
FOURTH AMENDMENT — SEARCH AND SEIZURE — NINTH CIRCUIT UPHOLDS ISSUANCE OF WARRANT BASED ON E-MAIL RECIPIENT LIST. — *United States v. Kelley*, 482 F.3d 1047 (9th Cir. 2007).

The rise of cybercrime has sparked debate about its relationship to traditional “brick and mortar” offenses.¹ The novelty of the Internet has at times obscured the functional similarities between some electronic interactions and those that take place in the “real” world. Recently, in *United States v. Kelley*,² the Ninth Circuit held that passive receipt of child pornography by e-mail established probable cause to search the recipient’s home and computer. The court relied upon the common receipt of the same e-mail by both the defendant and known child pornography offenders to infer that the defendant knowingly and intentionally possessed the content. The court in its analysis erred by declining to fully recognize the utility of analogies to more traditional crimes. To cure this analytic deficiency, future courts should instead evaluate associations arising solely from e-mail according to the level of reciprocity demonstrated by the conduct involved. By evaluating e-mail interactions on a functional basis, courts will more faithfully adapt established Fourth Amendment principles to Internet-based contacts. Such an approach appropriately recognizes that although advancing technology presents unique challenges, courts can nonetheless often ground their analyses in the law of more traditional crimes.

While investigating a German child pornography suspect, investigators came across four illegal e-mails on which a screen name later linked to Kenneth Kelley appeared as a recipient.³ On the basis of this information, U.S. investigators obtained a search warrant for Kelley’s America On Line (AOL) account.⁴ Another screen name associated with Kelley’s account then surfaced in a separate investigation of a child pornography suspect in Kansas.⁵ Combining the fruits of the first search⁶ with the information about Kelley’s other screen names, the government obtained a second warrant, which authorized a search of Kelley’s home and computer.⁷ The search revealed multiple files

¹ See, e.g., Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001); Sean J. Petrie, Note, *Indecent Proposals: How Each Branch of the Federal Government Overstepped Its Institutional Authority in the Development of Internet Obscenity Law*, 49 STAN. L. REV. 637, 638 (1997).

² 482 F.3d 1047 (9th Cir. 2007).

³ *Id.* at 1049.

⁴ *Id.*

⁵ *Id.*

⁶ The search of Kelley’s AOL account revealed that he had sent or received 500 images of child pornography. *Id.*

⁷ *Id.* at 1049–50.

containing child pornography.⁸ At trial, the district court granted Kelley's motion to suppress the evidence obtained from his AOL account, finding that the affidavit used to obtain the warrant failed to establish probable cause.⁹ The fruits of the first search were then redacted from the affidavit filed to support the second warrant. Once redacted, the affidavit indicated that Kelley had received nine e-mails, attached to all of which were sexually explicit images of young boys.¹⁰ It also contained an offender typology, consisting of general statements about behaviors common among child pornography offenders.¹¹ The affidavit, however, did not provide a concrete link between Kelley and this typology.¹²

Kelley ultimately filed a motion to suppress the evidence uncovered in the home search.¹³ The district court granted Kelley's second suppression motion, finding no probable cause because the affidavit did not include evidence of a direct connection between Kelley and known child pornography traffickers.¹⁴ Distinguishing prior Ninth Circuit Internet child pornography cases, the district court emphasized that the court of appeals had found probable cause only where there had been some indicia of either intent to solicit the material or affirmative steps to download it.¹⁵ The court concluded that more than mere receipt was required to establish probable cause for a home search; the difficulty of determining whether e-mails were solicited did not justify lowering the probable cause standard to permit home searches absent any indication that the recipient desired the offending e-mails or actually viewed their contents.¹⁶

The Ninth Circuit reversed. Judge Rymer¹⁷ held that Kelley's receipt of contraband e-mails, along with reasonable inferences, established probable cause for the search. The court began by examining its precedent in *United States v. Gourde*,¹⁸ which made clear that

⁸ *Id.* at 1050.

⁹ See *United States v. Kelley*, No. CR 05-0125 PJH, at 5-6 (N.D. Cal. July 22, 2005) (order granting defendant's second motion to suppress) [hereinafter Order Granting Second Motion].

¹⁰ *Kelley*, 482 F.3d at 1048.

¹¹ *Id.* at 1049-50.

¹² See *id.*

¹³ *Id.* at 1049.

¹⁴ See Order Granting Second Motion, *supra* note 9, at 10-11 (noting that absent a showing of a direct connection between Kelley and known child pornography offenders, evidence of intent, solicitation, or actual opening of attachments was "essential").

¹⁵ *Id.* The district court distinguished, for example, *United States v. Hay*, 231 F.3d 630, 635 (9th Cir. 2000), which upheld a home search where the affidavit showed that the defendant had actually received nineteen images of child pornography via direct transfer. Order Granting Second Motion, *supra* note 9, at 7.

¹⁶ Order Granting Second Motion, *supra* note 9, at 10.

¹⁷ Justice O'Connor (ret.), sitting by designation, joined Judge Rymer's opinion.

¹⁸ 440 F.3d 1065 (9th Cir. 2006) (en banc).

probable cause to search a personal computer for evidence of child pornography turns on the totality of the circumstances, including reasonable inferences.¹⁹ Judge Rymer admitted, however, that the facts in *Gourde* were distinguishable and had more clearly supported a finding of probable cause.²⁰ *Gourde* had taken affirmative, intentional steps to become a member of a website that provided access to illegal images, whereas Kelley could have passively received the contraband e-mail attachments without either intention or knowledge.²¹ Given this factual distinction, the court looked for another aspect of the fact pattern that could support a similar inference of knowing receipt.²² The court bridged this gap by adapting its reasoning in *United States v. Hay*²³ to the e-mails in *Kelley*.²⁴ *Hay* involved receipt of pornographic materials via a direct file transfer protocol (FTP), and there the court rejected the defendant's contention that he received the files without soliciting them.²⁵ The court noted that two of Kelley's screen names surfaced in two separate, unrelated investigations of pornography offenders, and the multiple independent sources of associational evidence against Kelley largely eliminated the possibility that the e-mails were unsolicited spam.²⁶

Judge Thomas dissented.²⁷ He began by discussing the prevalence of spam, noting that such messages may include images of child pornography or links to websites displaying illegal content.²⁸ Judge Thomas analogized *Kelley* to *United States v. Weber*,²⁹ in which the court found that "mere receipt of pornographic images" via postal mail did not generate probable cause for a home search.³⁰ Judge Thomas found

¹⁹ *Id.* at 1071.

²⁰ *Kelley*, 482 F.3d at 1052.

²¹ *See id.*

²² *Id.*

²³ 231 F.3d 630 (9th Cir. 2000).

²⁴ *Kelley*, 482 F.3d at 1053. The defendant in *Hay* "argued that pornographic images can be received by spam as well as unintentionally by programs that automatically download files in bulk [The] 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." *Id.* Further, the decision in *Hay* rested in part on the fact that there was evidence of "Hay's extreme interest in young children." *Id.* at 1057 (Thomas, J., dissenting) (quoting *Hay*, 231 F.3d at 634) (internal quotation marks omitted).

²⁵ *Id.* at 1053 (majority opinion). The *Kelley* court did not, however, discuss whether differences between e-mail and FTP technologies might affect the relative probabilities that material received through the different pathways was unsolicited spam. *See id.*

²⁶ *See id.*

²⁷ *Id.* at 1055 (Thomas, J., dissenting).

²⁸ *Id.* at 1055-56. In support of his assertion, Judge Thomas cited several newspaper articles, as well as FBI requests for reports of child pornography spam. *Id.* at 1056 n.3.

²⁹ 923 F.2d 1338 (9th Cir. 1990).

³⁰ *Kelley*, 482 F.3d at 1056 (Thomas, J., dissenting). In *Weber*, the government had evidence that the defendant had been mailed, but never picked up, material advertising child pornography. The court concluded that the government lacked probable cause to search Weber's home based on

this comparison more illuminating than that to *Gourde*, as the defendant in *Gourde* had committed affirmative acts that showed that he “could not have become a member [of an illegal website] by accident.”³¹ He further noted that other Ninth Circuit child pornography cases had required some additional corroborating evidence beyond mere receipt to establish probable cause for home searches.³² Judge Thomas found this additional showing to be missing and saw nothing to indicate that the nine e-mails sent to Kelley were not spam.³³ Judge Thomas concluded by counseling against the majority’s “unwarranted erosion of the Fourth Amendment” and arguing that the court reached a result inconsistent with Ninth Circuit precedent as established by *Weber*, *Gourde*, and *Hay*.³⁴

Under the totality of the circumstances standard articulated in *Illinois v. Gates*³⁵ and reiterated in *Gourde*, probable cause requires a “fair probability” that evidence of a crime will be found if a search is carried out.³⁶ Courts have recognized that a suspect’s association with a known criminal offender can sometimes serve as one of many factors that may establish probable cause.³⁷ The reasonable inference to be drawn from such association, however, is also subject to well-recognized limitations: minimal or otherwise unreliable contact cannot create probable cause for a search or arrest.³⁸ To achieve results properly in line with the commitment to individual privacy embodied in traditional Fourth Amendment law,³⁹ courts facing fact patterns like

this limited evidence, because mere receipt of illicit images was insufficient to create a “fair probability” that child pornography would be found in the defendant’s home. *Weber*, 923 F.2d at 1343–45 (citing *United States v. Rabe*, 848 F.2d 994, 997 (9th Cir. 1988)).

³¹ *Kelley*, 482 F.3d at 1057 (Thomas, J., dissenting) (quoting *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006) (en banc)) (emphasis omitted).

³² *Id.* Such additional evidence had included affirmative acts to acquire child pornography, a tendency toward pedophilia supported by external corroborating evidence, or a showing “that the defendant was a collector of child pornography.” *Id.*

³³ *Id.*

³⁴ *Id.* at 1058.

³⁵ 462 U.S. 213 (1983).

³⁶ *See id.* at 246; *see also Gourde*, 440 F.3d at 1069.

³⁷ *See, e.g., Sibron v. New York*, 392 U.S. 40, 68 (1968) (Douglas, J., concurring); *United States v. Collins*, 427 F.3d 688, 692 (9th Cir. 2005); *United States v. Hillison*, 733 F.2d 692, 697 (9th Cir. 1984); *United States v. Oates*, 560 F.2d 45, 60 (2d Cir. 1977).

³⁸ *See, e.g., Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (finding that “mere propinquity” to offender was insufficient to generate probable cause to search bar patrons); *Sibron*, 392 U.S. at 62–63 (finding unreasonable the inference that a defendant observed talking to drug addicts was engaged in drug trafficking); *United States v. Soyland*, 3 F.3d 1312, 1314 (9th Cir. 1993) (finding that “mere presence” at vehicle search where inspector found drugs was insufficient to generate probable cause for a personal search).

³⁹ *See, e.g., Camara v. Mun. Court*, 387 U.S. 523, 537 (1967) (stating that the Fourth Amendment reasonableness standard requires “balancing the need to search against the invasion which the search entails”).

Kelley's should distinguish reciprocal online interactions from the passive receipt of messages that could potentially be unsolicited spam.

Although the warrant standard requires only probable cause to search, this reduced evidentiary burden does not render *any* chance of uncovering evidence sufficient.⁴⁰ The legal system often treats purely probabilistic evidence — that based solely on generalizations about a category of individuals to which the suspect arguably belongs — with skepticism.⁴¹ The lines around what constitutes a “reasonable” inference of knowing receipt need to be redrawn where the disincentives to random distribution of illegal content are heavily diluted, as they are when criminal transactions are conducted through the Internet.⁴² Pornographers have demonstrated a particular eagerness to adapt their distribution schemes to take full advantage of emerging technologies.⁴³

Although the use of associational inferences is, for example, very common in evaluating probable cause to search and arrest in drug cases,⁴⁴ the inferential strength of the associations generated by drug sales is distinguishable from those created by e-mail receipt. Anyone with an e-mail account can be the unwitting recipient of contraband; the recipient need not perform any act for a message to be sent and appear in his inbox.⁴⁵ The likelihood that a person will unintention-

⁴⁰ See, e.g., *United States v. Patacchia*, 602 F.2d 218, 220 (9th Cir. 1979) (finding no probable cause to search absent “the fact or two necessary to convert a strong hunch into probable cause”).

⁴¹ See FREDERICK SCHAUER, *PROFILES, PROBABILITIES, AND STEREOTYPES* 79–107 (2003). Where, for example, the standard of proof is a preponderance of the evidence, statistical evidence that proves the plaintiff’s case to a probability of .51 is routinely held insufficient to support a finding of liability. See *id.* at 81.

⁴² See Katyal, *supra* note 1, at 1010, 1042 (explaining that “[t]he lack of high perpetration costs is one factor that explains the rise in cybercrime” and arguing that Internet criminal offenders find it “easier to escape detection and apprehension”).

⁴³ See Mark Griffiths, *Sex on the Internet: Observations and Implications for Internet Sex Addiction*, 38 J. SEX RES. 333, 333 (2001).

⁴⁴ See, e.g., *United States v. Gutierrez-Arce*, 134 F. App’x 143, 145 (9th Cir. 2005) (finding warrantless arrest did not violate Fourth Amendment where defendant was observed driving in parking lot while an associate conducted drug transactions); *United States v. Garza*, 980 F.2d 546, 550 (9th Cir. 1992) (discussing relevance to probable cause determination of “arresting agents’ knowledge that drug dealers are unlikely to use innocent drivers in a multi-kilogram cocaine delivery”); *United States v. Hillison*, 733 F.2d 692, 697 (9th Cir. 1984) (finding that defendant’s association with known drug dealers at time of their criminal conduct created inference that he knew what they were doing). Concerns about the use of standards amounting to “guilt by association” have also been raised with regard to practices such as FBI surveillance targeting particular political or religious groups, especially in connection with national security and antiterrorism efforts. See, e.g., Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 623–25 (2004).

⁴⁵ People frequently receive unsolicited e-mail messages without knowing the precise nature of the contents, or sometimes even without knowing that the e-mail has been sent or received. As spam filtering programs become more common, it becomes less reasonable to assume that messages are even received: an illegal e-mail sent from one computer can be automatically blocked by a spam filter before it can be delivered to the intended recipient’s inbox. See Appellee’s Responding Brief at 18 n.13, *Kelley*, 482 F.3d 1047 (No. 05-10547), 2006 WL 2379704 (arguing that if de-

ally receive contraband drugs from a dealer he meets is, by comparison, very low. Absent a concrete indication of the breadth of the distribution of the pornography sent to Kelley, the court lacked the baseline probabilities it needed to draw a strong associational inference. If a trafficker sent the e-mails unsolicited to a hundred thousand people, one of whom was a known child pornography offender, the fact of shared receipt would tell the court nearly nothing about the probability that a search of Kelley's home would uncover evidence.⁴⁶ Pure chance suggests that such a broad distribution scheme, absent any concrete analysis of the particular characteristics of the group of recipients of a message, will likely encompass a member of any category of offenders for whom investigators wish to search. In short, the realities of electronic communication today are such that the mere fact of a name appearing on a recipient list, without more information, cannot tell a court anything about whether the e-mail was solicited, opened, or even received.

Courts have at times recognized the functional distinctions among some technologically similar cases and have sought to devise sorting mechanisms to better understand the relationships among the parties involved. Even when courts have evaluated inferences drawn from website membership, where joining the site is often an affirmative action that indicates a desire to receive contraband, some courts have noted that a subdivision of computer contacts can be a useful means of evaluating the evidence submitted in search affidavits. For example, in *United States v. Coreas*,⁴⁷ the Second Circuit suggested that it might have found probable cause for a home search had investigators shown that members of a website that offered access to child pornography had actually received e-mails from the site.⁴⁸ The single act of clicking a button to join an illicit website *might* support probable cause in some cases,⁴⁹ but the *Coreas* court sought to distinguish mere membership from the defendant's more substantial, bidirectional transaction of

defendant used a spam blocker, the e-mails would never have been "received" on his computer, and any evidence of bounce-back would have appeared only on sender's computer); see also Leslie Brooks Suzukamo, *Reports of Child-Porn Spam Are Increasing*, ST. PAUL PIONEER PRESS, Dec. 17, 2001, at 1A.

⁴⁶ The affidavit lacked several key facts about the pattern of e-mail distribution that led to Kelley's association with child pornographers. The facts allow for multiple explanations for the presence of the e-mails on the relevant computer. See *Kelley*, 482 F.3d at 1049–50.

⁴⁷ 419 F.3d 151 (2d Cir. 2005).

⁴⁸ *Id.* at 156–58.

⁴⁹ See Lauren E. Curry, Note, *Whose Candy Are We Really Taking?: An Exploration of the Candyman Cases and the Divide Within the Second Circuit*, 75 *FORDHAM L. REV.* 119, 120 (2006) (noting the existence of a marked split of opinion as to what constituted probable cause in the "Candyman" child pornography e-group cases).

joining the website and receiving requested content via e-mail.⁵⁰ This requirement of reciprocal transfer of information strengthened the inference the court drew from the suspect's association with the website, its creators, and its other members. The *Coreas* court appropriately recognized the substantive differences that exist among different types of transactions that involve the computerized transfer of child pornography.

If courts continue to infer knowing receipt and to authorize home searches on the basis of even a very tenuous association with a known offender, the potential for electronic harassment to blossom into government-authorized invasion will increase to troubling levels. A malicious acquaintance need only introduce someone's e-mail address to a spam distribution network,⁵¹ and the recipient, even if he does not know that he has been sent an offending e-mail, could be subjected to a full home search.⁵² The *Kelley* court's strong emphasis on multiple (unidirectional) connections to child pornographers does not significantly alleviate the risk of unwarranted invasion. The typology provided in the search affidavit explained that collectors and traffickers often generate lists of individuals with similar interests and create clandestine networks through which they share their collections, suggesting that an e-mail address, once introduced into the network, might find its way to new offenders without any additional effort by the recipient or whoever provided his e-mail address in the first instance.

The *Kelley* majority appeared unwilling to go so far as to say that receipt of a single e-mail was enough to support an inference of willing receipt.⁵³ But when one considers the incentives to use e-mail spam as a means of harassment and the ease with which one could create multiple, apparently "independent" sources of such material, Judge Rymer's conclusion that multiple associations can be compounded to cre-

⁵⁰ The court suggested that a two-step exchange provided better support for an inference of knowing receipt, as it tended to reduce the likelihood that membership occurred by "accident" and indicated that the defendant not only took action to join the website, but also failed to cancel his membership. See *Coreas*, 419 F.3d at 156.

⁵¹ Information about the methods used by spammers to collect e-mail addresses suggests that merely making an address widely available on the Internet, without targeting it specifically to child pornographers, might greatly increase the odds that its owner will receive spam e-mails with illegal content. See *Suzukamo*, *supra* note 45.

⁵² The court in *Kelley* knew, although it could not explicitly consider, that the unredacted affidavit contained considerable evidence indicating Kelley's extensive possession of child pornography. This knowledge may have colored the court's evaluation of the redacted affidavit before it. That the fruits of the first search indicated Kelley's possession of criminal evidence, however, does not eliminate the possibility that genuinely innocent parties could receive the same materials as child pornography offenders.

⁵³ See *Kelley*, 482 F.3d at 1055 (declining to decide if receipt of e-mail in different circumstances would support finding of probable cause for home search).

ate a stronger inference does not meaningfully separate spam victims from child pornography solicitors. Police resources would be better directed towards investigations of substantively superior leads — such as those that include evidence of reciprocal associations with known offenders or other corroborating evidence of solicitation — that are more likely to result in the successful prosecution of the most active child pornography offenders. Previous case law indicates no shortage of such cases on which investigators might focus their energies.⁵⁴

Legal reasoning relies on the application of necessarily imperfect analogies when courts confront novel, highly technological fact patterns. Online relationships, such as those between spammers and the recipients of their messages, can be analogized to many different physical-space relationships. Wise Fourth Amendment policy depends on choosing the best among these several plausible analogies to produce consistent and reasonable outcomes. Receipt of an e-mail message, or multiple messages for that matter, often says no more about the recipient than does the receipt of multiple telemarketers' phone calls or multiple instances of junk mail; in fact, given the lower costs of Internet communication and crime, it may well say even less.

⁵⁴ See, e.g., *United States v. Rice*, 358 F.3d 1268 (10th Cir. 2004), *vacated*, 543 U.S. 1103 (2005), *overruled on other grounds by* 405 F.3d 1108 (10th Cir. 2005); *United States v. Froman*, 355 F.3d 882 (5th Cir. 2004); *United States v. Hay*, 231 F.3d 630 (9th Cir. 2000); *United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997).