FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant,* v. KENNETH KELLEY, *Defendant-Appellee.*	No. 05-10547 D.C. No. CR-05-00125-PJH ORDER AMENDING OPINION AND GRANTING APPELLANT'S MOTION FOR CLARIFICATION AND AMENDED OPINION

Appeal from the United States District Court
for the Northern District of California
Phyllis J. Hamilton, District Judge, Presiding

Argued and Submitted
October 20, 2006—San Francisco, California

Filed March 1, 2007
Amended April 9, 2007

Before: Sandra Day O'Connor, Associate Justice (Ret.),*
Pamela Ann Rymer, and Sidney R. Thomas, Circuit Judges.

Opinion by Judge Rymer

*The Honorable Sandra Day O'Connor, Associate Justice of the United States Supreme Court (Ret.), sitting by designation pursuant to 28 U.S.C. § 294(a).

COUNSEL

Amber S. Rosen, Assistant United States Attorney, San Jose, California, for the plaintiff-appellant.

Elizabeth M. Falk, Assistant Federal Public Defender, San Francisco, California, for the defendant-appellee.

ORDER

The opinion in this case, which appears at slip op. 2285[1] (9th Cir. March 1, 2007), is hereby amended as follows: the first paragraph of section III beginning at slip op. 2293 is hereby amended to read: "Kelley argues, and the government does not seriously dispute, that unwitting receipt of e-mail containing contraband will not support probable cause. *See* 18 U.S.C. § 2252A(a)(2) (criminalizing the knowing receipt of child pornography); *United States v. Romm*, 455 F.3d 990, 998 (9th Cir. 2006) (holding that a person receives child pornography if he seeks it out). The disagreement centers on whether the affidavit is sufficient even though it lacks direct evidence that Kelley actually solicited the offending attachments."

[1]478 F.3d 1068 (9th Cir. 2007).

Accordingly, the petition for clarification is GRANTED.

OPINION

RYMER, Circuit Judge:

Kenneth Kelley's home computer was searched for images of child pornography pursuant to a warrant based on information discovered during two unrelated computer searches for child pornography, demonstrating that Kelley had received nine e-mails with attachments depicting young boys in sexually explicit positions. He moved to suppress evidence obtained in the search after he was indicted for possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), and for receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2). Granting the motion, the district court found that probable cause was not established by proof of receipt of e-mails absent direct evidence about those who had sent them, Kelley's connection with the persons who owned the other computers on which e-mails to his screen name appeared, or Kelley's having reached out in some way for the pornography attached to the transmissions. The government appeals, arguing that the district court improperly applied a bright-line rule for what is required to establish probable cause in a case involving possession of child pornography, whereas the totality of the circumstances, which it submits is the proper test, allows the reasonable inference that Kelley wanted to receive the offending e-mails.

Since the district court's decision in this case, this court has made clear that probable cause to search a computer for evidence of child pornography turns on the totality of the circumstances, including reasonable inferences. *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc). In this case, there is a reasonable inference from facts set out in the affidavit that Kelley was not an accidental recipient of e-

mails with attachments containing illicit child pornography. As we conclude that it was fairly probable that child pornography Kelley willingly received would be found on his computer, we reverse.

I

Kelley's account on America On Line (AOL) was searched in December, 2004, and his home computer was searched in February, 2005. This appeal concerns the February, 2005 search of his computer, but Kelley's problems stem from an investigation by German police officers into the activities of a German citizen, Herman Mumenthaler, in 2002. Executing a search warrant on November 11 of that year, they found 25 outgoing, and 450 incoming, e-mails on Mumenthaler's computers that contained child pornographic attachments. "Gay1dude" was listed as a recipient on four of these e-mails that had attachments depicting images of boys between the ages of 8 and 14, including images of masturbation and oral copulation between two minor males. It was confirmed that "Gay1dude" was a screen name that Kenneth Michael Kelley used for his e-mail account on AOL. He also used other screen names, including "KKEL924," "Mickeydice," "Rockenwry," "Sirfreelancalot," "Coppalozoeetrope," "HIGH5JIVELIVE," and "K MICHAEL KELLEY." Acting on this information, American authorities sought, and obtained, a warrant that was issued on December 2, 2004 to search the content of Kelley's AOL account. This search revealed 500 images of child pornography that Kelley sent or received, consisting primarily of prepubescent males in sexually explicit poses. Kelley's motion to suppress evidence obtained in this search was granted June 17, 2005, and that ruling has not been appealed.

Meanwhile, on February 9, 2005, the government applied for a second warrant to search Kelley's residence, including his computer, for child pornography. The affidavit in support was made by a Special Agent with the United States Depart-

ment of Homeland Security, United States Immigration and Customs Enforcement (ICE), assigned to the office of the Special Agent in Charge, San Francisco, California. It describes the German child pornography investigation involving Mumenthaler, and summarizes the contents of Kelley's AOL account from the December 2, 2004 search. The affidavit also relates details of a separate child pornography trafficking investigation that originated in Wichita, Kansas, involving Ronald D. Hutchings. According to the affidavit, on September 10, 2004, ICE agents served a search warrant on AOL for Hutchings's e-mail accounts which turned up evidence that Kelley, using the screen name "K MICHAEL KELLEY," and Hutchings, using the screen name "Youngbottom16," each received five e-mails with 38 attachments from an individual using the screen name "Badatt178" on August 10 and 15, 2004. Of the 38 attachments, 36 were image files (JPEGs) and two were movie files (MPEGs). The JPEGs included images of boys approximately 10-15 years of age in sexually explicit positions, including erect penises, masturbation, oral copulation between young males and anal intercourse between young and adult males. One MPEG depicts a young boy about four years old engaged in intercourse with an adult male while the other depicts a young girl about six being forced to perform oral sex on an adult male. In addition, the affidavit generally describes how computer connections to the Internet, and e-mail, work. Based on his training and experience, the affiant avers that persons whose sexual objects are minors collect sexually explicit material for their own sexual gratification and fantasy; that they tend to possess and trade this material in a clandestine manner; and that they often assemble lists or addresses of persons with similar sexual interests that may have been generated by personal contact or through advertisements in various publications. The affidavit further states that such persons almost always maintain their material at home or some other secure location where it is readily available, and rarely, if ever, dispose of the collection. Finally, the affidavit explains that the

computer has become one of the preferred methods of distribution of pornographic materials.

A magistrate judge authorized the warrant on February 19, 2005. Forensic examination of Kelley's computer turned up numerous images of child pornography, in both picture and movie formats, depicting young boys engaged in sexual acts with adult males.

Kelley again moved to suppress, maintaining that the affidavit accompanying the February 9, 2005 application, without the evidence seized from his AOL account pursuant to the December 2, 2004 warrant, failed to establish probable cause. Although finding it a close call, the district court agreed. The court reasoned that the excised affidavit did not explain how or where the e-mails, originating from unidentified sources, ended up on the computers of two traffickers. It observed that no volitional act is required by the owner of an e-mail account for that account to receive e-mails, and conversely that it is almost impossible to prevent someone else from sending unwanted e-mail. Therefore, the court held, something more than proof of receipt or opening an e-mail is required to establish probable cause that the recipient is in actual possession of contraband contained in an e-mail attachment. As it was unable to conclude that there was a direct connection between Kelley and known traffickers, and evidence of his intent, or solicition, or actual opening of the attachments was critical, but missing, the court granted Kelley's motion to suppress.

The government timely appeals from this order.

II

The standards for determining probable cause for a search were spelled out in *Illinois v. Gates*, 462 U.S. 213 (1983), and apply with equal force to cases involving child pornography on a computer. *United States v. Gourde*, 440 F.3d 1064, 1069 (9th Cir. 2006) (en banc). Thus, probable cause means a "fair

probability" that contraband or evidence is located in a particular place. *Gates*, 462 U.S. at 246; *Gourde*, 440 F.3d at 1069. Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a "commonsense, practical question." *Gourde*, 440 F.3d at 1069 (citing and quoting *Gates*, 462 U.S. at 230, 246). Neither certainty nor a preponderance of the evidence is required. *Id*. (citing *Gates*, 462 U.S. at 246).

Normally, we do not "flyspeck" the affidavit supporting a search warrant through de novo review; rather, the magistrate judge's determination " 'should be paid great deference.' " *Gourde*, 440 F.3d at 1069 (quoting *Gates*, 462 U.S. at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969))). In addition, the Supreme Court has reminded reviewing courts that "[a]lthough in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, resolution of doubtful or marginal cases in this area should largely be determined by the preference to be accorded to warrants." *Gates*, 462 U.S. at 237 n.10 (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965).

This case presents an unusual situation because a portion of the affidavit was redacted by the district court. The propriety of the redaction is unchallenged. Other circuits have concluded that review of the sufficiency of an excised affidavit cannot be deferential. *See, e.g.*, *United States v. Elkins*, 300 F.3d 638, 651 (6th Cir. 2002); *United States v. Kolodziej*, 712 F.2d 975, 977 (5th Cir. 1983). We agree that this limited exception to the "great deference" rule makes sense, for the magistrate's judgment would have been based on facts that are no longer on the table. In this case, the paragraph that was purged recites powerful evidence seized from Kelley's AOL account that cannot be factored into the probable cause calculus. We have no way of telling the extent to which the excised portion influenced the magistrate judge's determination. Therefore, we will review his determination without particular deference. The ultimate question remains whether there is a

substantial basis for concluding that the search would likely uncover evidence of wrongdoing. *See Gates*, 462 U.S. at 236; *see also United States v. Bishop*, 264 F.3d 919, 924 (9th Cir. 2001) (noting that once an affidavit is purged of illegally obtained information, the court determines whether the remaining facts still afford a substantial basis for concluding that the search warrant was supported by probable cause).

III

Kelley argues, and the government does not seriously dispute, that unwitting receipt of e-mail containing contraband will not support probable cause. *See* 18 U.S.C. § 2252A(a)(2) (criminalizing the knowing receipt of child pornography); *United States v. Romm*, 455 F.3d 990, 998 (9th Cir. 2006) (holding that a person receives child pornography if he seeks it out). The disagreement centers on whether the affidavit is sufficient even though it lacks direct evidence that Kelley actually solicited the offending attachments.

[1] The government maintains that the totality of the circumstances allows the reasonable inference that Kelley wanted the offending e-mails, even though there was no direct evidence that he solicited them, because he was sent multiple e-mails with sexually explicit images of children, he was linked to two individuals known to possess or receive child pornography, the child pornography was of the same type and this shows Kelley's interest, the type of child pornography Kelley was sent is not the kind of material likely to be received by unwitting recipients, and he received the contraband on different occasions at two different screen names. Kelley, on the other hand, points out that there was no evidence about who sent the small number of e-mails or when some of them were sent; or that he solicited, desired, opened, or even received them as the e-mails could have been bounced back by a spam blocker; or that connects him to the offender typology; or that corroborates any interest or intent on his part to obtain or possess child pornography. Therefore, he submits,

the inferences drawn by the district court about personal e-mail are reasonable, whereas the inferences urged by the government are both unsupported in the affidavit and contrary to other reasonable inferences that the court could draw based on its practical experience and common sense.

[2] Recently sitting en banc in *Gourde*, we made clear that probable cause to search a computer for child pornography is determined under the "totality of the circumstances test" reinstated by *Gates*. Accordingly, "a probable cause determination may be based in part on reasonable inferences." *Gourde*, 440 F.3d at 1071. This means, as *Gourde* illustrates, that it can be "fairly probable" that images of child pornography would be found on Kelley's computer without concrete evidence that Kelley actually solicited the e-mails if it appears likely that he did from the facts averred in the affidavit and reasonable inferences drawn from them.

Gourde involved a warrant to search a computer for child pornography in the context of an internet website that displayed child pornography. Gourde had joined the website. The affidavit established that the website, "Lolitagurls.com," contained illegal content; Gourde subscribed to "Lolitagurls-.com," by paying for a membership; membership gave him unlimited access to illegal images; and he remained a member for two months (until the FBI shut down the site). These facts indicated that Gourde intended to have and wanted to have access to illegal images on the site. There were no facts, however, showing that Gourde had actually received or downloaded images. He argued that a search warrant for child pornography may issue only if the government provides concrete evidence, without relying on any inferences, that he *actually* received or possessed offending images. This court rejected this argument. *Id.* at 1074. Instead, this court found that it was not illogical or contrary to common sense to conclude from Gourde's having paid for access to the website for two months that he probably had viewed or downloaded such

images onto his computer. Hence, the warrant was supported by probable cause.

The circumstances in *Gourde* are different from the circumstances in this case, and easier to resolve in favor of the warrant, because Gourde took the affirmative steps of obtaining and paying for a membership to access illegal images which Kelley did not do. Gourde's intentional steps to become a member of the website were the facts supporting the inference that he viewed or downloaded illicit images. It does not follow from the absence of such facts in Kelley's case that the affidavit fails the probable cause test. Rather, the question is whether there is some other set of facts that supports the same kind of inference — that he knowingly received the e-mail attachments.

It is undisputed that Kelley was the subscriber for AOL screen names "Gay1dude" and "K MICHAEL KELLEY," among others. Kelley's account with AOL, which he opened in 1999, was active, with a listed address of a P.O. Box in San Francisco, California. Kelley provided a phone number and credit card for the account. Twenty-five outgoing e-mails and 450 incoming e-mails found on computers at the residence of Herbert Mumenthaler in Düsseldorf, Germany, contained child pornographic attachments. This indicates that Mumenthaler was a trafficker in child pornography. Kelley's screen name "Gay1dude" was the recipient of four e-mails that were also on Mumenthaler's computers. The e-mails received by "Gay1dude" that were also on Mumenthaler's computers contained attachments with 15 child pornographic or erotica images depicting boys between the ages of 7 and 13 in various sexually explicit positions.

In addition, five e-mails with 38 attachments containing child pornography or child erotica from an individual using the screen name "Badatt178" were received by Kelley, using the screen name "K MICHAEL KELLEY," and by Ronald D. Hutchings, who lives in Wichita, Kansas and used the screen

name "Youngbottom16." Thirty-six of the files received by both Kelley and Hutchings were image files and two were movie files. The image files depict young males in various sexually explicit positions; the two movie files show an adult male performing sex acts upon a four-year old boy and a six-to-eight-year old girl.

[3] Thus, the salient facts are that Kelley, using two different screen names, received nine different e-mails with numerous attachments containing the same type of illicit child pornography (depicting sexually graphic conduct by young boys) that two other, unrelated individuals also had on their computers. There is no question that at least one of these individuals, Mumenthaler, also distributes child pornography, and that Hutchings collects it. As the affidavit explains, those who collect child pornography often collect addresses of persons with similar interests as a means of referral, exchange, and profit. The reasonable inference from receipt of e-mails in care of different screen names that pertain to a discrete type of pornography — young boys in sexually explicit poses — and that also ended up on the computers of two unrelated people who were also receiving or distributing the same type of material, is that Kelley was part of network of persons interested in child pornography primarily involving young boys. As a matter of practical, common sense, this is unlikely to occur without prior communication or connection. From these circumstances it is reasonable to infer a "fair probability" that attachments depicting child pornography were addressed to Kelley's screen names because he wanted them to be.

We are mindful of the possibility that these e-mails *could* have been spam, as Kelley suggests. The affidavit does not specifically discount this possibility, and Kelley relies heavily on the fact that distribution of inappropriate and unsolicited material has become a reality of Internet life. We have previously rejected a similar argument, however. *See United States v. Hay*, 231 F.3d 630, 633-34 (9th Cir. 2000). In *Hay*, a warrant to search the defendant's computer was issued based on

information that his Internet address had received a transmission of 19 images of child pornography from a known trader. The transmission was made through a protocol for direct transfer of files, not by e-mail, but like Kelley, Hay argued that pornographic images can be received by spam as well as unintentionally by programs that automatically download files in bulk for later viewing. As in this case, the affidavit said nothing to disprove either possibility. Nevertheless, this court held that the magistrate judge was entitled to infer that there had been prior communication and that the transfers were neither unsolicited nor accidental.

[4] Forceful though the spam argument might be in different circumstances, we are not persuaded by Kelley's view in the circumstances of this case where, like *Hay*, it is reasonable to infer that receipt of transmissions with a particular type of illicit child pornography was neither unsolicited nor accidental. Kelley did not receive *an* e-mail containing illicit pornographic images, or even two or three, but nine such e-mails sent to more than one of his screen names. That he received the same kind of attachments on multiple occasions and in different screen names makes it more probable that the transmissions were not accidental. The attachments were not a varied, random assortment of inappropriate subjects; they were, with one exception, of young boys in graphic sexual poses. Further, the images were not just of pornography, which can be perfectly legal, but were of a plainly unlawful sort. And others apparently interested in receiving or sending the same genre of pornography received (and kept) the same attachments.

We are also unpersuaded that the lack of further evidence such as who sent the e-mails to Kelley or how some of them ended up on Mumenthaler's computer and others on Hutchings's, undermines the "fair probability" of willing receipt shown by the totality of the circumstances. *Gates* does not compel the government to provide more facts than necessary to show a "fair probability." *Gourde*, 440 F.3d at 1071. Con-

sequently, it does not matter whether additional facts could have been obtained or recited if the totality of the circumstances that *are* set forth adds up to a "fair probability" that Kelley willingly received child pornography which will be found on his computer. The affidavit establishes that Mumenthaler had copies of offending e-mails sent to Kelley, and that Hutchings and Kelley were jointly copied on e-mails. The logical inference is that Mumenthaler, who was a trader, had copies of the e-mails sent to Kelley because Mumenthaler was copied on them, or received a forwarded copy with Kelley's screen name in the "header" (sender/recipient information), or sent them to Kelley himself. Whoever the sources may have been, they were including Kelley in their distribution of contraband along with a known trafficker. Likewise, regardless of who "Badatt178" was, he sent Hutchings and Kelley five e-mails on two different days with attachments containing explicit sexual images of young children. It is reasonable to infer that the communications, given these connections, are not purely coincidental.

Relying on *United States v. Weber*, 923 F.2d 1338, 1344 (9th Cir. 1991), Kelley faults the affidavit on the additional ground that it provided an "offender typology" but failed to connect him to the profile. In *Weber*, the defendant placed an order for four pictures of child pornography and, anticipating a planned delivery, officers obtained a warrant to search his house for other similar items. We found inadequate the affiant's boilerplate recitation of how child molesters, pedophiles, and child pornography collectors behave because, absent evidence indicating that Weber was any of these things, probable cause did not exist that Weber would have material other than the four pictures at his house. However, the affidavit in this case provides evidence that Kelley's screen names appear on multiple e-mails with attachments containing child pornography of young boys in sexually explicit positions. The typology reports that persons who collect this type of sexually explicit material rarely dispose of it. While the affidavit offers no external corroboration of Kelley's interest in young boys,

it can be inferred from the fact that nine separate e-mails with the same type of attachments were received on different occasions spanning at least ten months that those images and others would be found on Kelley's computer. *See Hay*, 231 F.3d at 635 (noting that the question is whether contraband is likely to be on the suspect's computer, not whether the affidavit shows that the defendant did or did not fall within the class of persons likely to collect child pornography).

Finally, Kelley disputes the inference that spammers are not likely to send out contraband. He suggests that prescription drugs are often marketed through e-mails, even though it is illegal to do so without a prescription, and that sexually-charged offers to join hotlines or subscribe to pornography websites are common. The receipt of such unwanted or illegal invitations, he posits, does not fairly imply anything about the recipient. We have no occasion to comment on this, for the e-mails Kelley received are more than an invitation; they consist of hardcore child pornography that it is illegal to distribute as well as to receive or possess. The affidavit also indicates that this particular kind of pornography is exchanged clandestinely. Given this practice and the patent illegality of the material received by Kelley, we cannot say that it is insensible to infer, as part of the mix that informs the totality of the circumstances, that indiscriminate distribution was unlikely.

[5] As *Gates*, *Gourde* and *Hay* emphasize, a location such as Kelley's computer can be searched for evidence of a crime even if there is no probable cause for arrest, or a prima facie showing of criminal activity, let alone proof sufficient to prosecute a criminal case beyond a reasonable doubt, or even to prevail under the civil burden that it is more likely true than not that he knowingly received or possessed child pornography. *See Gates*, 462 U.S. at 235; *Gourde*, 440 F.3d at 1072-73; *Hay*, 231 F.3d at 635. Put differently, we are not asked to decide whether Kelley could be arrested, or convicted on the basis of the evidence in the affidavit. We must simply decide whether there is a "fair probability" that, based upon the facts

set forth and inferences from them, his computer would house child pornography which he willingly received. *See Gourde*, 440 F.3d at 1066 (observing that the Fourth Amendment requires "no more" than this). We are not required to decide, and we do not decide, whether receipt of e-mail in any circumstances other than those present in this case would support a finding of probable cause. We conclude only that the totality of the circumstances described in the affidavit for the search of Kelley's computer makes it fairly probable that images of child pornography, which he received willingly, would be found on his computer. The affidavit does not fall short of probable cause solely because it contained no concrete evidence that Kelley actually solicited the nine e-mails he received. Rather, reasonable inferences from the facts averred can, and in this case do, supply the missing links. The reasonable inference here is that Kelley would not have received so many e-mails on different occasions, addressed to different screen names, containing attachments that depict the same genre of illicit child pornography, that were also on the computers of other collectors of the same genre of child pornography, unless he wanted to receive them. For these reasons, the excised warrant was supported by probable cause, and evidence obtained pursuant to it should not have been suppressed.

REVERSED.

THOMAS, Circuit Judge, dissenting:

Each day, billions of unsolicited email messages are sent over the Internet.[1] These unwanted emails, popularly termed

[1]*See* Adam Hamel, Note, *"Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?,"* 39 New Eng. L. Rev. 961, 961 (2006) ("Spam accounts for as much as eighty percent of the estimated fifty-seven billion e-mail messages that are transmitted across the Internet daily."); Brad Stone, *Spam Doubles, Finding new Ways to Deliver Itself*, N.Y. Times, Dec. 6, 2006, at A1 (noting that "[w]orldwide volumes of spam have doubled since last year" and that nine out of every ten email messages is junk mail).

"spam,"[2] often carry commercial messages. Many of the commercial messages are dubious in nature and origin, and a substantial proportion consists of pornographic images or links to pornographic websites. Spam may also contain child pornography or links to illegal websites containing child pornography.[3] The true content of these messages is often disguised. As the United States Senate Committee on Commerce, Science, and Transportation noted:

> Pornographic spam is more likely than other spam to contain fraudulent or misleading subject lines. In its recent report, the FTC found that more than 40 percent of all pornographic spam either did not alert recipients to images contained in the message or contained false subject lines, thus "making it more

[2]The term "spam" in this context does not refer to the processed meat product invented by Jay Hormel in 1937, but apparently was derived from a sketch by the British comedy group Monty Python's Flying Circus first broadcast in 1970, in which a restaurant patron is presented with a menu containing nothing but variants of Spam. *Compuserve, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 n.1 (S.D. Ohio 1997). As part of the routine, a group of Vikings in the restaurant insistently sing a chorus about Spam, increasing in volume until other conversation is impossible. "Hence, the analogy applied because [unsolicited commercial e-mail] was drowning out normal discourse on the Internet." Hamel, 39 New Eng. L. Rev. at 963 n.18.

[3]*See, e.g.*, Leslie Brooks Suzukamo, *Reports of Child-Porn Spam Are Increasing*, St. Paul Pioneer Press, Dec. 17, 2001, at A1; Paul Mores, *Child Porn E-mails Shock Residents Hit by Spam*, Hamilton Spectator, Oct. 18, 2005, at A3; Mark I. Johnson, *Volusia Seizes Child Porn Stash; Edgewater Man Netted in N.Y.-Based Sting*, Daytona News-J., Oct. 4, 2005, at 1C (describing child pornography investigation that began with a tip from someone who received "a spam email offering child pornography"); *The Spaminators: So Why Do They Call It "Spam"?*, Chi. Trib., April 23, 2003, at 9 (stating that the FBI investigated child pornography spam in 1996). *See also* Anti-Child Porn Organization, at http://www.antichildporn.org/mailadvisory.html (describing spam containing embedded images of child sexual abuse); FBI, Baltimore Field Office, "Cyber Crime," *at* http://baltimore.fbi.gov/cyber_crime.htm (requesting reports of child pornography spam).

> likely that recipients would open the messages without knowing that pornographic images will appear."

United States Senate Committee on Commerce, Science, and Transportation, *CAN-SPAM Act of 2003,* S. Rep. 108-102, p. 4 (July 16, 2003).

Despite the enormous volume of unsolicited pornographic emails sent every day, with the true content concealed from the recipient, the majority holds that the mere transmission of unsolicited pornographic emails creates probable cause to search the entire house of the email recipient. Because I respectfully disagree with this conclusion, and because it conflicts with our precedent, I would affirm the well-reasoned judgment of the district court that the warrant lacked probable cause.

I

This is not the first time we have confronted the question of whether unsolicited communication can form the basis for probable cause. In *United States v. Weber*, we considered the government's claim that it had probable cause to search a defendant's house for child pornography based on evidence that he had been sent — but had never picked up from the post office — material advertising child pornography and had later ordered four photographs from a government-created distributor. 923 F.2d 1338, 1344 (9th Cir. 1991). We concluded under those circumstances that the government lacked probable cause for the search. We held that the mere receipt of pornographic images and the subsequent ordering of photographs did not create a "fair probability" that the government would find child pornography at the defendant's house on the date of the search. *Id.* at 1344-45. Significant to the reasoning of *Weber* was the lack of evidence that the defendant was either a child molester or a collector of child pornography. *Id.* at 1345.

We recently considered the impact of *Weber* and its progeny on pornography distributed via the Internet in *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc). In *Gourde*, we examined a search of a defendant's computer based on affidavit evidence that he had taken " 'steps to affirmatively join' the website" featuring downloadable child pornography. *Id.* at 1068. In sustaining the warrant, we emphasized that "Gourde's status as a member manifested his intention and desire to obtain illegal images." *Id.* at 1070. In order to become a member, Gourde had to provide his home address, his email address, and his credit card information. *Id.* He then had to consent to have the fee deducted from his credit card every month. *Id.* We explained that "these steps, however easy, *only could have been intentional* and were not insignificant. *Gourde could not have become a member by accident or by a mere click of a button*." *Id.* (emphasis added).

In *Gourde*, we distinguished *Weber* precisely on the grounds of Gourde's unambiguous affirmative steps. We explained that "Gourde's *continuous, affirmative steps* to access a child pornography website can hardly be compared to the single controlled buy in *Weber* two years after his initial, and unconsummated, foray into child pornography." *Id.* at 1074 (emphasis added). *See also United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997) (noting that defendant took affirmative steps by placing telephone calls to and downloading photographs from a computer bulletin board system located in Denmark); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004) (relying in part on evidence in the affidavit that defendant took affirmative steps to join child pornography group and did not cancel his membership even though it was easy to do so).

In addition to holding that probable cause for a residential search was established when a defendant took affirmative steps to acquire child pornography, we have also sustained searches based on evidence suggesting that the defendant is a pedophile or child pornography collector. In *United States v.*

Hay, we upheld a magistrate judge's finding of probable cause by relying in part on the fact that "there was evidence of Hay's extreme interest in young children." 231 F.3d 630, 632-33, 634 (9th Cir. 2000). This evidence, combined with his receipt of nineteen child pornography images through a direct transfer download onto his computer, distinguished *Hay* from *Weber* and made it much more probable that the images "were neither unsolicited nor accidental." *Id.* at 634.

Similarly, the Tenth Circuit has relied on evidence of a defendant's personal history, in combination with his receipt of emails containing child pornography, to establish probable cause. *United States v. Rice*, 358 F.3d 1268 (10th Cir. 2004), *overruled on other grounds by United States v. Rice*, 405 F.3d 1108 (10th Cir. 2005). There, the defendant was a teacher who had, in a previous school system, taken pictures of two young girls in bikinis that "suggested an unhealthy and inappropriate interest in the bodies of young girls." *Id.* at 1275. This additional evidence of the defendant's interest in young children was present in the affidavit and was an important factor in the Tenth Circuit's decision to find the affidavit sufficient. *Id.*

In sum, we have sustained searches based on evidence (1) of affirmative acts to acquire child pornography, (2) of the defendant's tendencies toward pedophilia, or (3) that the defendant was a collector of child pornography. We have never held — until today — that mere receipt of unsolicited pornographic material, without more, establishes probable cause to search a residence for child pornography.

II

The paucity of the evidence that the government offered in support of the warrant is quite evident. The only evidence upon which the government relied at the time of the search was that Mr. Kelley had been sent nine emails containing child pornography over a period of at least nine months, quite

possibly longer. There was no evidence that Mr. Kelley requested the emails, viewed the emails, or actually received the emails in his "Inbox." There was no evidence refuting the possibility that Mr. Kelley's email program routed the emails to his spam folder, or that Mr. Kelley deleted the emails upon receipt. Nor was there evidence that Mr. Kelley at any point made any affirmative attempt to obtain child pornography or that he collected child pornography or had any affinity for it. In short, there was no evidence that these nine emails were anything more than unsolicited spam.[4]

Holding that the evidence the government submitted in this case constituted probable cause for an extensive residential search cannot be reconciled with the principles we adopted in *Weber*, *Gourde*, and *Hay*.

I can well understand the government's motivation. Child pornography is a scourge on our nation. But every hour, millions of unsolicited and deceptively disguised emails are sent to innocent computer users. Lowering our standards of probable cause to permit government intrusion into private residences based solely on proof of mere transmittal of unsolicited email constitutes an unwarranted erosion of the Fourth Amendment.

For these reasons, I respectfully dissent.

[4]Aside from the allegation that Kelley had been sent pornographic messages, the rest of the probable cause affidavit consisted of generic, boilerplate language — the use of which we eschewed in *Weber*. 923 F.2d at 1345 (noting that the affidavit contained "rambling boilerplate recitations" about pedophiles and collectors of child pornography, but "not a whit of evidence . . . indicating that Weber was a 'child molester.' ").