FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

TODD M. CHISM, individually and as husband and wife; NICOLE C. CHISM, individually and as wife and husband, *Plaintiffs-Appellants,* v. WASHINGTON STATE; WASHINGTON STATE PATROL; RACHEL GARDNER, individually; JOHN SAGER, individually, *Defendants-Appellees.*	No. 10-35085 D.C. No. 2:09-cv-00025-LRS OPINION

Appeal from the United States District Court
for the Eastern District of Washington
Lonny R. Suko, Chief District Judge, Presiding

Argued and Submitted
February 11, 2011—Seattle, Washington

Filed August 25, 2011

Before: Betty B. Fletcher, Richard A. Paez, and
Sandra S. Ikuta, Circuit Judges.

Opinion by Judge Paez;
Dissent by Judge Ikuta

COUNSEL

Robert A. Dunn and Susan C. Nelson, Dunn & Black, P.S., Spokane, Washington, for plaintiff-appellants Todd M. Chism and Nicole C. Chism.

Robert M. McKenna, Attorney General, and Catherine Hendricks, Senior Counsel, Seattle, Washington, for defendants-appellees Rachel E. Gardner and John Sager.

OPINION

PAEZ, Circuit Judge:

This civil rights action under 42 U.S.C. § 1983 arises from an internet child pornography investigation by Washington State Police (WSP) Officers Rachel Gardner and John Sager ("the officers"). As a result of information the officers acquired, Todd Chism became the focus of their investigation. Gardner prepared an affidavit in support of a search warrant application, which Sager reviewed. On the basis of that affidavit, a magistrate judge issued a broad search warrant to search Todd Chism's home and business office. Relying on the same information contained in Gardner's affidavit, Deputy Prosecuting Attorney Christian Peters obtained from the same magistrate judge a warrant to arrest Todd for violating Washington's child pornography laws.[1] A few days later, several WSP officers executed the search and arrest warrants.[2] A WSP detective eventually conducted forensic examinations of the Chisms' home computer and computers from the Spokane Fire Department, where Todd Chism worked as a firefighter. The investigation did not reveal any evidence of child pornography, and charges were never filed against Todd Chism.

[1]Specifically, the arrest warrant stated that probable cause existed to support the arrest and detention of Todd for violations of Revised Code of Washington §§ 9.68A.060 and 9.68A.070. Section 9.68A.060 prohibits "sending or bringing into the state depictions of a minor engaged in sexually explicit conduct." Section 9.68A.070 prohibits "possessi[ng] depictions of a minor engaged in sexually explicit conduct."

[2]The police report detailing the investigation seems to indicate that Sager was present for the search. It is unclear from the police report whether Gardner was present.

Several months later, Todd and his wife, Nicole Chism, filed this § 1983 action against the State of Washington, the WSP, Detective Gardner, and Sergeant Sager, alleging—among other things not relevant to this appeal—that the officers violated their Fourth and Fourteenth Amendment rights by securing the search and arrest warrants with an affidavit that deliberately or recklessly contained material omissions and false statements.[3] The Chisms and the officers filed cross motions for summary judgment on the issue of qualified immunity as to the constitutional claim. The district court granted the officers' motion, concluding that the officers' conduct did not violate a clearly established constitutional right of which a reasonable officer would have known. The Chisms timely appealed.

We reverse the district court's judgment and remand this case for trial. Viewing the evidence in the light most favorable to the Chisms, we conclude that the Chisms have made a substantial showing of the officers' deliberate falsehood or reckless disregard for the truth and have established that, but for the dishonesty, the searches and arrest would not have occurred. We also conclude that the officers are not entitled to qualified immunity because the Chisms' right to not be searched and arrested as a result of judicial deception was clearly established at the time Gardner prepared and submitted her affidavit.

I. BACKGROUND

On July 3, 2007, Washington's Missing and Exploited Children Task Force (MECTF) received a tip from the National Center for Missing and Exploited Children (NCMEC). The tip advised MECTF that roughly one week

[3]In addition to their constitutional claim, the Chisms' First Amended Complaint alleges nine other causes of action, most of which are tort claims relating to events that occurred after the search and arrest warrants were executed.

earlier, the web-hosting company Yahoo! had archived images of child pornography that were contained on the website *http://foelonipwin-cmezixecvom.us/* (the "foel website"). The tip listed Yahoo! user account *qek9pj8z9ec@yahoo.com* (the "first user account") as the "suspect." The tip stated that Internet Protocol (IP) address 68.113.11.49[4] was used to open the first user account on May 11, 2007. The tip did not provide the time or date that the child pornographic images were uploaded to the foel website, nor did it provide the IP address from which the child pornographic images were uploaded. Detective Gardner was assigned to investigate this tip.

On July 17, 2007, MECTF received another tip from NCMEC. Similar to the first tip, the July 17 tip indicated that two weeks earlier, Yahoo! archived images of child pornography that were contained on the website *http://qemtudawyownufiseip.com* (the "qem website"). The tip listed Yahoo! user account *qaagwcyI9ab@yahoo.com* (the "second user account") as the "suspect." The tip stated that IP address 67.160.71.115 was used to open the second user account on June 19, 2007. The tip did not provide the time or date that the child pornographic images were uploaded, nor did it provide the IP address from which the child pornographic images were uploaded. WSP Detective Vic Mauro was assigned to investigate this tip.

The detectives began their investigations by obtaining warrants to search Yahoo! records associated with the first and second user accounts.[5] In agreement with the first NCMEC tip, the Yahoo! records indicated that the foel website was

[4]As we have explained, "[e]very computer or server connected to the Internet has a unique IP address." *United States v. Forrester*, 512 F.3d 500, 510 n.5 (9th Cir. 2008).

[5]The record indicates that Gardner and Mauro independently obtained warrants to search Yahoo! records associated with the NCMEC tips because at that point in the investigation the detectives had no reason to believe the tips were connected.

created on May 11, 2007. The information for the first user account listed the name "Mr. Nicole Chism" with birthday May 20, 1966. The information indicated that "Mr. Nicole Chism" lived in Chile and used zip code "ucc16." The Yahoo! records also showed that the first user logged in to the account on June 18, 2007 from IP address 69.147.83.181, a different IP address than the one used to create the foel website. The billing information associated with the first user account listed Nicole Chism's name and contained the Chisms' correct residential address, phone number, and credit card number, which ended in 6907. Finally, the Yahoo! records showed that two months of "domain service" for the foel website had been paid with the Chisms' credit card.[6] The Chisms' credit card statements confirm that they were twice charged a monthly fee for domain service for the foel website.

The information that Yahoo! provided about the second user account was similar in character. In agreement with the second NCMEC tip, the Yahoo! records indicated that the qem website was created on June 19, 2007. The information for the second user account listed the name "Mr. Nicole Chism" with a birthday of March 11, 1977; indicated that "Mr. Nicole Chism" was from Bolivia; and used zip code "nf897." The Yahoo! records also showed that the second user logged in twice since opening the account. On July 3, 2007, the second user logged in twice: once from IP address 69.147.83.181 (the IP address from which the first user logged in on June 18, 2007), and once from a different IP address. Yahoo! did not provide any billing information for the second user account, but the Chisms' credit card statements showed that Yahoo! charged them one hosting fee for the qem website on June 22, 2007.

[6]The "domain service" fee is a fee that Yahoo! charges to host, or, provide server space and internet connection, for an individual website. We use the terms "domain service fee" and "hosting fee" interchangeably throughout.

Detectives Gardner and Mauro also independently obtained warrants to trace the IP addresses used to create the two user accounts and websites. Detective Gardner learned that the IP address used to open the first user account and to create the foel website was traced to Cheryl Corn of Walla Walla, Washington. The IP address used to open the second user account and to create the qem website was traced to Vitina Pleasant of Federal Way, Washington. It appears that neither Gardner nor Mauro traced IP address 69.147.83.181—the IP address from which the first user logged in on June 18, 2007 and the second user logged in on July 3, 2007.

A few months later, Mauro's assignment was transferred to WSP Detective Shelby Wilcox. After reviewing the information from Yahoo!, Gardner and Wilcox noticed that both user accounts used the name "Mr. Nicole Chism" and both websites had at some point been accessed from the IP address 69.147.83.181. Gardner and Wilcox concluded that the tips might be connected, and Gardner took over the investigation of both tips. Gardner decided to investigate the Chism lead, largely because Nicole's name was common to both tips.

Gardner first determined that the Chisms' 6907 card was a Bank of America Visa credit card. Gardner contacted Bank of America in September 2007 and learned from a Bank of America employee that the Chisms had reported a lost credit card in 2006. The 6907 card was a replacement for the lost card. The Bank of America employee, however, informed Gardner that no fraudulent activity had been reported on the 6907 card.[7] Gardner eventually obtained credit card statements for the 6907 card and confirmed that the Chisms had

[7]This information was, in fact, false. The Chisms reported fraudulent activity on their 6907 card in August 2007, roughly one month after Gardner received the NCMEC tips and roughly one month before Gardner spoke to Bank of America. Because the officers were not aware of this reported fraud at the time Gardner drafted her affidavit, we place no significance on the omission of this relevant information from the affidavit.

paid two charges for the foel website and one charge for the qem website. On the basis of this information, Gardner concluded that there was probable cause to believe that Todd Chism had committed a crime.

In January 2008, Gardner submitted a search warrant application and affidavit to a magistrate judge and obtained a warrant to search the Chisms' home in Nine Mile Falls, Washington, and Todd Chism's workplace in Spokane, Washington. Sager reviewed the affidavit and agreed that probable cause existed. On the same day, Deputy Prosecuting Attorney Christian Peters obtained a warrant to arrest Todd for "[s]ending, bringing into the state depictions of minor engaged in sexually explicit conduct and [p]ossession of depictions of [m]inor engaged in sexually explicit conduct." The warrants were executed five days later. WSP officers arrested, detained, and interrogated Todd; they scoured the Chisms' home; and they seized the Chisms' computers. No child pornography was found, and criminal charges were never filed against Todd.

The Chisms sued the State of Washington, the WSP, Detective Gardner, and Sergeant Sager under 42 U.S.C. § 1983, alleging violations of their constitutional rights. Both the Chisms and the officers moved for summary judgment on the issue of qualified immunity, and the district court granted the officers' motion and denied the Chisms' motion. The district court then declined to exercise supplemental jurisdiction over the Chisms' state law claims, pursuant to 28 U.S.C. § 1367(c)(3), and dismissed them. The Chisms appeal the district court's grant of summary judgment.

II. ANALYSIS

[1] We review de novo a grant of summary judgment on the ground of qualified immunity, and "must determine, viewing the evidence in the light most favorable to the nonmoving party, whether there are any genuine issues of material fact

and whether the district court correctly applied the relevant substantive law." *Prison Legal News v. Lehman*, 397 F.3d 692, 698 (9th Cir. 2005) The officers are entitled to qualified immunity unless: (1) the Chisms have "ma[de] out a violation of a constitutional right," and (2) "the right at issue was 'clearly established' at the time of [the officers'] alleged misconduct." *Pearson v. Callahan*, 555 U.S. 223, 232 (2009) (citing *Saucier v. Katz*, 533 U.S. 194, 201 (2001)); *Bull v. City and Cnty. of San Francisco*, 595 F.3d 964, 971 (9th Cir. 2010) (en banc). We may consider the two prongs of the qualified immunity analysis in any order. *Pearson*, 555 U.S. at 236. We begin with the first prong.

A. Constitutional Violation

[2] The Chisms argue that the officers violated their Fourth Amendment rights through judicial deception.[8] For the Chisms' judicial deception claim to survive summary judgment, the Chisms "must 1) make a substantial showing of [the officers'] deliberate falsehood or reckless disregard for the truth and 2) establish that, but for the dishonesty, the [searches and arrest] would not have occurred." *Liston v. Cnty. of Riverside*, 120 F.3d 965, 973 (9th Cir. 1997) (citing *Hervey v. Estes*, 65 F.3d 784, 788-89 (9th Cir. 1995)) (internal quotation marks omitted).[9]

[8]We disagree with the Dissent's brief suggestion that the Chisms waived the opportunity to argue that Gardner's affidavit contained false statements. The Chisms' failure to precisely articulate each false statement and omission to support their judicial deception claim does not undermine our ability to consider all of the false statements and omissions contained in Gardner's affidavit. The Supreme Court has explained that it is *claims* —not arguments—that are waived by failure to present an issue to the court below. *See Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374 (1991); *accord United States v. Guzman-Padilla*, 573 F.3d 865, 877 (9th Cir. 2009); *United States v. Pallares-Galan*, 359 F.3d 1088, 1095 (9th Cir. 2004).

[9]A judicial deception claim is different from a garden-variety claim that a warrant lacked probable cause on its face. We have explained that a

[3] We first observe that Gardner's affidavit contained several false statements and omissions. The first false statement contained in Gardner's affidavit was her assertion that, "[b]ased on the information received from NCMEC about the images downloaded by Todd M. Chism, it is likely to believe he was using internet service at his residence and/or his business office." Gardner's allusion to "images downloaded by Todd M. Chism" is inaccurate. When Gardner drafted the affidavit, she possessed no information that Todd had ever accessed any child pornographic images, let alone the particular images that were uploaded to the qem and foel websites. Nor did Gardner have any evidence that the images were ever downloaded by anyone. As far as Gardner knew, the only evidence linking Todd to the websites was the fact that the credit card he shared with Nicole was used to pay the hosting fees for the sites. Thus, Gardner's assertion that Todd downloaded images of child pornography was not a truthful representation of the evidence she had gathered.

[4] The second false statement contained in Gardner's affidavit was her assertion that the Chisms' credit card was "used to purchase the images of child pornography from the website." This statement was false because the Chisms' credit card was not used to buy images of child pornography. Rather, the Chisms' card was used to pay hosting fees for the sites to which illegal images were uploaded at some unknown time, date, and location. Gardner's statement that the Chisms'

---

plaintiff bringing a judicial deception claim "argues that [an officer] misled the magistrate judge when applying for the warrant, and had the magistrate considered all of the facts that the magistrate would not have found probable cause." *Smith v. Almada*, 640 F.3d 931, 937 (9th Cir. 2011). A judicial deception claim can be contrasted with a garden-variety claim that a warrant lacked probable cause on its face, in which "the arresting officer enjoys qualified immunity unless the warrant application is so lacking in indicia of probable cause as to render official belief in its existing unreasonable." *Id.* (quoting *Malley v. Briggs*, 475 U.S. 335, 344-45 (1986)) (internal quotation marks omitted).

card purchased child pornographic images was therefore patently false.

[5] Gardner's affidavit also contained several serious omissions. First, Gardner omitted her discovery that the IP addresses that were used to open the offending Yahoo! user accounts and websites were traced to people other than the Chisms. Second, Gardner omitted the fact that a third IP address—69.147.83.18—was used to log in to both the first and second user accounts on June 18, 2007, and that this IP address was never traced. Third, Gardner omitted the fact that Nicole shared the 6907 credit card account with Todd, even though Nicole's name—not Todd's—was associated with the two user accounts. Fourth, Gardner did not report that the user accounts contained nonsensical identifying information.[10]

Having determined that Gardner's affidavit contained false statements and omissions, we next consider whether the Chisms have made a substantial showing of the officers' intentional or reckless disregard for the truth; and, if so, whether their false statements and omissions were material to the probable cause determinations. *Liston*, 120 F.3d at 973.

1. *Intentional or Reckless Deception*

[6] As a first element of their judicial deception claim, the Chisms must demonstrate that the officers acted deliberately or with reckless disregard for the truth in preparing the affidavit. *Id.* at 973. Because the Chisms appeal from a grant of summary judgment, they need only make a "substantial showing" of the officers' deliberate or reckless false statements and omissions. *Id.* "Clear proof of deliberat[ion] or reckless[ness] is not required" at the summary judgment stage. *United States*

[10]As described above, the first user account was registered with the name "Mr. Nicole Chism," the country Chile, and the zip code ucc16. The second user account was registered with the name "Mr. Nicole Chism," the country Bolivia, and the zip code nf897.

v. Stanert, 762 F.2d 775, 781 (9th Cir.), *amended by* 769 F.2d 1410 (9th Cir. 1985). If the Chisms make such a substantial showing, then "the question of intent or recklessness is a factual determination" that must be made by the trier of fact. *Liston*, 120 F.3d at 974 (internal quotation marks omitted). Viewing the evidence in the light most favorable to the Chisms, we conclude that the Chisms have made a substantial showing that the officers' deception was intentional or reckless. The most commonsense evidence that the officers acted with at least a reckless disregard for the truth is that the omissions and false statements contained in the affidavit were all facts that were within Gardner's personal knowledge. For example, Gardner's false reference to "images downloaded by Todd Chism" was a statement that Gardner *knew to be false* when she drafted her affidavit.

[7] The declaration Gardner filed in the district court similarly demonstrates that she *knew* that the IP addresses used to register the user accounts and websites were traced to other people, and that she *knew* that the identifying information for the Yahoo! accounts was nonsensical. The fact that the affidavit did not report important factual information that was within the officers' knowledge at the time Gardner prepared her affidavit would allow a reasonable factfinder to conclude that the officers acted with at least a reckless disregard for the truth. *See Butler v. Elle*, 281 F.3d 1014, 1025-26 (9th Cir. 2002) (per curiam); *Stanert*, 762 F.2d at 781; *see also Liston*, 120 F.3d at 975 ("Given the importance of the [omitted information] to the probable cause analysis . . . a jury could reasonably conclude that [the affiant's] failure to mention [that information] in his affidavit amounted to at least reckless disregard for the truth.").

[8] A reasonable factfinder could also find that the officers acted recklessly or intentionally because the false statements and omissions contained in the affidavit all *bolster* the case for probable cause, which suggests that the mistakes were not the product of mere negligence. It is conspicuous that, cumu-

latively, the omissions purged the affidavit of any reference to the possibility that someone other than Todd Chism was responsible for the offending websites. Corn and Pleasant were the people to whom the offending IP addresses were traced, yet this information was omitted from the affidavit. Nicole Chism's credit card information was used to pay the hosting fees, yet the fact that Nicole was an authorized user of the credit card was omitted from the affidavit. All of the information in each Yahoo! profile was nonsensical, yet this information was omitted from the affidavit. In short, the net effect of Gardner's omissions was to obscure the prospect that someone other than Todd Chism might have registered the websites and uploaded images of child pornography. We have no difficulty deciding that a reasonable factfinder, viewing the evidence in the light most favorable to the Chisms, could conclude that Gardner's omissions reflected an affiant "reporting less than the total story . . . [to] manipulate the inferences a magistrate will draw." *Stanert*, 762 F.2d at 781. Accordingly, we hold that the Chisms made a substantial showing of the officers' reckless or intentional disregard for the truth.

2. *Materiality of the False Statements and Omissions*

[9] Our inquiry does not end with the Chisms' substantial showing that the affidavit contained reckless or deliberate false statements and omissions. To make out their judicial deception claim, the Chisms must also establish that the false statements and omissions were material to the magistrate judge's probable cause determination. Our inquiry into whether the false statements and omissions were material is a purely legal question, which we analyze de novo. *See Butler*, 281 F.3d at 1024. The false statements and omissions contained in Gardner's affidavit were material if "the affidavit, once corrected and supplemented," would not have provided a magistrate judge with a substantial basis for finding probable cause. *Stanert*, 762 F.2d at 782. We conclude that a corrected version of Gardner's affidavit would not have pro-

vided the magistrate with a substantial basis for finding probable cause.

i. Materiality as to the Search Warrants

[10] While there is no "numerically precise degree of certainty corresponding to probable cause, . . . it is clear that only the probability, and not a prima facie showing, of criminal activity is the standard of probable cause." *Illinois v. Gates*, 462 U.S. 213, 235 (1983) (citing *Spinelli v. United States*, 393 U.S. 410, 419 (1969)) (internal quotation marks omitted). The Supreme Court has declined to articulate a "neat set of legal rules" for evaluating probable cause, *id.* at 232, and instead has instructed magistrate judges to determine probable cause by considering the "totality-of-the-circumstances," *id.* at 230. In issuing a search warrant, the magistrate judge simply must determine whether there is a "fair probability" that evidence of a crime will be found. *Id.* at 238, 246.

[11] Our probable cause analysis is guided by *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc), a recent case involving the search of a criminal defendant's computer for images of child pornography. In *Gourde*, we held that three key pieces of evidence, considered together, were sufficient to establish probable cause to believe Gourde's computer contained images of child pornography: (1) that the accessed website "was a child pornography site whose primary content was in the form of images"; (2) that as a subscriber to the website, "Gourde had access and wanted access to these illegal images"; and (3) that "[h]aving paid for multi-month access to a child pornography site," and owing to the "long memory of computers," Gourde's computer was likely to contain evidence of a crime. *Id.* at 1070-71. In other words, we looked for evidence in the affidavit: (1) that a crime was committed; (2) that it was Gourde who committed the crime; and (3) that evidence of the crime would be found in the place to be searched. In light of this "triad of solid facts," we concluded that "the reasonable inference that

Gourde had received or downloaded [child pornographic] images easily meets the 'fair probability' test." *Id.* at 1071. We use this framework to determine whether Gardner's affidavit would have supported probable cause if it had presented a truthful description of the evidence she collected during her investigation of Todd Chism.

[12] Like the website at issue in *Gourde*, the parties do not dispute that the qem and foel websites here contained images of child pornography. Therefore, Gardner's affidavit meets the first prong of the *Gourde* inquiry: it presents evidence that a crime was committed. We also assume without deciding that Gardner's affidavit satisfied the third prong of the *Gourde* framework by presenting evidence that a computer used to upload child pornographic images would contain evidence of a crime.[11] The remaining prong of the *Gourde* inquiry requires us to consider whether a truthful version of Gardner's affidavit would have provided a "fair probability" that Todd Chism committed a crime.

[13] A truthful version of Gardner's affidavit would have indicated that the sole evidence connecting Todd Chism to the child pornographic images was the fact that the credit card he shared with Nicole was charged three times for hosting the websites that contained child pornographic images. This connection is a far cry from the facts presented in the affidavit, which stated that Todd "downloaded" and "purchase[d]" child pornography.[12] A supplemented version of Gardner's affidavit

[11]Specifically, Gardner's affidavit stated that "in [her] experiences and from [her] conversations with computer forensic examiners, computer evidence can remain stored on computers for extended periods of time," and can be recovered from a computer even if it is deleted by the user." The affidavit also stated that "[p]ersons involved in sending or receiving child pornography tend to retain it for long periods of time." The Chisms do not challenge these assertions.

[12]The Dissent downplays the significance of the affidavit's misstatements. We agree with the Dissent that the affidavit's use of the word

also would have informed the magistrate judge that the IP addresses used to register the websites were traced to people other than the Chisms, and that the Yahoo! user accounts associated with the websites contained nonsensical identifying information. In considering all of the information available to the officers, we do not think it sufficient to establish a fair probability that evidence of a crime would be found at the Chisms' home or Todd Chism's office.

[14] We find it particularly significant that the IP addresses from which the qem and foel websites were created were traced to internet subscribers hundreds of miles away from the Chisms' home in Nine Mile Falls, Washington. We have explained that a computer that is connected to the internet can be *uniquely* identified by its IP number, much like a land-line phone can be uniquely identified by its phone number. *See Forrester*, 512 F.3d at 510 n.5. Moreover, we have repeatedly recognized the utility of using IP address information to investigate child pornography offenders. *See United States v. Craighead*, 539 F.3d 1073, 1080-81 (9th Cir. 2008) (holding that probable cause existed where the IP address from which child pornographic images were shared was traced to the defendant)*; United States v. Hay*, 231 F.3d 630, 634-35 (9th Cir. 2000) (holding that an affidavit demonstrated probable cause where the agent carefully detailed how the IP address associated with the child pornographic images was connected to the defendant). Our sister circuits take the same approach.

"downloaded" instead of "uploaded" is not material because evidence that Todd Chism had uploaded images of child pornography—if such evidence had existed—would have been just as damaging as evidence that he downloaded child pornography. *See* Revised Code of Washington 9.68A.050-9.68A.070 (prohibiting possessing, disseminating, and sending child pornography). The problem with the affidavit is *not* that it uses the word "downloaded" instead of "uploaded," but rather, that it improperly states that Todd Chism was the perpetrator. As we have explained, this error was significant because there was no evidence that Todd Chism had ever accessed either of the offending websites.

See, e.g., *United States v. Vosburgh*, 602 F.3d 512, 526-27 (3d Cir. 2010) ("[S]everal Courts of Appeals have held that evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address.") (footnote omitted); *United States v. Stults*, 575 F.3d 834, 843-44 (8th Cir. 2009); *United States v. Perrine*, 518 F.3d 1196, 1205-06 (10th Cir. 2008); *United States v. Perez*, 484 F.3d 735, 738-40 (5th Cir. 2007); *United States v. Wagers*, 452 F.3d 534, 539 (6th Cir. 2006)); *Hay*, 231 F.3d at 635-36; *see also United States v. Bynum*, 604 F.3d 161, 165 (4th Cir. 2010).

[15] Here, the IP address associated with child pornographic images led to locations different from the locations to be searched, and the affidavit did not establish a physical link between the illegal images and the locations to be searched.[13] Several inferences would have to be drawn in order to conclude that Todd violated Washington's laws against child pornography. First, one would have to infer that Todd had used his wife's name rather than his own to pay the hosting fees for the sites. One would also have to infer that Todd devised a way to access the foel and qem websites with a forged IP address. Finally, one would have to infer from the previous two inferences that Todd was the person who uploaded the child pornographic images from his computer to the websites at an unknown time, date, and location. This convoluted string of inferences reduces the possibility that child pornography

[13]We disagree with the Dissent that *Gourde* is factually indistinguishable from this case. In *Gourde*, we noted that the FBI was able to "link[ ] the email user—'gilbert95@yahoo.com,' a known subscriber to [a child pornographic website]—to Gourde and to his home address in Castle Rock, Washington." 440 F.3d at 1071. We did not specify in *Gourde* whether the FBI used IP address information to link the user information to Gourde, nor did any of the evidence in *Gourde* raise the specter of identity theft. In contrast to *Gourde*, several pieces of evidence in this case suggested that Todd Chism was not connected to the child pornographic images.

would be found at Todd Chism's home and office to far below a "fair probability." *See United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990) (explaining that "with each succeeding inference, the last reached is less and less likely to be true.").[14]

Our conclusion also finds support in the WSP's training materials, which explain:

> Much, if not all, of the cyber-evidence (the E-mail addresses and IP addresses used) will lead you to an innocent person. That's why simply identifying which account was used to commit a crime does not provide you with probable cause to get a search or arrest warrant for the name and address on that account. You'll need to do more investigating to determine if there is a link between the account holder (or other members of the household) with the criminal activity that was committed with that account.

The affidavit submitted by Marcus Lawson, the president of a computer forensic company that examined Todd Chism's computers similarly admonishes:

> [T]o have any success as an Internet criminal, regardless of whether one was a thief, a hacker or a child pornography collector, it would be incumbent to use other people's identities to do so. . . . It is primarily for this reason that relying only on informa-

[14]The Dissent argues that "the *lack* of a match between the IP addresses used for registration and the Chisms' IP address has no probative value." Dissent at 16339. We disagree. Where, unlike here, a person's IP address is used to upload or download child pornography, there is a direct link between that person's physical location and evidence of a crime. When this direct link is absent, at least one, if not several, additional inferences are necessary to conclude that evidence of a crime will be found at the location to be searched.

> tion provided by the user of a credit card that is associated with criminal activity is *inherently unreliable*.

(emphasis added).

[16] We are mindful that "[a] letter-perfect affidavit is not essential." *United States v. Esparza*, 546 F.2d 841, 844 (9th Cir. 1976). In this case, however, we do not believe that a reasonable magistrate judge would have issued the search warrant if she had been apprised of an accurate version of the evidence. We therefore hold that the affidavit's false statements and omissions were material to the probable cause determination for the search warrants.

ii. Materiality as to Todd Chism's Arrest

[17] Unlike the search warrants—which were supported by Gardner's affidavit—the warrant for Todd's arrest was supported by a Certification of Probable Cause (CPC) from Peters, a state prosecutor. In the CPC, Peters cited Gardner's investigation as the source of his information.

[18] Like Gardner's affidavit, Peters' CPC contained material false statements and omissions. For example, like Gardner's affidavit, Peters' CPC stated that the Chisms' card was used to "purchase the images of child pornography," which is a false statement. Also like Gardner's affidavit, Peters' CPC omitted critical information, including the fact that the IP addresses used to create the Yahoo! user accounts and websites were traced to Corn and Pleasant. Peters similarly withheld the fact that the two Yahoo! user accounts contained nonsensical identifying information for the Chisms, and that Nicole shared the 6907 credit card with Todd. These false statements and omissions were material as to Todd Chism's arrest for the reasons discussed above.

[19] That the CPC supporting probable cause was submitted by Peters—not Gardner—is inconsequential. In fact, the

officers do not dispute that they might be held responsible for damages stemming from Todd's arrest even though the warrant for this arrest was supported by Peters' CPC rather than Gardner's affidavit. Moreover, we have held that a "deliberate or reckless omission by a government official who is not the affiant can be the basis for a [suppression claim under *Franks v. Delaware*, 438 U.S. 154 (1978)]." *United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992). Because *Franks* suppression claims and judicial deception claims under § 1983 involve the same constitutional right, we do not see any reason to distinguish *DeLeon* from this case. *Hervey*, 65 F.3d at 789 ("The showing necessary to get to a jury in a section 1983 action is the same as the showing necessary to get an evidentiary hearing under *Franks*."). Therefore, we hold that the Chisms have made out a judicial deception claim for Todd's arrest.

B. Qualified Immunity

[20] Qualified immunity shields the officers from liability "insofar as their conduct d[id] not violate clearly established statutory or constitutional rights of which a reasonable person would have known." *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). Although there are genuine triable issues of fact as to the merits of the Chisms' judicial deception claim, our discussion in the previous section demonstrates that the Chisms have made an adequate showing that there was a constitutional violation. Therefore, we must consider whether the Chisms' constitutional rights were clearly established at the time that Gardner submitted her affidavit.

[21] In determining whether the Chisms' constitutional rights were clearly established at the time of the officers' conduct, we ask whether the contours of the Chisms' rights were so clear that "every 'reasonable official would have understood that what he is doing violates that right.' " *Ashcroft v. al-Kidd*, 131 S. Ct. 2074, 2083 (2011) (quoting *Anderson v. Creighton*, 483 U.S. 635, 640 (1987)). Although "[w]e do not

require a case directly on point, [ ] existing precedent must have placed the statutory or constitutional question beyond debate." *Id.*

[22] Our analysis of this prong is brief because we have already held that governmental employees are not entitled to qualified immunity on judicial deception claims. In *Branch v. Tunnell*, 937 F.2d 1382 (9th Cir. 1991) (overruled on other grounds by *Galbraith v. City and Cnty. of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002)), we explained that

> if an officer submitted an affidavit that contained statements he knew to be false or would have known were false had he not recklessly disregarded the truth and no accurate information sufficient to constitute probable cause attended the false statements, . . . he cannot be said to have acted in a reasonable manner, and the shield of qualified immunity is lost.

Id. at 1387 (quoting *Olson v. Tyler*, 771 F.2d 277, 281 (7th Cir. 1985)) (internal quotation marks omitted). We have consistently applied the rule that summary judgment on the ground of qualified immunity is not appropriate once a plaintiff has made out a judicial deception claim.[15] *See, e.g.*, *Liston*, 120 F.3d at 972; *Hervey*, 65 F.3d at 788. In light of *Branch*, *Liston*, and *Hervey*, we conclude that "every 'reasonable offi-

[15]In judicial deception cases, our qualified immunity analysis at the summary judgment stage is swallowed by the question of reckless or intentional disregard for the truth. *See Butler*, 281 F.3d at 1024 (noting that "our cases effectively intertwine the qualified immunity question (1) whether a reasonable officer should have known that he acted in violation of a plaintiff's constitutional rights with (2) the substantive recklessness or dishonesty question"). We have explained that this "merger" is sensible because "no reasonable officer could believe that it is constitutional to act dishonestly or recklessly with regard to the basis for probable cause in seeking a warrant. Accordingly, should a factfinder find against an official on this state-of-mind question, qualified immunity would not be available as a defense." *Id.*

cial would have understood' " that the Chisms had a constitutional right to not be searched and arrested as a result of judicial deception. *al-Kidd*, 131 S. Ct. at 2083. We therefore hold that the officers are not entitled to qualified immunity.

III. CONCLUSION

For the foregoing reasons, we reverse the district court's grant of summary judgment to the officers.

REVERSED AND REMANDED.

IKUTA, Circuit Judge, dissenting:

In *All the President's Men*, Deep Throat famously advised two investigative journalists that in order to find the truth, they had to "follow the money." In *United States v. Gourde*, we endorsed this maxim, holding that payment of subscription fees to a site on which child pornography is available was sufficient to support probable cause for a search warrant. 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc). Despite the fact that this case involved a direct connection between the Chisms' credit card and two websites populated with child pornography, the majority holds that the evidence was insufficient to support probable cause, and therefore the district court erred in granting summary judgment to the police on the basis of qualified immunity. In doing so, the majority tramples on controlling precedent and defies common sense. I respectfully dissent.

I

The Washington State Police received a hot "cybertip" about child pornography on two Yahoo!-hosted websites. Yahoo! lets users create their own websites (with unique domain names) and host their own content on those websites,

including populating the websites with images. Yahoo! may also provide users with domain-based email accounts.

The first tip directed the police to a website with the URL *http://foelonipwin-cmezixecvom.us* (referred to here as the "foel" website). According to the tip, 14 images of child pornography had been uploaded to this website. The tip identified the "screen user name" for the web site as "qek9pj8z9ec" and the email associated with this website as *"qek9pj8z9ec@yahoo.com"* (referred to here as the "qek" user name and email). Yahoo!'s subscriber information for the website identified the subscriber as "Nicole Chism," with the Chisms' address and phone number, and the qek email address. The user's log-in name was "qek," with the full name given as "Mr. Nicole Chism," and the country identified as "Chile." The Yahoo! Billing History showed that the Chisms' credit card had paid for two months of web hosting fees for the site.

The second tip identified a website with the URL *http://qemtudawyow-nufiseip.com* (referred to here as the "qem" website). According to the tip, 63 images of child pornography had been uploaded to this website. The tip identified the email associated with this website as *"qaagwcy19ab@yahoo.com"* and the user name as "qaagwcy19ab" (referred to here as the "qaag" email and user name). Yahoo! did not provide subscriber information, but according to Yahoo!, the user's full name was "Mr. Nicole Chism," the log-in name was "qaag," and the country was identified as "Bolivia." The Yahoo! Login Tracker showed that "qaag" had logged into the website three times, once from the same IP address used by "qek."

The police followed up with Bank of America, which had issued the credit card that paid for these child pornography sites. According to the bank, the Chisms had not reported any fraudulent activity on their card. Reviewing the card's billing records, the police confirmed that the Chisms' credit card was

used pay for the foel website for two months and the qem website for a month.

Based on this investigation, the police could reasonably conclude that a person using the name Chism, providing the Chisms' home address and phone number, and paying with the Chisms' credit card, had created two websites, populated them with child pornography, and logged on to the sites several times. Does this create a "fair probability," *Illinois v. Gates*, 462 U.S. 213, 246 (1983), that child pornography would be found on the Chisms' computer? Did the magistrate judge correctly answer the "commonsense, practical question" that there was probable cause to believe that evidence of child pornography was located at the Chisms' residence? *Id.* at 230. These questions answer themselves: it is reasonable to "follow the money" from the child pornography website, to the fees paying to host that website, to a credit card owned by the Chisms, to the address for the payee (which is the same address as the website's subscriber), and from there to the Chisms' computer. And if there was any doubt, *Gourde* requires us to hold that there was probable cause supporting the warrant, as explained below. Therefore, the district court did not err in rejecting the Chisms' claim that their Fourth Amendment rights were violated and granting summary judgment in favor of the police.

II

Our en banc decision in *United States v. Gourde* is directly on point and controls our probable cause analysis here.

In *Gourde*, the police investigated a website that featured child pornography (called "Lolitagurls.com") and obtained a membership list. 440 F.3d at 1067. The list included the name Micah Gourde, and provided Gourde's name, home address, date of birth, and email address. *Id.* at 1068. According to the membership list, Gourde's credit card had been used to pay a fee of $19.95 a month for unlimited access to the website

and its images for over two months, until the FBI shut down the site. *Id.* at 1067-68.

We concluded, based on the evidence that Gourde's credit card had been used to pay subscription fees to a site that contained child pornography, that there was a "fair probability" that "Gourde's computer contained evidence that he violated" federal child pornography laws. *Id.* at 1069.

First, we inferred that Gourde "had access and wanted access to [ ] illegal images." *Id.* at 1070. We based this inference on evidence that Gourde had been a paying member of a website containing images of child pornography. Because his credit card had been used to pay for access to the website, and Gourde could not have paid two months of subscription fees "by accident or by a mere click of a button," *id.*, we reasoned that Gourde had knowingly and willingly paid for unlimited access to illegal images, *see id.* at 1070-71.

Given this conclusion, we made the further inference that there was "near certainty that his computer would contain evidence of a crime had he received or downloaded images" in violation of federal law. *Id.* at 1071. As we explained, "[i]t 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." *Id.*

Based on this "triad of solid facts," namely that: (1) "the site had illegal images," (2) the inference that Gourde intended to have and wanted access to these images; and (3) our further inference that "these images were almost certainly retrievable from his computer if he had ever received or downloaded them," we determined that "the reasonable inference that Gourde had received or downloaded images easily meets the 'fair probability' test." *Id.* "Employing the principles of *Gates*-practicality, common sense, a fluid and non-

technical conception of probable cause, and deference to the magistrate's determination," we concluded that the search warrant was supported by probable cause. *Id.*

In reaching this conclusion, we rejected Gourde's argument that the police should have looked for evidence of Gourde's downloads in the computer hosting the child pornography website, and his claim that "absent such concrete evidence, the profile data and other facts are insufficient to support a warrant." *Id.* at 1072. We disagreed that the police had any obligation to conduct such additional investigation or obtain any additional evidence: *Gourde* asserted that the police did not need to turn a "fair probability" into a "near certainty." *Id.* at 1073.

Gourde is directly applicable and controls the outcome of this case. The same "triad of solid facts" found in *Gourde* are present here: (1) the foel and qem websites contained images of child pornography, (2) the Chisms' credit card paid to host both sites, raising the inference that the Chisms intended to have and wanted access to these images, and therefore (3) images of child pornography "were almost certainly retrievable from [the Chisms'] computer if [the Chisms] had ever received or downloaded them." *Id.* at 1071. Like the defendant in *Gourde*, the Chisms could not have paid two months of hosting fees for the sites "by accident or by a mere click of a button," *id.* at 1070, and the inference that the Chisms' computer contained child pornography was eminently reasonable given that they paid multi-month fees to host a child pornography website, *see id.* at 1071. Under *Gourde*, these two facts raise the additional inference that images of child pornography were retrievable from the Chisms' computer had they "ever received or downloaded them." *Id.* at 1071. Indeed, this additional inference is even stronger here than it was in *Gourde*, because there was evidence that the user names asso-

ciated with a "Mr. Nicole Chism" were used to log in to both the foel and qem websites.[1]

Under any reasonable reading, *Gourde* dictates that the link between the Chisms' credit card and the websites containing child pornography, coupled with the multi-month charges, the repeated log-ins, and the lack of any billing challenge from the Chisms, is necessarily sufficient to establish probable cause. Even viewing the record in the light most favorable to the Chisms, the police had probable cause to search the Chisms' residence irrespective of any alleged misrepresentations or omissions in the affidavits submitted to obtain the search and arrest warrants. The Chisms therefore suffered no Fourth Amendment violation, and their § 1983 claim for judicial deception must fail as a matter of law.

III

In supporting its contrary conclusion, the majority relies on both omissions and alleged false statements in the affidavit, Maj. Op. at 16320-21, but places the most weight on alleged misrepresentations that are clearly immaterial. Indeed, their immateriality is amply evidenced by the fact that the Chisms failed to even mention the alleged misrepresentations until this appeal. Before the district court, the Chisms alleged only that the affidavit contained material omissions. Now, for the

[1]The majority's attempt to distinguish *Gourde* is unavailing. *See* Maj. Op. at 16327 n.13. In *Gourde*, the FBI used subscription information provided by Lancelot Security to link membership in the Lolitagurls.com website to Gourde and his home address in Castle Rock, Washington. 440 F.3d at 1070-71. Here, the police used subscription information provided by Yahoo! and credit card information provided by Bank of America to link the user accounts for the foel and qem websites to the Chisms and their home address in Nine Mile Falls, Washington. The information is effectively identical. In addition, the majority's attempted distinction of *Gourde* on the ground that none of the evidence in that case raised "the specter of identity theft" is peculiar, given the majority's correct statement that here the police had no reason to know of any reported credit card fraud. Maj. Op. at 16317 n.7.

first time on appeal, the Chisms raise the claim that the affidavits contained recklessly made false statements. Even assuming the latter claim is appropriately before us, *cf. Whittaker Corp. v. Execuair Corp.*, 953 F.2d 510, 515 (9th Cir. 1992), it is baseless in any event.

To be clear, the Chisms have been able to dig up only two alleged false statements in the police officers' affidavit. First, the affidavit notes the credit card number used to pay for the foel website, and states: "This is the [credit] card the suspect used to purchase the images of child pornography from the website '[foel].' " Although the majority places much weight on the fact that the credit card "was not used to buy images of child pornography," Maj. Op. at 16320, this error in the affidavit is immaterial, given that the Chisms' credit card was used to buy the website itself, that is, to pay hosting fees for a website populated with child pornography. While the affidavit's misstatement may evince carelessness, or a lack of precision, it does not establish a deliberate or reckless disregard for truth.

Second, the affidavit states, "Based on the information received from NCMEC about the images downloaded by Todd M. Chism, it is likely to believe he was using internet services at his residence and/or business office." Again, the majority makes much of the fact that there was no evidence that Todd Chism had *downloaded* images of child pornography. But any error is again immaterial. The evidence establishes that someone controlling the foel website *uploaded* child pornography to the website, and uploading images of child pornography raises exactly the same inferences as downloading such images. Moreover, *Gourde* instructs that we can infer that a person who pays for access to images of child pornography has downloaded them. 440 F.3d at 1071. Again, the affidavit's use of the word "download" instead of "upload" cannot be the basis of a judicial deception claim.

The majority places less weight on the alleged omissions in the affidavit, and for good reason: they are either immaterial,

or not really omissions at all. First, the majority points to the affidavit's failure to state that the IP addresses used to register the foel and qem websites were traced to Cheryl Corn and Vitina Pleasant. Maj. Op. at 16317, 16321. This carries little weight, given that the credit card used to pay the hosting fees for the sites and the usernames used to log in to both sites were registered to the name "Chism." Moreover, given the existence of proxy software, which allows an unknown individual to log on to the internet under another person's IP address, the *lack* of a match between the IP addresses used for registration and the Chisms' IP address has no probative value. *See, e.g.*, *United States v. Vosburgh*, 602 F.3d 512, 527 n.14 (3d Cir. 2010) (recognizing that "proxy servers can be used to mask IP addresses"); *Tagged, Inc. v. Does 1 Through 10*, 2010 WL 370331, at *2 (N.D. Cal. Jan. 25, 2010) (finding IP address information unreliable where pattern of IP addresses indicated the use of a proxy server). In other words, while a match between an IP address associated with pornographic images and the IP address of a defendant's computer *increases* probable cause that the defendant is involved in a crime, as the majority argues, Maj. Op. at 16326-27, no case has relied on the reverse proposition (that the *lack* of a match between an IP address associated with such images and the IP address of the defendant's computer *reduces* probable cause of the defendant's involvement). Indeed, in this case, the FBI determined that proxy software had been installed on Cheryl Corn's computer, allowing an unknown individual to log onto the internet under her IP address. Thus the absence of information in the affidavit about the IP addresses used to register the foel and qem sites was immaterial.

Second, Agent Gardner's failure to disclose the fact that the police never traced the IP address that was used to log in to both the foel and qem websites, Maj. Op. at 16317, 16321, cannot be deemed an omission: as in *Gourde*, the police have no obligation to turn a "fair probability" into a "near certainty" by conducting such an additional investigation. 440 F.3d at 1071. As *Gourde* explained, "[a]n affidavit may support

probable cause even if the government fails to obtain potentially dispositive information," *id.* at 1073 n.5.[2]

Third, the majority's reliance on the omission of the information that Nicole and Todd Chism both used the credit card that paid the hosting fees, Maj. Op. at 16320-21, is baffling. Surely the failure to inform the magistrate judge that husbands and wives often use the same credit card cannot be deemed a material omission. At a minimum, this revelation would not have changed the "fair probability" that child pornography would be found at the Chisms' residence.

In fact, no weight can be placed on any of the alleged misrepresentations and omissions given the ample evidence to support probable cause, and thus they cannot be used to support a judicial deception claim. It is well established that "[o]missions or misstatements resulting from negligence or good faith mistakes will not invalidate an affidavit which on its face establishes probable cause." *United States v. Smith*, 588 F.2d 737, 740 (9th Cir. 1978). Here, even if the affidavit was corrected per the Chisms' claimed omissions and misrepresentations, it was not "so lacking in indicia of probable cause as to render official belief in its existence unreasonable." *Malley v. Briggs*, 475 U.S. 335, 345 (1986).

Finally, the majority errs in its determination that the affidavit failed to establish probable cause because the police did not establish "a physical link between the illegal images and the locations to be searched." *See* Maj. Op. at 16327. The majority's ruling is directly contrary to the Supreme Court's decision in *Gates*, which held that a determination of probable

[2]The majority's argument that the lack of a match between the IP address used to register the foel and qem websites is a material omission and reduces probable cause because it means that "one additional inference is necessary to conclude that evidence of a crime will be found at the location to be searched," Maj. Op. at 16328 n.14, likewise runs afoul of *Gourde*'s admonition that the government need not "obtain potentially dispositive information." 440 F.3d at 1073 n.5.

cause must be based on the totality of the circumstances, not on the presence or omission of specific items of evidence. 462 U.S. at 230-31; *see also United States v. Martinez-Garcia*, 397 F.3d 1205, 1217 (9th Cir. 2005). And it is directly contrary to *Gourde*, which rejected the necessity for the sort of evidence (e.g., an IP address association or physical link) that the majority suggests is required. There was no need, *Gourde* tells us, for the police to develop any evidence that Gourde had ever received or downloaded images, let alone evidence of downloads traced to his IP address. *See* 440 F.3d at 1072-73. Given the government's evidence that phony IP addresses abound in cyberspace, the majority's "physical link" rule will baffle many an investigation into child pornography and its users and peddlers.

IV

While it turns out that the Chisms were not responsible for the child pornography websites under investigation by the police, ample evidence pointed to the conclusion that they were. The evidence established more than a fair probability that child pornography would be found on computers at the Chisms' residence; indeed, *Gourde* compels the conclusion that the police had probable cause for the search.[3] Therefore, there was no constitutional violation, and the district court did not err in granting summary judgment to the police on the basis of qualified immunity. In concluding that evidence leading to suspects who are paying to host their own child pornography websites does not create a "fair probability" that child pornography will be found on the suspects' computer, the majority turns its back on Deep Throat's adage, our case law, and the Supreme Court's probable cause jurisprudence. I dissent.

[3]Though the arrest warrant is a closer question, the evidence also supported probable cause to arrest *either* Todd or Nicole Chism. *See Smith v. Almada*, 640 F.3d 931, 937 (9th Cir. 2011).