mails contained illegal visual depictions, it is purely speculative for the majority to infer that the overriding purpose of the E-group was to trade illegal visual depictions.").
2. The Nexus Between the Defendant and the Site

The second prong of the test examines the connection between the defendant and the site. First, courts must require some individualized suspicion that the defendant knowingly possessed (i.e., downloaded) the visual depictions of child pornography. Group probabilities such as the illegal nature of the group, in and of themselves, are not sufficient to find probable cause under Chandler, Ybarra, Brown, and Rubio. Law enforcement agencies may obtain individualized evidence by examining ISP logs before applying for the search warrant. The fact that law enforcement agencies did not execute search warrants for many of the Candyman and girls12-16 defendants until a year after the sites were closed down shows there is ample time to conduct the necessary investigatory work to comply with the individualized suspicion required by Ybarra and the Fourth Amendment.

The affidavit must demonstrate a "fair probability" that the defendant himself attempted to access the visual depictions by substantially navigating through the site, or downloading or saving images from the site. While seemingly a good indicator of criminal activity, length of membership in an e-group is not revealing since some defendants may be

211. Id. at 75 (majority opinion). A nexus between the defendant and the site is the sixth fact in the Martin test for probable cause. Id.

212. See 18 U.S.C. § 2252A. Since Brinegar does not require evidence that would condemn a person, but evidence that must amount to more than merely a bare suspicion, ISP server records showing "recent and repeated[ ]" attempts to access child pornography would certainly satisfy this standard. See Brinegar v. United States, 338 U.S. 160, 177-78 (1949). Since the number of child pornographic items required to commit a crime is so low, evidence of a single, isolated page hit containing three images of child pornography might even satisfy this standard. See 18. U.S.C. § 2252A(d) (allowing an affirmative defense only if the defendant has downloaded fewer than three images, and either promptly destroyed the images, or notified and provided law enforcement access to each image). This could have significant public policy implications vis-à-vis legitimate researchers and watchdog organizations. See supra note 180.

213. See supra Parts I.B.2.a, I.B.2.b.ii.

214. United States v. Perez, 247 F. Supp. 2d 459, 485 (S.D.N.Y. 2003) (stating that it was possible for the government to obtain "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"); see also United States v. Coreas, 419 F.3d 151, 153 (2d Cir. 2005) ("[T]he Government had no knowledge of what [defendant] had received—even though . . . this was information it could readily have obtained from Yahoo if it had sought to do so.").


casual surfers who, shocked by the content they stumbled upon, abandoned the site without unsubscribing.\textsuperscript{217} Furthermore, web site content changes rapidly over time. The overriding nature of interactive sites may fluctuate greatly: from purely child erotica (legal) to child pornography (illegal), subjecting those who were members when the content was legal to searches for illegal content that they never downloaded or even had the capability of downloading when they originally accessed the site.\textsuperscript{218}

In sum, to satisfy the second prong of the test, the evidence supporting probable cause to search the defendant’s home and personal effects must be sufficiently grounded on the defendant’s individual actions, rather than his “mere propinquity to others independently suspected of criminal activity.”\textsuperscript{219}

IV. CONCLUSION

Several circuit courts of appeals and district courts have struggled to analyze cases presenting the novel issue of whether mere membership to an e-group found to contain child pornography is sufficient to find probable cause to search the member’s home. The Supreme Court has already held that one’s “mere propinquity” to a group suspected of criminal activity does not rise to the level of probable cause. Nevertheless, courts that have upheld search warrants—even in the face of recklessly made false statements—have virtually sidestepped this precedent. While few would find righteousness in a child pornographer’s trade, his Fourth Amendment right to be free from unreasonable searches and seizures unsupported by probable cause is a right that must be preserved. If courts continue the trend of upholding probable cause findings in these instances, the casual Internet user may easily be the next victim of an intrusive government search. Because of the grotesque nature of child pornography, it may be difficult to rally behind a cause that gives a child pornographer rights. Indeed, this is what gives the prosecution momentum and why so few child pornography cases go to trial. But in a world where Fourth Amendment search protections are slowly eroding,\textsuperscript{220} and the threat of general warrants has not completely

\textsuperscript{217} See Strauser, 247 F. Supp. 2d at 1145.

\textsuperscript{218} See supra note 205 (explaining the different evidentiary treatment that child erotica and child pornography receive).


\textsuperscript{220} Akhil Reed Amar, Fourth Amendment First Principles, 107 HARV. L. REV. 757, 759 (1994) (referring to the Fourth Amendment as “a sinking ocean liner—rudderless and badly off course” while noting that “most scholarship contents itself with rearranging the deck chairs”).
receded, perhaps there is no more appropriate time to change the course of the law.