Science and Technology Law Review

Volume 11 | Number 1 Article 6

2008

United States v. Gourde: Curtailing Privacy in the Technological World

Joseph Perera

United States v. Gourde: Curtailing Privacy in the Technological World

*Joseph Perera**

I. INTRODUCTION

Americans expect a certain amount of privacy in their lives. Since computers have become a prominent part of life, Americans expect that principles of privacy apply to their computer use as well. While many use computers to help make life easier, some use technology for illegal purposes. Like any other tool of crime, technology may become evidence that the government can seize and search in order to prosecute criminals. But, like any other government seizure, the government's power to investigate must be balanced with the privacy rights of individuals.

Recently, several cases involving the search and seizure of computers owned by accused collectors of child pornography have dealt with the scope of probable cause within the context of technology. The United States Court of Appeals for the Ninth Circuit delivered a ruling in *United States v. Gourde* that gives the government more leeway in establishing probable cause for the search and seizure of an individual's computer.[1] The opinion provides precedent that increases the power of the government at the expense of the privacy of computer users.

II. FACTS AND PROCEDURAL BACKGROUND

In August 2001, an FBI agent came across the website Lolitagurls.com, which contained "images of nude and partially-dressed girls, some prepubescent."[2] The website contained the language "THIS SITE updated weekly WITH NEW LOLITA PICS. This site is in full compliance with United States Code Title 18 Part I Chapter 110 Section 2256."[3] The website offered viewers three ways to access further pages on the site: "(1) take a free tour of the site, (2) become a new member of the site, or (3) log in as a returning member."[4] To become a member, a viewer would submit their credit card information to the website and the card would be charged $19.95 a month.[5] "Members received unlimited access to the website and . . .

---

* Joseph Perera is a May 2008 candidate for Juris Doctor at Southern Methodist University Dedman School of Law. A member of Phi Beta Kappa, he graduated *magna cum laude* from the University of Dallas with a Bachelor of Arts in History, and a concentration in Medieval and Renaissance Studies. He would like to express his gratitude to his family, his friends, and his teachers for their encouragement, support, and guidance.

1. United States v. Gourde (*Gourde III*), 440 F.3d 1065 (9th Cir. 2006).
2. *Id.* at 1067.
3. *Id.*
4. *Id.*
5. *Id.*

[could] . . . download images directly from the website."[6] The FBI agent registered as a member of Lolitagurls.com and "captured hundreds of images that included adult pornography, child pornography, and child erotica."[7]

In January 2002, the FBI had "identified the owner and operator of Lolitagurls.com and . . . executed a search warrant" and seized several items.[8] One of these items was the owner's computer containing images that had been displayed on the website.[9] The owner admitted that he operated the child pornography website, Lolitagurls.com, for a profit.[10]

The FBI issued a subpoena to the company that handled the credit card processing for Lolitagurls.com and obtained records about the website's subscribers.[11] These "records listed Gourde as a member and provided his address, date of birth, e-mail address and the fact that he had been a subscriber from November 2001 until January 2002."[12] With this information and the information provided in an affidavit by Agent David Moriguchi, the FBI obtained a search warrant from a magistrate judge to search Gourde's residence and computers.[13] Pursuant to this order, the FBI seized Gourde's "computer, which contained over 100 images of child pornography and child erotica."[14]

Gourde filed a motion to suppress the images taken from his computer, but the court applied a "common-sense" approach and denied the motion.[15] The court held that evidence of a subscription to a website containing both legal and illegal pornography "provided the necessary 'fair probability' to 'look further.'"[16] Gourde then "pleaded guilty to one count of possession of visual depictions of minors in explicit conduct in violation of 18 U.S.C. §§ 2252(a)(4)(B), 2252(b)(2) and 2256."[17] "Gourde conditioned his plea on his right to appeal the district court's denial of his motion to suppress."[18] The Court of Appeals for the Ninth Circuit subsequently held that the affidavit "failed to establish a fair probability that contraband or evidence of a crime would be found on Gourde's computer" and reversed the denial of the

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.* at 1067-68.

13. *Id.* at 1068.

14. *Id.* at 1067-68.

15. *See id.* at 1068-69.

16. *Id.* at 1069.

17. *Id.*

18. *Id.*

motion to suppress.[19] The Ninth Circuit later decided to rehear the case *en banc*.[20]

III. The Court's Holding and Analysis

Circuit Judge McKeown began the opinion with an analysis of the Fourth Amendment of the U.S. Constitution.[21] The Fourth Amendment prohibits "unreasonable search and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation."[22] The U.S. Supreme Court examined the issue of probable cause within the Fourth Amendment context in *Illinois v. Gates*.[23] In *Gates*, the Court employed a "totality of the circumstances" test and defined probable cause as "fair probability;" neither certainty nor a preponderance of the evidence is necessary.[24] To issue a search warrant, a judge needs only to answer the "commonsense practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place."[25] A probable cause determination may be based partly on reasonable inferences.[26]

The court then examined the content of the website itself.[27] Gourde argued that the affidavit failed because it did not properly describe the contents of Lolitagurls.com.[28] However, since the owner of the site admitted that it was a child pornography website, "the magistrate judge had no reason to question whether the images described constituted child pornography," thus quashing Gourde's objections.[29] Furthermore, the website's disclaimer stating that the website complied with federal law functioned only as "mere window dressing that absolves the owner or users of nothing."[30]

Having established that the site contained illegal images, the court next established that Gourde both had access and wanted access to these images. Since Gourde was a paying subscriber to a child pornography site for over two months, he had the opportunity to download and keep these images in

19. United States v. Gourde (*Gourde I*), 382 F.3d 1003, 1012, 1014 (9th Cir. 2004).

20. United States v. Gourde (*Gourde II*), 416 F.3d 961 (9th Cir. 2005).

21. *Gourde III*, 440 F.3d 1065, 1069 (9th Cir. 2006).

22. U.S. Const. amend. IV.

23. Illinois v. Gates, 462 U.S. 213 (1983).

24. *Id.* at 241, 246.

25. *Id.* at 230.

26. *See id.* at 240.

27. *Gourde III*, 440 F.3d 1065, 1070 (9th Cir. 2006).

28. *Id.*

29. *Id.*

30. *Id.*

violation of 18 U.S.C. § 2252.[31] By submitting his home address, e-mail address, credit card information and authorizing a monthly charge, Gourde's actions to gain access to the site were clearly intentional.[32] This evidence supports the conclusion that "Gourde had paid to obtain unlimited access to images of child pornography knowingly and willingly, and not involuntary, unwittingly, or even passively" and that there was a "near certainty that his computer would contain evidence of a crime had he received or downloaded images in violation of § 2252."[33] The court stated that his computer would contain a "digital footprint" of any downloaded images and that an expert could restore the images, even if Gourde had made an effort to erase them.[34]

Since the affidavit established that "the site had illegal images, Gourde intended to have and wanted access to these images, and these images were almost certainly retrievable from his computer," the magistrate judge only needed to infer that there was a "fair probability" that Gourd had received or downloaded illegal images in order to find probable cause for the search warrant.[35] The court held that such an inference successfully met the "fair probability" test stating that "it neither strains logic nor defies common sense to conclude, based on the totality of these circumstances, that someone who paid for access for two months to a website that actually purveyed child pornography probably had viewed or downloaded such images onto his computer."[36]

Additionally, the affidavit's profile of child pornographers and their use of computers strengthened the inference that Gourde received or downloaded images.[37] The affidavit described child pornographers as "pack rats," collecting images of child pornography for sexual gratification, rarely disposing of the sexually explicit images, and "seek[ing] out like-minded individuals, either in person or on the Internet."[38] Agent Mariguchi argued in the affidavit that Gourde fit the profile of a child pornography collector because he joined a subscription website that would allow him to view these images in privacy.[39] The court likened Mariguchi's affidavit to the one found in *United States v. Martin*, in which the affidavit's profile of child pornography collec-

31. *Id.*

32. *See id.*

33. *Id.* at 1071.

34. *See id.*

35. *Id.*

36. *Id.*

37. *Id.* at 1072; *see also* United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (reasoning that the magistrate judge could possibly conclude files were on a computer based on a collector profile).

38. *Gourde III*, 440 F.3d at 1068, 1072.

39. *Id.* at 1072.

tors supported a finding of probable cause.[40] Like Mariguchi's affidavit, the affidavit in *Martin* "contained an extensive background discussion of the modus operandi of those who use computers for collecting and distributing child pornography, including their reliance on e-groups, e-mail, bulletin boards, file transfers, and online storage."[41] The Ninth Circuit found the decisions of other circuit courts, helpful in their conclusions that the profile of child pornographers found in such affidavits "rose to the level of 'fair probability'" that the accused had received or downloaded illegal images, and established probable cause to issue a search warrant.[42]

Next, the court addressed Gourde's argument that probable cause was lacking because the FBI could have determined whether Gourde had downloaded the illegal images by searching for records of downloads from the seized computer of the "Lolitagurls.com" owner.[43] Without such tangible data, Gourde argued that "the profile data and other facts are insufficient to support a warrant."[44] The court rejected this argument, stating that such a ruling would transform the probable cause standard from "a 'fair probability' to a 'near certainty' that Gourde had received or possessed illegal images."[45] Instead, under the *Gates* analysis, the government was not required to show more information than needed to show a "fair probability" that Gourde received or possessed the images.[46] Furthermore, the Supreme Court's test did not require the affidavit to contain facts that made it "'more likely true than false' that Gourde possessed child pornography."[47]

Finally, the Ninth Circuit distinguished Gourde's case from that of *United States v. Weber*.[48] In that case, Weber was targeted for investigation after he failed to pick up a package addressed to him that contained two advertisements depicting child pornography.[49] Two years later, Weber or-

40. *Id.*; *see also* United States v. Martin, 426 F.3d 68, 75 (2d Cir. 2005).

41. *Gourde III*, 440 F.3d at 1072 (quoting *Martin*, 426 F.3d at 75).

42. *See Gourde III*, 440 F.3d at 1072; *see also* United States v. Riccardi, 405 F.3d 852, 860-61 (10th Cir. 2005) (holding that an affidavit containing a statement that "possessors of child pornography often obtain and retain images of child pornography on their computers," and other facts were "more than enough to support" probable cause); United States v. Chrobak, 289 F.3d 1043, 1046 (8th Cir. 2002) (holding that an affidavit's statement that based on "professional experience . . . child pornographers generally retain their pornography for extended periods," was enough to support probable cause).

43. *Gourde III*, 440 F.3d at 1072.

44. *Id.*

45. *Id.* at 1073.

46. *Id.*

47. *Id.* (citing Texas v. Brown, 460 U.S. 730, 742 (1983)).

48. *Id.* at 1073-74; United States v. Weber, 923 F.2d 1338 (9th Cir. 1991).

49. *Weber*, 923 F.2d at 1340.

dered, sight unseen, four pictures advertised as child pornography from a fictitious advertisement sent by the Customs Service.[50] The affidavit for the search warrant provided the details of these incidents and a general description of child pornography collectors but did not connect Weber with these profiles and did not address the two year lag between the first and second incidents.[51] The *Weber* court reversed the denial of the suppression motion because the issuance of a warrant under such facts would justify searching the house of any individual that tried to order child pornography, even if they did not receive it.[52] Furthermore, the court ruled the affidavit was deficient because it did not illustrate that Weber matched the profile of a pedophile or collector of child pornography.[53]

Gourde's case was factually different from *Weber*. Gourde had taken "continuous, affirmative steps to access a child pornography website," whereas *Weber* had involved a single transaction that occurred two years after an "initial, and unconsummated, foray into child pornography."[54] Also, the Moriguchi affidavit showed the link between Gourde and the child pornography collector profiles while the *Weber* affidavit had failed to do so.[55]

The Ninth Circuit, employing the *Gates* analysis of the Fourth Amendment, concluded that the search warrant was supported by probable cause.[56] Having reached this conclusion, the Ninth Circuit held that the district court did not err in denying Gourde's motion to suppress the images found on his computer.[57] The Court affirmed Gourde's conviction and remanded the case to a three-judge panel to rule on Gourde's request for a limited remand.[58]

IV. RHEINHARDT DISSENT

In his dissenting opinion, Judge Rheinhardt argued that the majority failed to consider the "totality of the circumstances" because it ignored the fact that "[a]t the time the government sought the warrant, it possessed direct evidence that established whether Gourde in fact had or had not downloaded illegal images."[59] Judge Rheinhardt labeled the government's failure to examine the website owner's computer for records of Gourde's activity as a

50. *Id.*

51. *Id.* at 1341.

52. *Id.* at 1344.

53. *Id.* at 1345.

54. *Gourde III*, 440 F.3d 1065, 1074 (9th Cir. 2006); *Weber*, 923 F.2d at 1340.

55. *Gourde III*, 440 F.3d at 1074; *Weber*, 923 F.2d at 1341.

56. *Gourde III*, 440 F.3d at 1071.

57. *Id.* at 1074.

58. *Id.*

59. *Id.* at 1074-75 (Rheinhardt, J., dissenting).

"conscious avoidance."[60] He argued that given these circumstances, Gourde had a valid *Franks* claim because "material omissions from the affidavit led the magistrate to issue a warrant for which there was no probable cause."[61] If the magistrate had known that the government had made such an omission, Judge Rheinhardt argued, he would probably not have issued the warrant.[62] Judge Rheinhardt argued that because the majority ignored the fact that the FBI admitted that it possessed evidence that would have determined whether Gourde had received child pornography and failed to provide this evidence, the majority did not properly consider "the totality of the circumstances" and erred in holding that government established probable cause.[63]

V. KLEINFELD DISSENT

Judge Kleinfeld also dissented from the majority. He disagreed with the assumption that an individual "who subscribes to an Internet site with both illegal and legal material must collect illegal material from the site."[64] Judge Kleinfeld argued that the court failed to consider that Gourde might have subscribed solely to look at the legal images.[65] According to Judge Kleinfeld, there were several indications suggesting that individuals would subscribe to the site to access the legal information.[66]

Next, Judge Kleinfeld noted the distinction between viewing child pornography and possessing child pornography. The applicable federal statutes punish an individual who "knowingly transports or ships . . . receives . . . or reproduces" child pornography; however, the statutes do not list "viewing" as a criminal activity.[67] Judge Kleinfeld noted that although "precedent does not settle the question, it does not square with common sense to treat looking as knowingly receiving."[68] Additionally, information in the browser's cache is not "received," as "the cache is an area of memory and disk space availa-

60. *Id.* at 1075.

61. *Id.* at 1075 n.2; *see* Franks v. Delaware, 438 U.S. 154, 156 (1978) (holding that if a defendant can establish perjury or reckless disregard by a "preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probably 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.")

62. *Gourde III*, 440 F.3d at 1076 (Rheinhardt, J., dissenting).

63. *Id.* at 1077.

64. *Id.* at 1084 (Kleinfeld, J., dissenting).

65. *Id.* at 1078.

66. *Id.* at 1079. These include the language, "This site is in full compliance with United States Code Title 18 Part I Chapter 110 Section 2256," and that much of the material on the site was legal pornography. *Id.*

67. *Id.* at 1079-1081; *see* 18 U.S.C. §§ 2252, 2252A (2000).

68. *Gourde III*, 440 F.3d at 1081 (Kleinfeld, J., dissenting).

ble to the browser software, not the computer user."[69] The browser software displays the web page from the cache "to save download time and web traffic," if "the computer accesses the same page . . . before the cache is overwritten."[70] However, the user cannot view the picture offline unless the user has downloaded the picture and saved as a JPEG or a PDF.[71] "Receiving" also implies possession, which "requires dominion and control."[72] Since a user does not have dominion and control of an image while it is in the cache, viewing a webpage is not analogous to possession.[73]

Finally, Judge Kleinfeld stated that the "totality of the circumstances" includes a consideration of "the legal environment in which the individual lives."[74] Individuals might participate in many prohibited activities were it not for the legal penalties that result.[75] Therefore, in light of the legal risks attached to the download of child pornography, Judge Kleinfeld argued it would take more than inferences to establish probable cause.[76]

VI. Implications of the Court's Holding

The Ninth Circuit's holding in *Gourde* greatly expands the "fair probability" standards in determining probable cause. This holding suggests that probable cause to search and seize an individual's computer can be established by the fact that (1) a website or data storage unit contained illegal material,[77] (2) an individual took affirmative action that would give them access to this material,[78] and (3) these actions match a profile of individuals that commit the crime.[79] These parameters severely endanger everyone's privacy in the realm of technology.

First, the holding does not differentiate between a "mixed website" that contains legal and illegal images and one that contains only illegal images – it is enough that the website possessed some illegal material. The court states that the "disclaimer" on the website was "mere window dressing that absolves the owners or users of nothing."[80] Internet users, therefore, cannot rely on the statements made on the website. The court is only concerned

69. *Id.* at 1082.

70. *Id.*

71. *Id.*

72. *Id.*

73. *See id.*

74. *Id.* at 1083.

75. *Id.*

76. *Id.* at 1084.

77. *See id.* at 1070 (majority opinion).

78. *See id.* at 1070-71.

79. *See id.* at 1072.

80. *Id.* at 1070.

with the existence of illegal material, despite the fact that the site has also has accessible permissible material. Therefore, it is possible that a user may access illegal information under the belief that they are accessing acceptable material. This analysis poses a problem if extended to the realm of servers and other data storage units. For example, a shared server may be used by several users. Its purpose is to facilitate work projects by providing access to information for the several users. But if the server also contains images of child pornography, does this constitute enough to meet the first requirement? Extending the court's analysis, it would seem that such a server would meet the requirement.

Second, the court argues that an individual's affirmative action to access a website (in contrast to stumbling on the illegal content) manifests an "intention and desire" to obtain the information on the website.[81] For the court, the fact that Gourde paid for access to the images implied that he possessed these images. The court forms its basis on the notion that when Gourde accessed the website, the images would remain on the computer in the form of a "digital footprint."[82] Furthermore, the court appears to equate viewing an image with "receiving" and "possessing" the image. The court fails to address Judge Kleinfeld's arguments concerning the difference between "view" and "receive," and the notion of "possession," within the context of internet browsers.[83] Since an individual cannot view the image from the cache while he is offline until he has downloaded it in some form, he cannot have "dominion and control" over the image while he views it on his web browser.[84] Additionally, the court simply ignores the possibility that Gourde may have subscribed to the site to view the legal images only. Under the court's analysis, a user "possesses" any information that he views while on the Internet. Therefore, when one accesses the McDonald's website, the viewer "possesses" the images of Ronald McDonald. This hardly fits the common conception of possession, yet the court equates any affirmative action to access a website as a desire to possess information and possession itself.

Third, the court holds that if the activities of an individual are similar to those matching the profile of a child pornography collector, this establishes grounds for probable cause.[85] The affidavit in *Gourde* stated that collectors of child pornography act like "pack rats," that they use the Internet to seek out like-minded individuals, trade and obtain illegal images, and store these images for a long period of time.[86] Since Gourde had accessed a website that

81. *Id.*

82. *Id.* at 1071.

83. *See id.* at 1081-82 (Kleinfeld, J., dissenting).

84. *See id.* at 1082.

85. *See id.* at 1072 (majority opinion).

86. *Id.*

contained child pornography, the court determines that there is a "fair probability" that he was a child pornography collector and would have these images on his computer. Here, the court seems to imply that a general resemblance to a profile is a "fair probability" that the subject meets that profile. Even if the government possesses evidence that could establish whether or not the subject actually is a member of the violating class (in this case, the computer of the website's owner), the government can use circumstantial evidence from a profile to stack inference upon inference to establish probable cause.

This holding has dangerous implications regarding technological privacy in today's society. For example, X, unbeknownst to the rest of his friends, has a large collection of child pornography on his computer. In order to find more opportunities to add to his collection, X joins an internet social network such as MySpace to find other collectors of child pornography. X uses MySpace to share and receive illegal images. On his MySpace profile, X not only displays photo albums of his trips around the world and surveys about his favorite movies, but also includes a cleverly disguised link for ordering pizza to access his pornography collection. But X also uses MySpace to stay in contact with Y, his old roommate from college and proud new father. Y has no interest in child pornography, nor does he know that X collects child pornography. Y's primary reasons for accessing X's MySpace page are to reminisce with his old friend and see pictures of X's travels around the world. The FBI targets X as a collector of child pornography, seizes his computer, and finds the collection of illegal images. While searching the computer, the FBI notices that Y is a part of X's network of friends on MySpace. The government seeks to obtain a search warrant and seize Y's computer. It bases its request on an affidavit that because Y was a friend of X on MySpace, and X had a massive collection of child pornography on his computer, Y's computer must also contain child pornography

According to the Ninth Circuit's holding in *Gourde*, this would be enough to search Y's computer because all three elements are met. Although X's MySpace profile contained legal images and information that were of interest to Y, the fact that there was a link, albeit a deceitful one, to access illegal images satisfies the first element. Second, by joining X's network of friends and viewing X's MySpace profile, Y took affirmative action to access a website that contained illegal images. And finally, Y's use of MySpace fits the profile of child pornography collectors because he was using computer resources to find like-minded individuals and to view information in relative privacy.

This example shows how extensively the *Gourde* decision might affect computer users. If the government seizes the computer of a child pornographer, the government can assert "fair probability" to seize the computers of anyone in that user's internet social networks, instant messenger list or e-mail address book. The *Gourde* decision may lead to a serious infringement of the privacy rights of computer users.

VII. CONCLUSION

Near the end of the *Gourde* opinion, the Ninth Circuit commented, "we are acutely aware that the digital universe poses particular challenges with respect to the Fourth Amendment."[87] Yet this decision does not seem to protect privacy interests, a main concern of the Fourth Amendment. Courts should not "grow lax in their duty to protect our right to privacy and . . . remain vigilant against efforts to weaken our Fourth Amendment protections."[88] Instead, this decision infringes upon people's right to privacy to a greater extent. Computers have become an integral part of our lives. We use them for work, for school and for pleasure. Our computers contain a wealth of personal information: term papers, appellate briefs, financial and medical records, and correspondence from loved ones. Some of our most private and intimate thoughts are stored within the hard drives of these machines. This decision, however, provides the government with a broad justification to seize our computers and reveal the personal information they contain. The *Gourde* decision effectively curtails the right of privacy in a key area of our increasingly technological society.

87. *Id.* at 1074.

88. *Id.* (Reinhardt, J., dissenting). As well, it should be noted that the majority opinion uses the same cautionary words. *Id.*