No. _____

In The
Supreme Court of the United States

NIKOLAI BOSYK,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

William D. Ashwell
Counsel of Record
MARK B. WILLIAMS & ASSOCIATES, PLC
27 Culpeper Street
Warrenton, Virginia 20186
(540) 347-6595
wdashwell@mbwalaw.com

Counsel for Petitioner ***Dated: January 7, 2020***

THE LEX GROUP[DC] ♦ 1050 Connecticut Avenue, N.W. ♦ Suite 500, #5190 ♦ Washington, D.C. 20036
(202) 955-0001 ♦ (800) 856-4419 ♦ www.thelexgroup.com

QUESTION PRESENTED

The Fourth Amendment establishes "[t]he right for people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and continues "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

Whether the single click of a URL link to child pornography by someone using an individual's IP address can provide probable cause to support a search warrant without any additional substantive factual information related to the suspect.

PARTIES TO PROCEEDING AND RULE 26.6 STATEMENT

Petitioner is Nikolai Bosyk. Respondent is the United States of America. No party is a corporation.

RELATED PROCEEDINGS

The following proceedings are directly related to this petition:

United States v. Bosyk, No. 1:17-cr-00302-LMB-1 (E.D.V.A.) (Bosyk Judgment entered May 7, 2018; *aff'd*, *United States v. Bosyk*, No. 18-4302 (4th Cir. August 1, 2019) (reported at 933 F.3d 319); Petition for Rehearing *En Banc* denied October 9, 2019.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

PETITION FOR WRIT OF CERTIORARI

Petitioner Nikolai Bosyk respectfully petitions for a writ of certiorari to review the judgment of the United States District Court for the Eastern District of Virginia and the Fourth Circuit Court of Appeals. Petition Appendix at 148a ("Pet. App."). The relevant order of the trial court is published.

INTRODUCTION

The principals of the Fourth Amendment are paramount to the basic freedoms enjoyed by every citizen, and provide "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As stated by Judge Wynn's dissent stemming 70 pages, "[t]his case presents a textbook example of why we must guard against the slow whittling away of constitutional rights, particularly as we apply constitutional rights adopted in an analog era to the new challenges of the digital age." Pet. App. 27a. This case presents the ever-expanding problem modern jurisprudence faces in adapting classic constitutional and legal principals to modern technology. While the temptation to adhere steadfastly to traditional principals in the application of precedent to modern legal issues, this approach fails to withstand constitutional scrutiny. In the instant case, as Judge Wynn's dissent continues, "[a] basic understanding of the technology at issue demonstrates that the government's bare-bones affidavit supporting a warrant to search the residence of Defendant … failed to establish a fair probability that, when clicking on a link to download child pornography, someone using Defendant's IP address

knew and sought out that illicit content. Indeed, rather than confronting the difficult technological questions courts must address in assessing warrant applications premised on online conduct, the majority opinion rests on analog frameworks that fail to account for the meaningful differences between the Internet and the physical world. With due respect to my colleagues in the majority, I believe the majority opinion displays a troubling incomprehension of the technology at issue in this matter." *Id*.

The immediate threat and risk of continued constitutional derogation stemming from the Fourth Circuit's analysis and precedent established in this matter cannot be overstated. The Fourth Circuit's majority opinion in *Bosyk* marks a stark deviation from precedent established throughout the circuits related to probable cause determinations in similar factual scenarios. Concerns abound in the majority's fundamental misunderstanding of technical issues that are pervasive throughout the subject search warrant. Further, the Fourth Circuit's decision is replete with error when the technology and facts at issue are properly analyzed and the inferences depended upon by the majority are appropriately placed in contact. To let the *Bosyk* decision stand would be in direct contravention of this Court's mandate that "'mechanical interpretation[s]'" of the Fourth Amendment that would allow the government to "capitalize" on such technology to invade the reasonable expectations of privacy and security protected by that Amendment. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001)). The Petition for Certiorari should be granted.

OPINIONS BELOW

The Fourth Circuit's opinion (Pet. App. 1a-148a) is reported at 933 F.3d 319.

JURISDICTION

The United States District Court for the Eastern District of Virginia issued its final order on May 7, 2018. Pet. App. 149a. On August 1, 2019, the United States Court of Appeals for the Fourth Circuit entered its published opinion. Pet. App. 148a. On October 9, 2019, the Fourth Circuit denied Mr. Bosyk's Petition for Rehearing *En Banc*. Pet. App. 159a. This Court's jurisdiction rests on 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment states in pertinent part "[t]he right for people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and continues "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

STATEMENT OF THE CASE

On April 8, 2016, the government sought a warrant to search Mr. Bosyk's residence located at 10966 Harpers Ferry Road, Purceville, Virginia 20132. Pet App. 5a. In support thereof, Homeland Security Special Agent Kristina Eyler provided a sworn affidavit in support of the application for a search warrant. Pet. App. 5a-6a. In the 10 page affidavit, less than a page of the subject affidavit

addresses any specific conduct or investigation specifically tailored to Mr. Bosyk. *Id*.

The affidavit, in and of itself, is dedicated largely to a description of the government's involvement and investigation into a website known as "Bulletin Board A." Pet App. 27a-31a. The affidavit specifically alleges Bulletin Board A is a file sharing internet based bulletin board where its users are primarily engaged in the sharing of child pornography images." Pet. App. 3a. There are actively 1,500 "approved users" posting new content on the forum; the affidavit describes "sub forums" which were investigated and believed to contain child pornography; the affidavit describes, in general terms, several posts investigated by the Department of Justice where a member of Bulletin Board A posted or otherwise shared a clip believed to depict child pornography and included a thumbnail of the video with a link for the user to access; according to the government's affidavit, this post and similar posts required the input of a password in order to access the suspected child pornography file. Pet App. 27a-31a.

The affidavit further outlines Bulletin Board A hosts files in various formats, including a storage service known as File Sharing Site (or "FSS"). Pet App. 4a. Further, the affidavit states in general terms that "law enforcement has reason to believe that FSS's service was used by members to store files containing child pornography and make them accessible to other members." *Id*. The affidavit alleges no specific conduct by Mr. Bosyk related to the posting, collection or sharing of child pornography on the FSS website or network, nor does it include facts constituting membership on Bulletin Board A. *Id*.

In the only section pertaining directly to Mr. Bosyk, under the header "IDENTIFICTION OF THE SUBJECT PREMISES," the government outlines Mr. Bosyk's *de minimis* connection to a single unique URL, to which the government alleges an IP address identified as 208.89.176.122 was "used to download or attempt to download file content associated with that URL." *Id*.

The affidavit does not match the subject unique URLs outlined in para. 7 through 8 and para. 16. Pet. App. 28a. From the government's receipt of information and IP addresses from FSS, a search was conducted related to the aforementioned IP addresses "download or attempt to download" which was found to be belonging to subscriber "Nik and Jennifer Bosyk" at 10966 Harpers Ferry Road, Purceville, Virginia 20132. Pet. App. 4a. There is no other specific information, allegations of conduct, specific recitations of behavior, information as to the collection or dissemination of items believed to be child pornography related to Mr. Bosyk. Pet. App. 30a. Crucially, the government's affidavit supporting the search warrant never alleges or associates Mr. Bosyk's IP address as being associated with Bulletin Board A. *Id*.

Specifically, the affidavit fails to allege Mr. Bosyk clicked any link in Bulletin Board A or that Bulletin Board A was the means that his IP address attempted to access the subject URL. Pet. App. 30a. The affidavit fails to allege Mr. Bosyk is a registered user of Bulletin Board A, despite the affidavit's general provisions related to the website having over "1,500 users," there is no allegation that Mr. Bosyk ever specifically visited Bulletin Board A,

and the affidavit instead alleges some individual associated with the subject IP address navigated to URL [http://[redacted].comxu5me9erdipp/brochure.rar.htmll.] Pet. App. 28a-31a.

The URL specifically referenced in the affidavit by the government contains no specific identifiers or indicators that the link contains illegal content or child pornography. Pet App. 28a. Further, the specific URL identified by the government as allegedly accessed by someone using Mr. Bosyk's IP address differs from the URL identified in the government's affidavit as containing child pornography on Bulletin Board A.[1] Pet. App. 28a. The affidavit itself contains absolutely no information on how the individual associated with Mr. Bosyk's IP address found or landed on the subject URL, and failed at any point to establish Mr. Bosyk accessed or attempted to access the subject URL through Bulletin Board A. Pet. App. 30a. There is no evidence or accusation that the actual content, alleged to contain child pornography, was ever accessed, viewed, downloaded, or otherwise utilized in any fashion by Mr. Bosyk or any person using his IP address. *Id*. The affiant for the government makes clear in the subject affidavit that the alleged illicit content must be accessed by the use of a password as a form of encryption, however fails at any point in the affidavit to establish or even allege that Mr. Bosyk or the individual using the subject IP

[1] The government identified a specific file posted on Bulletin Board A, believed to contain child pornography, however the subject affidavit does not indicate or establish this file was accessed or even attempted to be accessed by Mr. Bosyk or someone using his IP address. The only allegation pertained to the click of a URL. Pet. App. 4a; 30a.

address used any password, attempted to use a password, or ever gained access to the illegal content beyond clicking the subject URL. Pet. App. 3a; 9a. There is, in fact, an omission in the affidavit of facts substantiating any individual using the subject IP address entered any password in accessing or attempting to access the subject URL and the illicit content. *Id*. The only fact established by the affidavit supporting the search warrant was Mr. Bosyk's IP address, on one occasion, came upon the subject URL that appeared on its face to be absolutely harmless. Pet. App. 4a. There are no facts or circumstances supporting the government's position that the individual using the IP address knew of the website's contents, that the individual went to the website for a specific purpose or on purpose at all, or received, downloaded or otherwise gained access to illegal child pornography.

The final section of the subject affidavit contains sweeping and generalized "characteristics" of persons who collect child pornography. Pet. App. 4a-5a. Nothing in the affidavit contains any facts to establish or support the position that Mr. Bosyk or the person using the subject IP address is a collector of child pornography and, indeed, the only real accusation is a single instance of attempted access to purported child pornography. Pet. App. 57a. The subject search warrant was issued the same day as its application, and on April 12, 2016 the search warrant was executed on Mr. Bosyk's residence. Pet. App. 5a. A total of 14 items were removed from Mr. Bosyk's residence as a result of the subject search warrant, including computers and tablets. *Id*.

Over a year later, on December 14, 2017, the Defendant, Mr. Bosyk was charged with one count of receipt of child pornography in violation of Title 18, United States Code, Section 2252(a)(2) & (b)(1) and one count of possession of child pornography in violation of Title 18. United States Code, Section 2252(a)(4)(b) and (b)(2). Pet. App. 5a-6a. On January 3, 2018, Mr. Bosyk filed a Motion to Suppress which was ultimately denied by the trial court, with the district court finding the warrant was supported by probable cause and that suppression would be unwarranted under *United States v. Leon*, 468 U.S. 897 (1984). *Id*. On May 7, 2018, Mr. Bosyk was convicted consistent with a plea agreement permitting him the ability to challenge the denial of his motion to suppress on appeal. Pet. App. 6a.

An intensely divided panel from the Fourth Circuit affirmed the district court. Judge Diaz writing for the majority concluded, "[w]e are sensitive to the privacy interest at stake here. But we also cannot ignore that many crimes are committed with just a few clicks of a mouse—including the very serious crime of downloading child pornography. In cases like this, our job is to ask precisely what 'a single click' reveals under the circumstances presented, and whether that information justifies searching a person's most private places for evidence of a crime." Pet. App. 26a. In support of affirming the district court's denial of Mr. Bosyk's motion to suppress, the majority identifies the "critical fact" as being the timing the subject URL link was posted. Pet. App. 8a. The majority relies on the argument advanced by the government that "the close timing between the link's appearance on Bulletin Board A and the click by a user's IP address is highly relevant:

because the was accessed on the same day it appeared on Bulletin Board A, it is at least reasonable probable that the user clicked the link having encountered it on that website. Pet. App. 8a-9a.

As noted in the dissent's 70 page thorough and detailed analysis, Judge Wynn identifies the false assumptions relied upon by the majority in finding this "critical fact" established probable cause in the subject search warrant. Pet. App. 41a-45a. Namely, the government's temporal proximity argument rests on the "critical fact" that someone using Defendant's IP address clicked on the URL *after* the post containing the URL appeared on Bulletin Board A—a premise that the government repeatedly asserted in its briefing and argument to the district court and this Court." Pet. App. 41a-42a. Noting this key factual finding necessary to bolster the majority's reliance on this "critical fact," the dissent captures the key fallacy in the majority's reliance – that the subject affidavit fails to establish this "critical fact." Judge Wynn notes, "whereas the affidavit reports the time someone using Defendant's IP address clicked on the File Sharing Site URL—3:23 pm on November 2, 2015—it does not report at what time that day the post first appeared on Bulletin Board A." Pet. App. 42a. The dissent notes, in order for the majority to accept this "critical fact" as supportive of its position, the majority opinion impermissibly draws inferences on inferences to uphold the warrant. Pet. App. 44a. (quoting *Rosencranz v. United States*, 356 F.2d 310, 317 (1st Cir. 1966); noting that a magistrate may not "reach for external facts and . . . build inference upon inference in order to create a reasonable basis for his belief that a crime is presently being committed").

In identifying the multiple flaws and issues with the factual premise advanced by the majority, Judge Wynn grapples with the complex technological issues at hand and contextualizing the technological referenced included in the subject affidavit, and those that are omitted. The dissent importantly notes, "there are myriad ways users can encounter and navigate to a URL— including unintentionally, particularly when, as here, the text of the URL provides no indication as to the nature of the content to which it navigates. Pet. App. 53a.

REASONS FOR GRANTING PETITION

I. THE FOURTH CIRCUIT'S DECISION HIGHLIGHTS THE SPLIT AND SUBSTANTIVE DISCREPENCIES BETWEEN THE CIRCUIT'S AS TO PROBABLE CAUSE DETERMINATIONS IN FACTUALLY SIMILAR CASES.

There exists an unsettled landscape and split circuits on the application of the probable cause standard to search warrants related to internet related criminal investigation and activity. In part, this is due to advancing technology and the complex nature of applying analog constitutional standards to a digital world. The clarity and analysis from this Court will provide pivotal guidance and clarity to trial court application of Fourth Amendment standards to evolving, complex issues related to digital and internet based fact patterns in order to ensure individual liberty is protected and improper government intrusion is kept at bay.

A. There now exists a split between the circuits based on the *Bosyk* court's holding which warrants a grant of the petition.

This Court has previously recognized the crucial aspects of ensuring Fourth Amendment principals remain intact with the onset of new technology. In doing so, this Court has rejected "'mechanical interpretation[s]'" of the Fourth Amendment that would allow the government to "capitalize" on such technology to invade the reasonable expectations of privacy and security protected by that Amendment. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001)). In so finding, this Court reiterated courts must, "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* This Court in *Carpenter* stated, "our cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Id.* (quoting *Boyd v. United States*, 116 U.S. 616, 630, 6 S. Ct. 524, 29 L. Ed. 746 (1886); and *United States v. Di Re*, 332 U.S. 581, 595, 68 S. Ct. 222, 92 L. Ed. 210 (1948)).

The Second, Fourth, and Ninth Circuits all provide varying approaches and analysis to search warrants related to online child pornography. Despite the varying approaches by the Circuits, prior to *Bosyk* the appellate court analysis focused on particularized inquiries in search of established

probable cause in a subject search warrant. Further, in direct conflict with the Fourth Circuit's opinion in *Bosyk*, the Eastern District of Virginia has produced two diametrically opposed decisions to an identical search warrant in the *United States v. Reece*, 2017 U.S. Dist. LEXIS 220176 (E.D. Va. March 1, 2017) decision. The ability of two Court's in the same jurisdiction to produce such diametrically opposed decisions on the exact same issues highlights the importance that this Court address the issues raised in this appeal. The foregoing splits warrant the granting of the petition by this Court in order to settle the mechanical, legal and technical principals to apply when analyzing a search warrant involving complicated internet age concepts. As stated by Judge Wynn in the Fourth Circuit's order denying Appellant's Petition for Rehearing *En Banc*, "[t]he Government in this matter leads this Court to depart from the wisdom of our sister circuits and endorse an unsustainable approach to evaluating evolving technology." Pet. App. 160a.

The Ninth Circuit in *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc), established criteria for determining probable cause to search a defendant's residence in the landscape of child pornography. The Court in *Gourde* found probable cause based on facts set forth in affidavit establishing a fair probability that the suspect "inten[ded] and desire[d] to obtain illegal images," *Id*. at 1070. The facts relied upon included (1) the suspect paid for a subscription to the website Lolitagirls.com that "was a child pornography site whose primary content was in the form of images; (2) credit card records of the suspect revealed that in order to subscribe to the website the suspect has to submit "his home address,

email address and credit card data, and he consented to have $19.95 deducted from his credit card every month"; and (3) the suspect "became a member [of the website] and never looked back – his membership ended because the FBI shut down the site" after several months. *Id*. at 1070-71. In finding probable cause existed, the Court relief upon the premise that the defendant "could not have become a member by accident or by *a mere click of a button*[.]" *Id*. (emphasis added). The circumstantial evidence related to the defendant was crucial in the Court's determination of probable cause and the "countervailing probability" that the defendant innocently visited the website was low. See *United States v. Jackson*, 415 F.3d 88, 94 (D.C. 2005); see also, e.g., *United States v. Martin*, 426 F.3d 68, 78 (2d Cir. 2005) (finding probable cause to search a residence when electronic records revealed that an individual with a particular email address "joined . . . voluntarily and never cancelled his membership" to a child pornography website and that the user of the email address lived at the residence for which the warrant was sought).

In contrast to *Gourde*, other circuits have declined to find probable cause in instances where the government fails to include facts that diminish the likelihood that child pornography website was accesses innocently or unintentionally. The Second Circuit in *United States v. Falso* held a forensic analysis of a website server believing to host child pornography - revealing the identity of a suspect who has been charged 18 years earlier for sexually abusing a minor – had "either gained access of attempted to gain access" to a child pornography website did not establish probable cause to search his home. 544 F.3d at 114. In authoring the Second Circuit's opinion,

now-Justice Sotomayor held facts were insufficient to find probable cause because, unlike *Martin*, the search warrant affidavit included "no allegation that [the suspect] in fact gained access to the [child pornography] website, much less that he was a member or subscriber of any child-pornography website." *Id*. at 124.

In coming to its holding, the *Falso* Court identified several criteria that would satisfies the "fair probability" standard accompanying a warrant application, including that the suspect (1) took actions "tend[ing] to negate the possibility that his membership or subscription was unintended," such as being a member of multiple forums or child pornography website memberships; (2) use of an "e-mail address [] or screen name [] suggestive of an interest in collecting child pornography; or (3) a "criminal history relating to child pornography." *Id*. at 120. Further, the government could have "monitored the traffic of [the child pornography] website and ascertained whether [the suspect] (and others) actually downloaded pornography from the site." *Id*. at 124.

The *Falso* Court identified key factual distinctions in search warrants related to child pornography that the majority in *Bosyk* willingly chose to ignore. In justifying the departure from established criteria in the analysis of sufficient facts accompanying a search warrant application, the *Bosyk* court attempts to distinguish the holding from the *Falso* without success. As highlighted by the dissent in *Bosyk*, the majority relies on the premise that the affidavit in *Falso*, "contained no allegation that the defendant in fact gained access to a website

containing child pornography, nor any allegation that images of child pornography were downloadable from the site." Pet. App. 17a. This differed, according to the majority, because the *Bosyk* affidavit "alleged that [Defendant]'s IP address accesses a URL" containing child pornography. *Id.* The Bosyk majority misinterprets the meaning behind the click of a URL to facts establishing actual access of child pornography. The Court below in this matter has created a new test and criteria, different from other circuits, in no longer requiring the government allege actual receipt and/or accessing of illicit material, but instead simply requiring the click of a link. The link, which in and of itself, does not establish a suspect actually downloaded or accessed child pornography.

Disturbingly absent from the majority's opinion is a reference or analysis to the precedent established by the *United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005) (Rakoff, J.). In *Coreas*, the Defendant was investigated and the affidavit supporting an application for a search warrant issued after the Defendant clicked on a link to subscribe to a group with an invitation that read, "[t]his group is for People who love kids. You can post any type of messages you like too or any type of pics and vids you like too. P.S. IF WE ALL WORK TOGETHER WE WILL HAVE THE BEST GROUP ON THE NET." *Id.* at 152. In analyzing the sufficiency of probable cause based on the single click of the Defendant, the Second Circuit found:

> Once these allegations are excised, what is left to support the search in this case? Simply the allegation that Coreas logged onto the Candyman website and, by

> clicking a button, responded affirmatively to a three-sentence invitation (quoted supra) to join its e-group. The alleged "proclivities" of collectors of child pornography, on which the district court relied, are only relevant if there is probable cause to believe that Coreas is such a collector. But the only evidence of such in the excised affidavit is his mere act of responding affirmatively to the invitation to join Candyman.

Coreas, 419 F.3d at 156. The *Coreas* court focused on the same factual deficiencies contained in the instant search warrant, related to the boilerplate information describing "collectors" of child pornography, without any factual contentions or facts related to the Defendant actually being a collector. Like the instant case, the only facts relied upon in the issuance of the search warrant, and seemingly in the investigation of the Defendant altogether, was the click of one URL without evidence of collection.

The *Coreas* court went on:

> In the view of this panel, that does not remotely satisfy Fourth Amendment standards. We had thought it was well settled that a "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." All that Coreas did, so far as the excised affidavit shows, was to respond to a three-sentence suggestive invitation from Candyman to join its e-group ***by***

> ***clicking a button*** that added his e-mail address to its roll of members but in no way committed him to in any of its various activities, lawful or unlawful, or even to receiving its e-mails (which he had the option to refuse from the outset). The notion that, by this act of clicking a button, he provided probable cause for the police to enter his private dwelling and rummage through various of his personal effects seems utterly repellent to core purposes of the Fourth Amendment. (Emphasis added).

Id. at 156.

The instant case rests on the same proposition as the conclusion reached by the *Coreas* court – the single click on a URL, in and of itself, is insufficient as a matter of law to establish probable cause to a degree justifying the issuance of a search warrant of a person's premises. Even in *Coreas*, the Defendant had an idea that the link or content may be illicit or inappropriate – however, that fact standing alone does not establish the government's burden in establishing probable cause to search for child pornography.[2]

In comparing the obvious invitation to access illicit content in *Coreas*, the instant case contains no causal connection between the knowing actions of Mr. Bosyk, or some individual, in attempting to access the subject content on Bulletin Board A. Here, the motion

---

[2] The Second Circuit noted the invitation on its face was "suggestive," however, the Court focused on the actions taken by the Defendant pursuant to the affidavit – simply clicking on a link supplied in an email.

to suppress should have been granted on remarkably similar grounds as the *Reece* and *Coreas* courts. The subject affidavit was issued predicated on the scant facts contained in the affidavit related to Mr. Bosyk's URL attempting to access a URL that contained password protected alleged illicit content. Pet. App. 3a. This, in and of itself, fails to satisfy the probable cause and constitutes sufficient basis for grant of this petition. The majority's failure to consider the precedent established by its sister circuit constitutes a willful omission in order to come to the holding affirming the trial court.

B. The Eastern District of Virginia itself is split on the appropriate analysis and criteria for the trial court's consideration of identical search warrants that further supports the grant of the petition in this case.

The Eastern District of Virginia itself has generated a split in application of Fourth Amendment standards to the same affidavit at issue in *Bosyk*, identifying the further need for this Court to grant the instant petition to establish uniform analysis of the increasing volume of internet centered search warrants. In *United States v. Reece*, the Court granted defendant's motion to suppress an analogous search warrant to the one at issue in this petition, finding:

> In light of the totality of the circumstance and Special Agent Julsrud's knowledge that there was no evidence that a password was entered, this information must be deemed

> recklessly omitted. The omission likely contributed to a finding of probable cause, and the practice of omitting such essential information suggests systematic flaws in how these sensitive investigations are undertaken.

2017 U.S. Dist. LEXIS 220176 at 30. The *Reece* Court identified the key functional concern with adopting the *Bosyk* court's position of accepting inference upon inference to find probable cause in the subject search warrant. The majority's analysis below rewards the government's willful omission of key facts from an affidavit in order to obtain the issuance of a search warrant to invade a citizens dwelling and seize property. This is a stark departure from both the safeguards intended from the Fourth Amendment itself and the other circuits that have analyzed this issue under similar fact patterns.

In sum, the decision below represents a shift and deepening division between the circuits on crucial questions related to the Fourth Amendment. Although the majority in *Bosyk* attempts to distinguish the facts from *Falso*, its holding is nothing more than a deviation and split from the other circuits that have taken up this issue. Such a pivotal subject matter in everyday practice and a subject area that impacts the lives of countless citizens daily, the functional misapplication of the technical and legal principals in *Bosyk* cannot be ignored and the precedent cannot stand.

II. THIS CASE RAISES ISSUES OF CONSIDERABLE IMPORTANCE.

The importance of this case and issues raised herein cannot be overstated. As identified by the majority below, the privacy interests at stake here are of crucial importance to American jurisprudence moving forward. Pet. App. 26a. However, even more important than the privacy interests identified by the majority, as the dissent proclaims, ***"[t]his case presents a textbook example of why we must guard against the slow whittling away of constitutional rights, particularly as we apply constitutional rights adopted in an analog era to the new challenges of the digital age***." Pet. App. 27a. (Emphasis added).

The Fourth Amendment itself represents the Framers' "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). This Court has routinely rejected "'mechanical interpretation[s]'" of the Fourth Amendment that would allow the government to "capitalize" on such technology to invade the reasonable expectations of privacy and security protected by that Amendment. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001)). When confronted with new technology, this Court confirmed courts must seek to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* (quoting *Kyllo*, 533 U.S. at 34). "Technology is both a threat and a

promise." *Vieth v. Jubelirer*, 541 U.S. 267, 312 (2004) (Kennedy, J., concurring in the judgment). Although new technologies can foreclose certain avenues for the government to show probable cause—such as through geographic proximity—"new technologies [also] may produce new methods" of demonstrating probable cause. *Id*. at 312–13.

As the Court below noted, cases with technical issues similar to the facts at hand in this petition warrant significant input from litigants and others to explain technical issues and nuances. "This is why courts depend on *amici curiae* and, more importantly, the parties themselves, to explain technical issues in cases like this one, and to explain them well." *See, e.g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 306 n.1 (3d Cir. 2010) (thanking a group of *amici* led by the Electronic Frontier Foundation, who provided amici curiae below, for participating in a case involving an *ex parte* application by the government and an issue of first impression related to the Stored Communications Act and cell site location information). Pet. App. 163a.

This case presents a unique and compelling vehicle to bring the Fourth Circuit and other courts in line with this Court's precedents surrounding the Fourth Amendment and advancing technological influence on everyday life. Undoubtedly evolving technology will continually impact and question legal standing precedent at any given moment – and the goal, as stated by this Court, is to continually ensure that new technology does not hamper the Fourth Amendment protections and privacy concerns that existed when the Fourth Amendment was

adopted. See *Kyllo*, 533 U.S. at 34. This case provides an outstanding opportunity to take existing constitutional principles and apply them to the unique technological issues in order to provide clarify to trial and appellate courts forced to confront these issues on a daily basis. The issue presented is stark and clear: whether the single click of a URL link to child pornography by someone using an individual's IP address can provide probable cause to support a search warrant without any additional substantive factual information related to the suspect. In the instant case, like other court's referenced herein analyzing Fourth Amendment principles related to child pornography search warrants, there is little to no dispute on the content of the subject affidavit and what is and is not included by the affiant.

The Court dealt with a similar dilemma in addressing the advanced ability for the government to operate surveillance on individuals through GPS monitoring of individual cellular phones. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court dealt with "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." *Id*. at 2216. In recognizing the advancements of technology and the needs to constantly review and analyze the applicable standards of reviewing Fourth Amendment conduct, the Court opined, "[a]fter all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id*. at 2217. Similar to the concepts outlined by Justice Sotomayor above, nearly identical

principles are at issue in the instant petition. Few could imagine the advancements in technology that would constitute a world wide web with nearly every available video, image, webpage, or piece of information available with a simple search and click of a mouse from the comfort of one's home. With these technological luxuries comes the gigantic risk, at issue here, of the government's ability to use these technological advancements to abuse, infringe, and otherwise trample of individual constitutional rights and the privacy each citizen enjoys.

In short, the dissent below identifies the tremendous importance of the issues at hand in this appeal and the permeating error committed by the majority, stating, "our 'judicial duty' is to guard against infringements on our constitutional rights. Unfortunately, the majority's 'judicial choice' to use layers of unsupported inferences that do not meaningfully grapple with the technology at issue diminishes the constitutional rights of those who use the Internet—I say woe unto all users of the Internet." Pet. App. 103a.

III. THE FOURTH CIRCUIT ERRED IN RULING ON THE QUESTION PRESENTED IN THIS PETITION.

Certiorari should be granted in this case because, on the question at issue in this petition, the Fourth Circuit erred. A clear reading of the Fourth Amendment and the principles therein contained render the majority's opinion below clear error and this Court must overturn the precedent created by the *Bosyk* court. The majority's steadfast desire to ignore guidance from sister circuits, precedent from this Court, and the facts of the case are egregious errors

that cannot go ignored. With significant individual privacy and liberty issues at stake, the petition should be granted.

First and crucially, the majority below demonstrated a basic misunderstanding of facts material to the case and crucial to deciding the case on the merits versus mere speculation. The "critical fact" in the majority's analysis, and perpetrated repeatedly by the government at the district court and in the Fourth Circuit, was the alleged temporal connection between the posting of the link in Bulletin Board A and the URL being clicked by someone associated with Mr. Bosyk's IP address. Pet. App. 41a. Further, the government asserts – and the majority accepted – that the subject link "originated on a dark web forum dedicated to sharing sexual abuse content. Pet. App. 3a; 41a. The foregoing assumptions accepted by the majority are false and verifiably unsupported by the content of the subject affidavit in support of the search warrant.

The temporal proximity argument put forth by the majority – and the primary basis for the court affirming the trial court – is without support from the plain language of the affidavit. Indeed, if the subject URL was clicked before being posted on Bulletin Board A, then the person using the Defendant's IP address did not click the link on Bulletin Board A. As highlighted by Judge Wynn below, whereas the affidavit reports the time someone using Defendant's IP address clicked on the File Sharing Site URL—3:23 pm on November 2, 2015—it does not report at what time that day the post first appeared on Bulletin Board A. Pet. App. 42a. Rather, it simply states that the post appeared on Bulletin Board A sometime on

November 2, 2015. *Id.* Crucially, the post could have appeared on Bulletin Board A anytime within a window of 8 hours, 37 minutes *after* someone using Defendant's IP address downloaded or attempted to download the child pornography from File Sharing Site. *Id.* What was missing from the subject affidavit – and accepted as fact by the majority below at the insistence of the government – was any factual support for the premise that the subject URL link was posted on Bulletin Board A before being clicked by someone using the defendant's IP address.

The dissent below points out the government's repeated argument and explanation of the sequence of events related to the link posting in its brief at all levels, which finds no direct support in the facts set forth in the warrant application at issue. Pet. App. 43a. The inability to establish by discernable facts included in the subject affidavit are fatal to the majority's reliance on the "critical fact" which is the temporal proximity argument. The majority even goes so far as to consider this assumption as fact, instead of the unsubstantiated inference that it is. Pet. App. 8a-9a.[3] As stated in *See Rosencranz v. United States*, 356 F.2d 310, 317 (1st Cir. 1966), a magistrate may not reach for external facts and . . . build inference upon inference in order to create a reasonable basis for his belief that a crime is presently being committed."

With the majority's reliance on the temporal timing fact misplaced as explained above, the majority further fails to appreciate the complexity of

[3] Indeed, the majority asserts, "[t]hat chronology of the URL click following the Bulletin Board A post] sets in motion the series of plausible inferences described above." Pet. App. 10a-11a; 44a.

the technical nuances at hand and the facts in the record. With the click of a URL at issue, the majority seemingly overlooks or misunderstands how URLs work, as the *Bosyk* court concluded, "the randomness of the URL helps the government, as internet users aren't likely to type a truly random string of characters into their web browser by mistake." Pet. App. 15a. This concept that the URL was typed, of course, does not support the probable cause theory advanced by the government and relied upon by the majority that the link was intentionally clicked in Bulletin Board A because the individual believed it led to child pornography. Fundamentally, the majority's examples and factual assumptions demonstrate a fundamental misunderstanding of URLs, their purpose, and the content behind them. As the dissent articulates:

> [T]here are myriad ways users can encounter and navigate to a URL—including unintentionally, particularly when, as here, the text of the URL provides no indication as to the nature of the content to which it navigates. Accordingly, even if the Bulletin Board A post preceded the attempt by someone using Defendant's IP address to download child pornography from File Sharing Site—again, a fact not established by the affidavit—there are potentially millions of paths through which someone using Defendant's IP address could have encountered and navigated to the File Sharing Site URL hosting the child pornography other than through Bulletin Board A. Put

> simply, the affidavit does not establish the probability of the single sequence of events upon which the majority opinion relies—that someone using Defendant's IP address navigated to the File Sharing Site URL after encountering it on Bulletin Board A. *See* Figure B at 54a (contrasting the majority opinion's myopic focus on one pathway between Defendant's IP address and the File Sharing Site URL with the myriad pathways, only some of which are reflected by the dashed lines, consistent with the affidavit). Pet. App. 53a.[4]

The foregoing argument and the detailed analysis included in the dissent below establish the majority ignored the realities of the facts and information included in the subject search warrant in order to affirm the trial court. In doing so, the majority has created precedent with disturbing and far-reaching consequences.

Second, the majority relies on the generalized and boilerplate language included in the affidavit in support of their holding. In large part, the majority ignores the special agent affiant's failure to follow the "go-by" language provided by Homeland Security in preparing the subject affidavit. For issuance of a search warrant, the Fourth Amendment permits courts to rely on "the affiant-officer's experience" and knowledge regarding given crimes only when the affidavit contains sufficient evidence linking an

---

[4] See Pet. App. 54a-56a for a detailed analysis of the mathematical probabilities that relate to the majority's "crucial fact" as to the click timing sequence explained herein.

individual to that crime. Wayne R. LaFave, 2 Search & Seizure § 3.7(d) (5th ed. 2018).[5]

In the instant case, the special agent's directive in conducting the investigation and issuing the subject search warrant directed the boilerplate "collector" language be included in the affidavit be included "ONLY if" the affiant can "tie [collector] characteristics to the specific offender. Pet. App. 59a; quoting *United States v. Reece*, No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176, at 22 (E.D.Va. Mar. 1, 2017); an Eastern District of Virginia case that dealt with the identical investigation and search warrant). The special agent affiant in this case chose to include the boilerplate language without particularized facts related to the subject and collecting activity, further calling into question the majority's reliance on this language as supporting a probable cause determination. Pet. App. 13a; 59a. The subject boilerplate language was not only misleading to the magistrate below issuing the search warrant, but also mislead the majority into ignoring the facts in the record in favor of pure speculation.

The *Reece* court, having analyzed the instant issue regarding the search warrant in March of 2017, is not factually distinguishable from the instant case. In fact, the *Reece* affidavit established the posting of the subject link in Bulletin Board A before it was clicked by the subject's IP address. Pet. App. 64a; *Reece*, No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176.

---

[5] *See United States v. Underwood*, 725 F.3d 1076, 1082–83 (9th Cir. 2013), holding when individualized information connecting an individual to a crime is absent, an affiant—much less a court—cannot rely on generalized, boilerplate assumptions about criminal habits.

Trying to distinguish the *Reece* facts from the *Bosyk* affidavit, the government and the majority continually rely on the false temporal timing argument – as explored herein – in support of their position and ignoring the analysis put forth in *Reece*. This logic is fallacious and contrary to a correct reading of the two search warrants, as the *Reece* affidavit establishes the very "critical fact" the *Bosyk* affidavit does not – that the subject URL was posted on Bulletin Board A *before* it was accessed by the suspect. Pet. App. 64a-65a.

Authority from other circuits support the *Reece* court's decision and highlights the error of the *Bosyk* court. Related to the majority's reliance below on the temporal proximity and "collector" language inclusion, the court in R*ichardson* contradicted this misplaced reliance. *United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010). The court highlighted:

> Although "there is no question that time is a crucial element of probable cause," the existence of probable cause cannot be determined "by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit," Instead, we "look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." In the context of child pornography cases, courts have largely concluded that a delay--even a substantial delay--between distribution and the issuance of a search warrant

> does not render the underlying information stale. This consensus rests on the widespread view among the courts--in accord with Agent White's affidavit--that "collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes."

Id. at 370 (*quoting United States v. Johnson*, 461 F.2d 285, 287 (10th Cir. 1972)); see also *United States v. Farmer*, 370 F.3d 435, 439 (4th Cir. 2004) (Emphasis added). None of the criteria highlighted by the *Richardson* court was present in the Bosyk affidavit, and the inferential leaps from the court below are simply without support.[6]

Third, the majority demonstrated an unfortunate departure from established precedent from sister circuits and a deviation from the principles perpetuated by this Court in affirming the trial court.[7] While advancing and evolving technology create unique problems for a court to address in a Fourth Amendment context, other circuits have grappled with internet age issues in similar if not identical fact patterns and carved out criteria and precedent that was ignored by the *Bosyk* majority.

---

[6] See also *United States v. Raymonda*, 780 F.3d 105, 114-15 (2d Cir. 2015); establishing delineated criteria for a court's consideration of whether an individual should be considered a "collector" of child pornography; see also *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005).

[7] See also Section I herein.

As previously addressed herein, the Ninth Circuit in *Gourde* established delineated criteria in finding probable cause in a search warrant related to internet based child pornography. *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc). Namely, the holding that supporting facts including paid membership, the suspect's email address associated with the website, and continued membership up and until the subject website was shut down established sufficient probable cause to uphold the validity of the search warrant. *Id*. at 1070-71. Crucially, the Court determined a crucial factor was the membership of the subject to the group – and the fact this did not occur by the *mere clicking of a button*. *Id*. In comparison, the *Bosyk* court completely ignored this established criteria.[8]

Finally, the majority's reference to documents and files, allegedly downloaded from the link on Bulletin Board A, being recovered from the hard drive obtained from Mr. Bosyk's home point to a propensity to justify the inferences relied upon by the majority in coming to their conclusion. Pet. App. 31a. While the majority and dissent agree this fact has <u>*no bearing*</u> on the determination of probable cause in the subject search warrant, this fact pointed out by the majority in their holding points to a disturbing reliance on the "ends justifying the means." *McColley v. Cty. of Rensselaer*, 740 F.3d 817, 841 n.3 (2d Cir. 2014) ("Probable cause is not backward looking. Thus, the results of a search are immaterial to a determination of whether the search was supported by probable cause."); *United States v. Sims*, 553 F.3d 580, 583 (7th Cir. 2009) ("[T]here is a practical reason for requiring

[8] See also the *United States v. Falso* analysis included herein.

warrants where feasible: it forces the police to make a record before the search, rather than allowing them to conduct the search without prior investigation in the expectation that if the search is fruitful a rationalization for it will not be difficult to construct, working backwards." (citation omitted)). While it is well-settled law that the Fourth Amendment analysis is not backward looking as to the success of the search, the majority below seems to rely upon this as to justify upholding the search. The petition for a writ of certiorari should be granted.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

WILLIAM D. ASHWELL
VSB No. 83131
MARK B. WILLIAMS & ASSOCIATES, PLC
27 Culpeper Street
Warrenton, Virginia 20186
Telephone: 540-347-6595
Facsimile: 540-349-8579
wdashwell@mbwalaw.com
Counsel for Nikolai Bosyk

JANUARY 7, 2020

APPENDIX

APPENDIX TABLE OF CONTENTS

[ENTERED: August 1, 2019]

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-4302

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

NIKOLAI BOSYK,

Defendant – Appellant.

ELECTRONIC FRONTIER FOUNDATION,

Amicus Supporting Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Leonie M. Brinkema, District Judge. (1:17-cr-00302-LMB-1)

Argued: January 31, 2019 Decided: August 1, 2019

Before WYNN, DIAZ, and RICHARDSON, Circuit Judges.

Affirmed by published opinion. Judge Diaz wrote the majority opinion, in which Judge Richardson joined. Judge Wynn wrote a dissenting opinion.

ARGUED: William Davis Ashwell, MARK B. WILLIAMS & ASSOCIATES, PLC, Warrenton, Virginia, for Appellant. Fletcher Nathaniel Smith III, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. Stephanie Lacambra, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amicus Curiae. **ON BRIEF:** G. Zachary Terwilliger, United States Attorney, Lauren Britsch, Trial Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. Sophia Cope, Andrew Crocker, Aaron Mackey, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amicus Curiae.

DIAZ, Circuit Judge:

The basic facts are these. One day, a link appeared on a secretive online message board. Accompanying the link was a message describing its contents unmistakably as child pornography, as well as numerous thumbnail images depicting sexual molestation of a female toddler. And if you clicked the link, it took you, as promised, to multiple videos of child pornography.

On that same day, an IP address associated with Nikolai Bosyk's house accessed the link. Based on these facts, the government obtained a warrant to search Bosyk's home for evidence of child pornography. The primary question before us is

whether that warrant was supported by probable cause. Concluding that it was, we affirm.

I.

In September 2015, a Department of Homeland Security cybercrimes unit began investigating an online message board known as "Bulletin Board A." This board was "dedicated to the advertisement, distribution and production of child pornography," and had more than 1,500 "approved users." J.A. 163–64. The site contained several forums and subforums in which members could post and view various genres of child pornography.[1]

One such posting occurred on November 2, 2015. That day, an unidentified member of Bulletin Board A posted a message in the board's "Pre-teen Hardcore" section describing in graphic terms the contents of four videos. J.A. 164. Below the message were three sets of 20 video thumbnail images depicting "juvenile females engaged in sexual acts." *Id.* And below those images was a URL link—an apparently random string of numbers and letters.

The post also contained a password "which users could input to access and open the content of the file associated with that unique URL." J.A. 165. Using this password, federal investigators downloaded and viewed an encrypted file, which showed a man molesting a young girl, apparently a

[1] In related cases, the government has explained that Bulletin Board A is a dark web forum, accessible only through an anonymous web browser that users must download. *See United States v. Reece*, No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176, at *4 (E.D. Va. Mar. 1, 2017).

toddler. Three other videos associated with the link also contained child pornography.

This link and its contents were hosted by a separate filesharing site (referred to as "the File Sharing Site"). This site allows users to upload and share various media, and hosts plenty of lawful content. But the government also knew that Bulletin Board A's members used the File Sharing Site (and similar services) to share sexually explicit content with one another. So, in December 2015, investigators subpoenaed the File Sharing Site for business records related to web pages containing illicit material. In response, the company produced records showing that on November 2, 2015, at 3:23 p.m., an IP address "was used to download or attempt to download file content associated with" the URL containing the four videos. J.A. 167–68. In other words, the records showed that on the same day that the post and link appeared on Bulletin Board A, someone using this IP address clicked that same link.

By subpoenaing a broadband provider, investigators connected the IP address to Bosyk's home in Purcellville, Virginia. In April 2016, the government applied for a warrant to search Bosyk's house. It supported the application with an affidavit sworn by DHS Special Agent Kristina Eyler, which recounted the facts above.

Eyler's affidavit also described several "characteristics of individuals who possess or access with intent to view child pornography." J.A. 168. Such people, she said, may collect explicit materials and use them for arousal or to groom victims. They often store these materials electronically "for several

years," and frequently keep them nearby for ease of viewing. J.A. 169. Some individuals have been known to download, view, then delete child pornography from their electronic devices on a cyclical basis. But "evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools." J.A. 169.

Based on this information, Agent Eyler submitted that there was probable cause to suspect violations of federal laws against distributing, receiving, possessing, and accessing with intent to view child pornography, *see* 18 U.S.C. §§ 2252, 2252A, and that evidence of those suspected crimes would be found at Bosyk's address. A magistrate judge agreed, issuing a warrant that allowed the search of Bosyk's residence and the seizure of computers, digital devices, storage media, and related evidence.

Investigators executed the warrant four days later (on April 12, 2016) and recovered devices containing thousands of images and videos of child pornography, including the particular video described in the search warrant affidavit.[2] Agents also found evidence that Bosyk had used an anonymous web browser to access dark-web child pornography websites, including Bulletin Board A.

Bosyk was later indicted on child pornography charges. He moved to suppress the evidence obtained under the warrant and sought a hearing under

---

[2] As for the (undisputed) results of the search, our friend notes that what was found has no bearing on the question of probable cause. *See* Dissenting Op. at 31-32. But our substantive analysis is entirely faithful to that principle.

Franks v. Delaware, 438 U.S. 154 (1978), to show that Eyler had misled the magistrate judge. The district court denied the motion, holding that the warrant was supported by probable cause and that, in any event, suppression would be unwarranted.[3] Bosyk later pleaded guilty to one count of receiving child pornography and was sentenced to five years in prison.

II.

Having reserved the right to appeal the denial of his motion to suppress, Bosyk asks us to reverse that ruling and vacate his conviction. He raises three

---

[3] Our dissenting colleague posits that the government duped the district court into ignoring the important distinction between Bulletin Board A and the File Sharing Site, and into presuming that Bosyk's IP address accessed the URL after (rather than before) its posting on Bulletin Board A. *See* Dissenting Op. at 32-35. But we see little indication that the district court misunderstood the facts. Rather, we think the court's oral ruling as transcribed can be read to reflect a proper understanding both of the chronology of events and of the relationship between Bulletin Board A and the File Sharing Site. Regarding the timing, the court said that the URL was clicked "the same day" that the posting appeared on Bulletin Board A, J.A. 76, which is perfectly consistent with the affidavit. As for the distinction between the two websites, the court noted that on the day in question, "the IP address that is linked to a computer in the defendant's home . . . attempts to or at least shows an interest in that particular site." J.A. 76–77. It's admittedly unclear whether "that particular site" refers (incorrectly) to Bulletin Board A or (correctly) to the File Sharing Site. But the preceding sentence includes references to both the "posting" and "the URL that is linked," so both readings are possible. J.A. 76. Furthermore, the district court later noted the delay "between the time of that contact with the URL" and the warrant's issuance, J.A. 77, suggesting the court understood that Bosyk accessed the URL and not (necessarily) Bulletin Board A.

arguments. First, he argues that the search of his home violated the Fourth Amendment as it wasn't supported by probable cause. Second, he contends that even if the government had cause to search his home in November 2015 (when the post appeared on Bulletin Board A and the link was accessed), it didn't in April 2016 when it actually obtained and executed the warrant. Finally, Bosyk argues that suppression is warranted under *United States v. Leon*, 468 U.S. 897 (1984), because Eyler's affidavit was misleading and lacked any indicia of probable cause.

When considering a district court's denial of a suppression motion, we review its legal conclusions de novo, viewing the evidence in the light most favorable to the government. *United States v. Kolsuz*, 890 F.3d 133, 141–42 (4th Cir. 2018). For reasons that follow, we find no error.

III.

Before searching a home, the government generally must obtain a warrant, supported by probable cause. *Fernandez v. California*, 571 U.S. 292, 298 (2014); *see* U.S. Const. amend. IV. Probable cause requires only "a fair probability," and not a prima facie showing, that "contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause is therefore "not a high bar." *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (quoting *Kaley v. United States*, 571 U.S. 320, 338 (2014)). And officers need not "rule out a suspect's innocent explanation for suspicious facts" to obtain a warrant. *Id.* at 588.

Since a magistrate judge issued the challenged warrant, our task isn't to assess probable cause de

novo. *Gates*, 462 U.S. at 236. Instead, we apply a deferential and pragmatic standard to determine whether the judge "had a substantial basis for concluding that a search would uncover evidence of wrongdoing." *Gates*, 462 U.S. at 236 (alterations and internal quotation marks omitted). In doing so, we consider only the facts presented in the warrant application. *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018).

A.

Bosyk and his amicus (the Electronic Frontier Foundation, or "EFF") argue that the facts recounted in Agent Eyler's affidavit didn't give the government probable cause to search Bosyk's house for evidence of child pornography. They argue that the government obtained its warrant based on a "single click" of a URL, which, they say, cannot support a search of somebody's home. We disagree. The facts in the affidavit support a reasonable inference that someone using Bosyk's IP address clicked the link knowing that it contained child pornography. This in turn makes it fairly probable that criminal evidence would have been found at Bosyk's address.

The "critical fact" in this case, as the district court observed, is the timing. J.A. 76. On the very day that someone clicked the link, it appeared on a website whose purpose was to advertise and distribute child pornography to its limited membership. And it appeared in a post containing text and images that unequivocally identified its contents as child pornography. The close timing between the link's appearance on Bulletin Board A and the click by a user's IP address is highly relevant:

because the link was accessed on the same day it appeared on Bulletin Board A, it is at least reasonably probable that the user clicked the link having encountered it on that website.

With this fair assumption, several inferences drop into place to support the magistrate judge's decision to issue the warrant. If one assumes, given the close timing, that the user accessed the link after seeing it on Bulletin Board A, it's fair to conclude that the user also knew it contained child pornography, as that much was explicit from the posting. On top of that, one can fairly conclude that the same person typed the password posted on Bulletin Board A, downloaded the content, and viewed the video contained at that URL. For why else would someone who had seen the pornographic stills and read the description on Bulletin Board A click the link if not to access its contents? Thus, if we suppose that someone accessed the link through Bulletin Board A, it's fairly probable that the same person downloaded or viewed child-pornographic images.

Recall that the magistrate judge knew someone using Bosyk's home IP address had clicked the link. Given that fact—and the permissible inferences described above—we think it was fairly probable that child pornography would be found on computers or other devices within Bosyk's property. And because child pornography constitutes contraband or evidence of a crime, this is all that was needed for probable cause to search Bosyk's house. *See* 18 U.S.C. §§ 2252(a)(4), 2252A(a)(5) (crime to knowingly possess or access with intent to view any video depicting child pornography); *see also, e.g.*, *United States v. Contreras*, 905 F.3d 853, 858 (5th Cir. 2018) (probable

cause to search house based on two child pornography images uploaded to messaging app); *United States v. Richardson*, 607 F.3d 357, 361, 371 (4th Cir. 2010) (same, based on two emailed images); *United States v. Vosburgh*, 602 F.3d 512, 526–28 (3d Cir. 2010) (same, based on attempt to download one video).

We acknowledge that the probability of this particular version of events depends on the link being clicked *after* it was posted on Bulletin Board A. The affidavit doesn't specify what time on November 2, 2015, the post appeared on Bulletin Board A, meaning that the link (which was accessed at 3:23 p.m. that day) could have been clicked before its posting.[4]

This ambiguity, however, is not as fatal to probable cause as our dissenting colleague suggests. As his own analysis shows, it was almost twice as likely that the post preceded the click as the other way around. *See* Dissenting Op. at 43 (Figure A) (showing more than 64% probability that link was clicked after being posted on Bulletin Board A). Thus, the much likelier scenario based on the attested facts was that the link was posted and then accessed hours later (perhaps even sooner) by Bosyk's IP address. That

[4] The government has at times represented or implied that the link was clicked after the post. *See, e.g.*, Appellee's Br. at 4 (stating that link was posted "less than 24 hours earlier" than attempted access). Bosyk has never sought to correct this impression; indeed, his counsel advanced this chronology at oral argument. Oral Arg. at 11:15–11:31 (arguing that click "on November 2 *close after the posting* on Bulletin Board A" did not necessarily evidence knowledge of the password (emphasis added)). Nevertheless, we must "confine our review to the facts that were before the magistrate judge," *Lyles*, 910 F.3d at 791 (quotation omitted), which here do not firmly establish the timeline.

chronology sets in motion the series of plausible inferences described above.[5]

In short, although the search relied on a "single click" of an internet link, the click was to a video of child pornography in circumstances suggesting the person behind that click plausibly knew about and sought out that content. We think the magistrate judge therefore had a substantial basis for concluding that searching Bosyk's address would uncover evidence of wrongdoing.

B.

Arguing otherwise, Bosyk and EFF train their sights on the first inference in this chain of reasoning: that the user at Bosyk's IP address quite probably knew the link contained child pornography. They note that Eyler's affidavit didn't say whether the link existed elsewhere on the internet, or whether the site linked at the URL contained content other than the

[5] It's true that in this version of events, the likelihood that the user at Bosyk's IP address downloaded child pornography hinges on two probabilities combined: first, that he clicked the link after it appeared on Bulletin Board A, and, second, that (if so) he clicked the link having seen it on Bulletin Board A. Contrary to our dissenting colleague's suggestion, however, there's nothing wrong with finding probable cause based on compound probability—provided, of course, that the probabilities taken together establish a fair likelihood of criminal conduct. But more fundamentally, we reject the dissent's apparent premise—that probable cause is subject to rigid statistical analysis. To the contrary, the Supreme Court has told us in no uncertain terms that probable cause isn't subject to precise articulation but is instead a "commonsense, nontechnical" conception dealing with "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Ornelas v. United States*, 517 U.S. 690, 695 (1996) (internal quotation marks and citation omitted).

illegal videos described in the affidavit. And they also point out that the URL didn't indicate what it linked to and that, in general, the act of clicking a URL doesn't prove familiarity with its contents. We do not find these alleged shortcomings fatal to probable cause.

Bosyk's main critique is that the affidavit doesn't establish whether the user who clicked on the link accessed it through Bulletin Board A. He and EFF point out that the affidavit doesn't exclude the possibility that the user might have stumbled upon the link from another, perhaps innocent, source—especially given how easily and frequently links are shared over the internet. This is also the essence of our dissenting colleague's position. *See* Dissenting Op. at 44-55.

The problem with this argument, however, is that it demands more proof than is required to obtain a warrant. Probable cause, as the Supreme Court has reiterated time and again, "does not require officers to rule out a suspect's innocent explanation for suspicious facts." *Wesby*, 138 S. Ct. at 588. Instead, the government needs to demonstrate only a fair probability that contraband or evidence of a crime will be found at the place to be searched. To be sure, innocent reasons may explain why someone accessed a file sharing page containing child pornography. Perhaps (as our friend in dissent posits) someone received the link from a malicious sender, or was looking for innocuous material hosted at the same filesharing webpage, or truly stumbled upon the URL accidentally. But this is all conjecture—no facts in the affidavit suggested the link existed anywhere on the internet but Bulletin Board A. And the possibility

that it did doesn't defeat probable cause when it's fairly probable, given the temporal proximity, that the person clicked on the link because he saw it on Bulletin Board A and wanted to view child pornography.[6]

Indeed, given the nature of the content, we think the magistrate judge had reason to be skeptical about possible innocent explanations. The notion advanced by EFF and accepted by our dissenting colleague that a link containing child pornography would spread throughout the internet like more benign web content seems implausible in light of the present record and the law's experience with online pedophiles. As Eyler's affidavit explained, people who possess and view child pornography often take steps to conceal their contraband material, guard it closely, and sometimes delete it to avoid detection. Cases likewise show that consumers of child pornography frequently employ complex measures to keep their online activities secret. *See, e.g.*, *United States v. McGarity*, 669 F.3d 1218, 1230–31 (11th Cir. 2012) (child pornography ring used elaborate system of encryption, codenames, and hidden instructions to conceal activities from outsiders), *abrogated on other grounds by Paroline v. United States*, 572 U.S. 434 (2014); *Vosburgh*, 602 F.3d at 516–17 (child pornography website used secret gateways and cumbersome links to evade detection). Thus, the likelihood that a specific filesharing page containing child pornography would find its way to somebody

[6] For similar reasons, the possibility that the linked filesharing page also contained innocent material doesn't destroy probable cause. It is undisputed that clicking this unique URL led to at least one video of child pornography, so the circumstances nevertheless warrant suspicion.

uninterested in such contraband—thereby exposing its distributors to detection, capture, and loss of their materials—is probably quite low.

This point bears emphasis. Our dissenting colleague is of course right that Bosyk's IP address could have connected with a link containing child pornography in a variety (though probably not "millions," *see* Dissenting Op. at 44) of different ways. But, contrary to our friend's suggestion, these many possible alternative paths aren't of equal *probability*; rather, the likelier avenues incriminate Bosyk.

In the first place, the facts involve material that, for reasons just explained, is unlikely to travel widely outside child pornography circles. On top of that, there is a suspiciously short interval between such material appearing on a members-only child pornography forum and being accessed by a user at Bosyk's IP address. Given these facts, we believe a magistrate judge could reasonably think it fairly likely—if not most likely— that the user found the link through Bulletin Board A or otherwise received it knowingly from a member of that site. *See* J.A. 169 (explaining that people who possess and view child pornography may "share information and materials" with one another). Contrary to our colleague's suggestion, this belief is not "wholly unsupported speculation," Dissenting Op. at 84; rather, it is based on the contents of the affidavit, the magistrate judge's likely familiarity with online child pornography crimes, and his ability to reach "common-sense conclusions about human behavior." *Gates*, 462 U.S. 231–32 (quoting *United States v. Cortez*, 449 U.S. 411, 418 (1981)).

Bosyk's and EFF's other arguments also miss the mark. They focus, for instance, on the fact that the URL looked like a random string of numbers and letters and therefore betrayed little about its contents. Certainly, the government could have established probable cause more easily had the link been clearer about its illicit content. But here, the URL appeared in a post that described and depicted its contents on the same day that somebody clicked it. This context provides evidence about the probable knowledge and intent of the user that is otherwise lacking from the face of the URL.[7]

EFF and our dissenting colleague's broader arguments against the inferential value of URLs merit the same response. They point out that because URLs are often randomly generated, shortened, or masked, they don't necessarily reveal their contents to the person accessing them. Thus, EFF says, that an IP address accessed a URL associated with contraband doesn't necessarily provide cause to search property and devices related to that address. That may often be true, and in a case based purely on an IP address connecting with a URL, probable cause may be hard to establish absent other incriminating evidence. But that is not the case before us because such evidence exists here: whoever clicked did so on the same day that the link was advertised in a closed forum dedicated to child pornography.

Finally, we are unswayed by the cases Bosyk and EFF rely on. Bosyk draws heavily from *United*

---

[7] And, in a different way, the randomness of the URL helps the government, as internet users aren't likely to type a truly random string of characters into their web browser by mistake.

States v. Reece, an unpublished district court opinion invalidating a warrant issued as part of the same investigation of Bulletin Board A. *See* No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176, at *12–15 (E.D. Va. Mar. 1, 2017). The *Reece* court held that because the affidavit (as here) lacked evidence that the defendant subscribed to or accessed Bulletin Board A, the only possible inference was that he "could have" accessed the video through that website. *Id.* at *12–14. That inference, the court said, was "insufficient to support the resulting search" without the "inferential leap that Defendant *must have accessed* Bulletin Board A to navigate to the illicit material." *Id.* at *14 (internal quotation marks omitted). As we have explained, however, the law doesn't require the government to show that Bosyk "must have" accessed the video via Bulletin Board A; the fair probability that he did so is enough to sustain the search. By suggesting otherwise, the *Reece* court erred.

In any event, *Reece* is distinguishable because, there, two days passed between the post on Bulletin Board A and an attempt to access the link. *See id.* at *5–6. Here, in contrast, those two events happened on the same day. Whether or not the facts in *Reece* supported probable cause, it's notable that the connection between the suspect and Bulletin Board A is much closer in this case. *Cf. United States v. Evans*, No. 16-20292, 2018 WL 1773308, at *3 (E.D. Mich. Apr. 12, 2018) (probable cause to search home when IP address accessed link within 25 hours of being posted on Bulletin Board A).

Both Bosyk and EFF also refer frequently to the Second Circuit's divided decision in *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008). There, the court

invalidated a search warrant based on allegations that the defendant "appeared" to have "either gained access or attempted to gain access" to a website associated with child pornography. *Id.* at 114 (alterations omitted). The majority found that the "inconclusive statements" about whether the defendant accessed the website, combined with the lack of details about the website itself, fell short of establishing probable cause. *Id.* at 121. Concurring in the judgment,[8] Judge Livingston faulted the majority's probable cause analysis for overlooking that the defendant's email address was found on the site, which she (reasonably, in our opinion) thought "probative evidence that Falso visited that website and either signed up or attempted to sign up for a membership." *Id.* at 130–31 (Livingston, J., concurring in part and concurring in the judgment).

We decline to follow *Falso*. That case is distinguishable because there, the affidavit contained "no allegation that [the defendant] in fact gained access" to a website containing child pornography, nor any allegation that "images of child pornography were downloadable from the site." *Id.* at 124 (majority opinion). Here, by contrast, the affidavit alleged that Bosyk's IP address accessed a URL whose content "consisted of four child pornography videos." J.A. 167–68. Thus, the inference that someone at Bosyk's address "in fact accessed a website" sharing child pornography—crucially missing from *Falso*, 544 F.3d at 124—is readily drawn in this case. *See Vosburgh*, 602 F.3d at 526–27 (probable cause to search home

[8] Judge Livingston nonetheless agreed that the government's good faith reliance on the warrant made suppression unnecessary. *See* 544 F.3d at 113, 125–29 (majority opinion).

when IP address clicked link purporting to contain child pornography); *cf. United States v. Martin*, 426 F.3d 68, 75–76 (2d Cir. 2005) (probable cause to search home when email address registered there joined website sharing child pornography); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) (same).

Contrary to the dissent's suggestion, our opinion is not "at odds" with out-of-circuit decisions reviewing search warrants based on online encounters with child pornography. Dissenting Op. at 71. The cases our colleague cites differ factually from this one in meaningful respects, and therefore aren't useful precedents. *See Ornelas*, 517 U.S. at 698. Still, to the extent our sister circuits have at times emphasized "additional facts . . . over and above the single click of a URL that provides for download of child pornography," Dissenting Op. at 71, we are all in tune. Here, an important additional fact is the abbreviated time frame, which lessens the likelihood that Bosyk's IP address accessed the link independently of Bulletin Board A. *Accord, e.g.*, *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006) (en banc) (suspect's paid subscription to child pornography website reduced possibility that visit was accidental).

In sum, the magistrate judge had a substantial basis for finding probable cause to search Bosyk's house given two factual allegations—first, the appearance on Bulletin Board A of a post unambiguously promoting a link containing child pornography videos, and second, an attempt to access that link on the same day by someone at Bosyk's address. The closeness of these two events established a fair probability that child pornography or evidence of attempts to access it would be found in Bosyk's house.

IV.

Alternatively, Bosyk argues that even if Agent Eyler's affidavit established probable cause to search his house in November 2015 when the link was accessed, it didn't permit a search in April 2016 when the warrant issued. "A valid search warrant may issue only upon allegations of 'facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.'" *United States v. McCall*, 740 F.2d 1331, 1335–36 (4th Cir. 1984) (quoting *Sgro v. United States*, 287 U.S. 206, 210 (1932)). Accordingly, Bosyk argues that the warrant was based on "stale" probable cause, and thus invalid, because it issued five months after the underlying events took place.

The existence of probable cause, however, can't be determined by "simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit." *Richardson*, 607 F.3d at 370 (quoting *McCall*, 740 F.3d at 1136). Instead, like probable cause more generally, staleness is judged based on "all the facts and circumstances of the case, including the nature of the unlawful activity" and "the nature of the property to be seized." *Id.*

Importantly for this case, when it comes to child pornography, courts have largely concluded that "even a substantial delay" between download or distribution of child pornography and the issuance of a search warrant doesn't render the underlying information stale. *Id.* This consensus rests, as we explained in *Richardson*, "on the widespread view" that "collectors and distributors of child pornography value their sexually explicit materials highly, rarely if ever dispose of such material, and store it for long

periods in a secure place, typically in their homes." *Id.* (internal quotation marks and citations omitted); *accord United States v. Raymonda*, 780 F.3d 105, 114 (2d Cir. 2015) (staleness inquiry is "unique" in child pornography context); *Gourde*, 440 F.3d at 1072; *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005). It also rests, in many cases, on the fact that digital media files persist for a long time and can often be forensically recovered even after being "deleted." *See Richardson*, 607 F.3d at 370–71; *see also United States v. Seiver*, 692 F.3d 774, 775–78 (7th Cir. 2012) ("'Staleness' is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file.").

As a result, in cases involving online child pornography, courts (including ours) have sustained warrants issued many months, and even years, after the events that gave rise to probable cause. *See, e.g.*, *Contreras*, 905 F.3d at 858–59 (warrant sought 11 months after suspect uploaded two images); *Richardson*, 607 F.3d at 371 (warrant sought four months after suspect emailed child pornography); *Vosburgh*, 602 F.3d at 528 (warrant sought four months after three attempts to access download link); *United States v. Morales- Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (warrant sought three years after last downloads).

In accordance with these cases, Agent Eyler's affidavit described the tendency of "individuals who possess or access with intent to view child pornography" to collect such material and hoard it for a long time. J.A. 168–69. But Bosyk says the inference that child pornography will be found months after

possession or attempted possession applies only when the suspect is plausibly a "collector" of child pornography. And, according to Bosyk, nothing in the affidavit identified him as a "collector."

We agree with Bosyk to the following extent—the value of this inference "depends on the preliminary finding that the suspect is a person interested in images of child pornography." *Raymonda*, 780 F.3d at 114 (internal quotation marks omitted). Such a finding, as the Second Circuit has explained, "tend[s] to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged." *Id.* at 115. Officials may support this inference with, say, information that the suspect paid for access to child pornography, had a history of possessing pornographic images, was an admitted or convicted pedophile, took elaborate steps to access illegal content, or distributed content to others. *Id.* at 114–15 (collecting cases). In each of these cases, it's possible to infer that the suspect is a collector of child pornography because of "circumstances suggesting that he had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *Id.* at 115.

Where we disagree with Bosyk, however, is in applying these principles. We think it was possible to infer from the affidavit that whoever clicked on the link did so willfully and deliberately because he was interested in images of child pornography. Specifically, as we have already explained, the facts in the affidavit support the inference that somebody saw the description and video thumbnails on a website devoted to child pornography, Bulletin Board

A, and then deliberately sought out the video by clicking the link.[9] The magistrate judge could therefore further infer that someone at Bosyk's home likely downloaded, stored, and kept that content, since people "with an interest in child pornography tend to hoard their materials and retain them for a long time." *Vosburgh*, 602 F.3d at 528. We therefore find the warrant valid even though it issued five months after the underlying events took place.

V.

Finally, we note that regardless of the warrant's validity in this case, we would nonetheless affirm as we may not suppress evidence "obtained in objectively reasonable reliance on a subsequently invalidated search warrant." *United States v. Leon*, 468 U.S. 897, 922 (1984).[10]

---

[9] That was not so in *Raymonda*. There, the government sought a warrant based entirely on the fact that, nine months earlier, an IP address had accessed a webpage containing thumbnails of child pornography. Nothing suggested that the suspect discovered the site while searching for child pornography, or that he clicked on the thumbnails to view the full-size images. 780 F.3d at 117. Rather, the facts were "equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window." *Id.* The Second Circuit therefore held that the evidence was too stale to create probable cause.

[10] Principles of judicial restraint often support skipping the probable cause question when *Leon* bars suppression. But "when a Fourth Amendment case presents a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for [a court] to decide the violation issue before turning to the good-faith question." *Gates*, 462 U.S. at 264 (White, J., concurring) (italics omitted). As demonstrated by the divergent decisions of district courts, this is one such case.

Bosyk, however, invokes two exceptions that the Supreme Court has carved out of this rule. First, he argues that the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for [her] reckless disregard for the truth." *Id.* at 923 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)). Second, he and EFF maintain that the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975) (Powell, J., concurring)). Neither exception applies.

The first exception is inapplicable because Bosyk doesn't actually identify any omitted or misstated facts in Eyler's affidavit. Instead, he complains that Eyler *didn't note the absence* of certain facts, such as the lack of any allegation that a user at his IP address was a member of Bulletin Board A, accessed the link through that site, or entered the password displayed there. But we agree with the government that agents need not include disclaimers specifically pointing out facts absent from the affidavit to obtain a warrant. A warrant application is "judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added." *United States v. Allen*, 211 F.3d 970, 975 (6th Cir. 2000) (en banc). Here, the affidavit accurately explained that Bulletin Board A had members, that a URL was posted there, and that an IP address at Bosyk's residence accessed the URL. From these facts, along with the absence of other allegations, the magistrate judge could fairly assess the strength of the government's evidence.

Our dissenting friend believes the affidavit was materially misleading because, in his view, most factual material was unrelated to Bosyk and, therefore, served only to lend the affidavit a false appearance of substance. Dissenting Op. at 90-91 (citing *United States v. Wilhelm*, 80 F.3d 116, 123 (4th Cir. 1996)). This is a blinkered reading of the affidavit. Our colleague apparently believes it "irrelevant," *id.* at 90, that Bulletin Board A was a dedicated child pornography site; that a link appeared on this site next to pornographic images; and that the link contained videos of a girl being sexually abused. True, these facts don't literally "address allegedly unlawful conduct of someone using [Bosyk's] IP address." *Id.* at 91. But as our analysis above makes plain, they are nonetheless crucial to understanding why the government believed Bosyk's home would contain evidence of criminal activity. These details are hardly irrelevant "puffing." *Contra id.*

Neither is the dreaded "boilerplate" about collectors. *But see id.* at 91-92. This information drew on accepted case law and served to establish that Bosyk's computer would contain child pornography (or at least its remnants) some months after the attempted access. Our colleague clearly disagrees with us about whether, at the end of the day, the information in the affidavit established probable cause. But he cannot seriously think these facts are so immaterial to the probable cause inquiry that the sole purpose for their inclusion was to put one over on the magistrate judge. *Cf. Wilhelm*, 80 F.3d at 123 (suppressing evidence when affidavit distracted from lack of probable cause by describing anonymous informant as "a concerned citizen," and "a mature person" with a "truthful demeanor").

Our dissenting colleague would also vacate Bosyk's conviction because of an allegedly omitted fact—the exact timing of the post on Bulletin Board A—that isn't in the record and, for all we know, may not even exist. Dissenting Op. at 93-94. We cannot do so. As our colleague well knows, a defendant can't suppress evidence on grounds that the affiant intentionally or recklessly omitted facts without first making "a substantial preliminary showing" to that effect. *United States v. Tate*, 524 F.3d 449, 454–55 (4th Cir. 2008) (quoting *Franks*, 438 U.S. at 155–56). And, importantly, that showing requires "a detailed offer of proof" of the missing information. *Id.* at 455 (quotation marks omitted); *see also Franks*, 438 U.S. at 171 ("Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained."). Yet despite moving for a *Franks* hearing in the district court, Bosyk never offered proof of *any* omitted fact, nor explained why he couldn't offer such proof. That failure precludes suppression on the basis of intentional or reckless omissions.

Alternatively, Bosyk argues for suppression because, he says, the affidavit lacked any indicia of probable cause. This argument also fails. Suppression on such grounds is "inappropriate" when an affidavit produces "disagreement among thoughtful and competent judges as to the existence of probable cause." *Leon*, 468 U.S. at 926. That's the case here. District court judges have reasonably disagreed on the constitutionality of warrants like this one. *Compare* J.A. 74–79 (probable cause to search home months after IP address accessed link posted on Bulletin Board A), *Evans*, 2018 WL 1773308, at *3 (same), *and United States v. Seitter*,

No. 17-10041-JTM, 2017 WL 4516909, at *3–4 (D. Kan. Oct. 10, 2017) (same), *with Reece*, 2017 U.S. Dist. LEXIS 220176, at *19–20 (no probable cause). And, as evidenced by our separate opinions, the judges on this panel are also divided on the question. In such circumstances, we cannot say that it was objectively unreasonable for the government to rely on the warrant. *Leon*, 468 U.S. at 926 (declining to suppress evidence when court of appeals panel split on probable cause question); *Falso*, 544 F.3d at 128–29 (same).

Accordingly, even if there hadn't been probable cause to search Bosyk's house, suppression would be inappropriate because the government obtained a warrant and reasonably relied on it to execute the search. For this independent reason also, we must affirm the district court's judgment.

VI.

We are sensitive to the privacy interests at stake here. But we also cannot ignore that many crimes are committed with just a few clicks of a mouse—including the very serious crime of downloading child pornography. In cases like this, our job is to ask precisely what "a single click" reveals under the circumstances presented, and whether that information justifies searching a person's most private places for evidence of a crime. Here, the magistrate judge who issued the warrant had a substantial basis for concluding that it did. For that reason, the district court's denial of Bosyk's motion to suppress is

AFFIRMED.

WYNN, Circuit Judge, dissenting:

This case presents a textbook example of why we must guard against the slow whittling away of constitutional rights, particularly as we apply constitutional rights adopted in an analog era to the new challenges of the digital age.

A basic understanding of the technology at issue demonstrates that the government's bare-bones affidavit supporting a warrant to search the residence of Defendant Nikolai Bosyk ("Defendant") failed to establish a fair probability that, when clicking on a link to download child pornography, someone using Defendant's IP address knew and sought out that illicit content. Indeed, rather than confronting the difficult technological questions courts must address in assessing warrant applications premised on online conduct, the majority opinion rests on analog frameworks that fail to account for the meaningful differences between the Internet and the physical world. With due respect to my colleagues in the majority, I believe the majority opinion displays a troubling incomprehension of the technology at issue in this matter. Accordingly, I respectfully dissent.

I.

This matter arose from the government's monitoring of Bulletin Board A, an "Internet-based bulletin board . . . dedicated to the advertisement, distribution and production of child pornography" with over "1500 'approved users.'" J.A. 163–64.

According to an affidavit submitted by the government in support of the challenged search warrant, the government began "observ[ing] various

postings" and "captur[ing] content" on Bulletin Board A in October 2015. J.A. 164; Gov't Br. at 4, 5, 13. On November 2, 2015, a Bulletin Board A member posted on a sub-forum of Bulletin Board A. That post described a particular child pornography video; posted "three different sets of twenty video thumbnail images" of the video; and included a URL[1] composed of a largely random sequence of letters and numbers, described in the affidavit alternatively as "http://[redacted].rar.html" and "http://[redacted].comxu5me9erdipp/brochure.rar.html."[2] J.A. 49.

The affidavit states that the Bulletin Board A post also provided a password, which users could input to access the content of the file associated with that unique URL. Gov't Br. at 5. Without the password, the file could not be opened and viewed. The affidavit does not identify at what time on November 2, 2015, the Bulletin Board A member made the post. And notwithstanding that the government was routinely "observ[ing]" and "captur[ing]" content on Bulletin Board A at that

---

[1] A Uniform Resource Locator, or "URL," "provide[s] Internet users with the ability to access web addresses" and contains "specific protocol information needed by a web browser to direct users to a specific image, file, webpage, program, or other resource on the Internet." Br. *Amicus Curiae* Electronic Frontier Foundation in Supp. of Def.–App. and Reversal ("Amicus Br.") at 7. Absolute URLs include "(1) a protocol designation, (2) a root domain or host name or address, and (3) a file path or resource location." *Id*.

[2] The government represented below that the two URLs reference the same URL, but that the agent "redacted more of the file name" in paragraph 8 than in paragraph 16 of the affidavit. J.A. 49. According to the government, the two URLs are "the same in substance." *Id*.

time, the affidavit does not state whether the URL and password had previously or subsequently been posted on Bulletin Board A or elsewhere on the Internet. J.A. 164; Gov't Br. at 4, 5, 13.

Significant to an understanding of the technology at play in this matter, Bulletin Board A did not host the URL or the content accessible through the URL. Rather, a wholly independent website "offer[ing] online file hosting and sharing services" (such as DropBox, Google Drive, or Apple iCloud)—which the affidavit refers to using the pseudonym "File Sharing Site"—hosted the URL and content. J.A. 165–66; Gov't Br. at 14. File Sharing Site is also used to store and share lawful content.

To that end, File Sharing Site's "Terms of Service" expressly prohibit users from storing or sharing "[p]ornography, nudity, sexual images and any kind of offensive images or videos." J.A. 166. According to the affidavit, law enforcement officers nonetheless had "reason to believe" that File Sharing Site "was used by [Bulletin Board A] members to store files containing child pornography and make them accessible to other members." J.A. 165–66; Gov't Br. at 14. In addition to File Sharing Site, Bulletin Board A members used "several" other "cloud-based storage services" to store and share files "depicting minors engaging in sexually explicit conduct." J.A. 165; Gov't Br. at 6.

Sometime after the November 2, 2015, post, law enforcement officers monitoring Bulletin Board A clicked on the URL, navigated to File Sharing Site, and then downloaded an encrypted video file from File Sharing Site. The officers used the password

provided in the post to open the video file, which depicted child pornography.

Thereafter, the officers obtained an order directing File Sharing Site to disclose business records pertaining to unique URLs containing files that law enforcement knew to depict minors engaging in sexually explicit conduct. In response, File Sharing Site produced the "dates, times, and IP addresses connected to the downloading of the file content associated with the URLs specified in the application for the Order." J.A. 167; Gov't Br. at 6. These records revealed that at 3:23 pm on November 2, 2015, an IP address associated with Defendant's residence was "used to download or attempt to download file content associated with that URL." J.A. 167–68.

The affidavit does not explain what "download" or "attempt to download" entailed. The affidavit does not state that Defendant or anyone likely to be using Defendant's IP address was a member of Bulletin Board A—or had ever even visited Bulletin Board A—and the government subsequently conceded that "membership in Bulletin Board A could not be definitively established." Gov't Br. at 30. Nor does the affidavit state whether someone using Defendant's IP address ever used the password to open the files hosted and shared on File Sharing Site.

In addition to describing the Bulletin Board A investigation and someone using Defendant's IP address to "download or attempt to download" the child pornography stored on File Sharing Site, the affidavit does include several paragraphs describing certain characteristics of "individuals who possess or

access with intent to child pornography"—individuals commonly referred to as "collectors." J.A. 168–69. But the affidavit does not state that Defendant or someone likely to be using Defendant's IP address was a "collector" of child pornography or exhibited any of the particular behaviors associated with collectors set forth in the affidavit.

Based on the foregoing information, on April 8, 2016, the magistrate judge issued a warrant authorizing the government to search Defendant's residence, including any electronic devices found therein. On April 12, 2016, law enforcement officers executed the warrant. A forensic examination of the hard drive of a laptop computer found in Defendant's residence revealed thousands of images and videos of minor children engaged in sexually explicit conduct, in folders created from April 14, 2012, to November 18, 2015.

I note that the majority opinion points out that the video available through the File Sharing Site URL was among the files found on the hard drive of Defendant's laptop. *Ante* at 5–6. But the majority and I agree that fact is irrelevant to the issue at hand because it is well-settled law that what an illegal search ultimately reveals has *no bearing* on whether the evidence the government provided to the magistrate was adequate to establish probable cause to conduct the search in the first place. *Ante* at 6 n.2. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("[I]n determining the lawfulness of entry and the existence of probable cause we may concern ourselves only with what the officers had reason to believe *at the time of their entry*." (citation omitted) (emphasis in original)); *United States v. Di Re*, 332 U.S. 581, 595

(1948) ("We have had frequent occasion to point out that a search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success." (citation omitted)); *Byars v. United States*, 273 U.S. 28, 29–30 (1927) ("Nor is it material that the search was successful in revealing evidence of a violation of a federal statute. A search prosecuted in violation of the Constitution is not made lawful by what it brings to light; and the doctrine has never been recognized by this court, nor can it be tolerated under our constitutional system, that evidences of crime discovered by a federal officer in making a search without lawful warrant may be used against the victim of the unlawful search where a timely challenge has been interposed."); *A.M. v. Holmes*, 830 F.3d 1123, 1139 (10th Cir. 2016) ("Neither the officer's subjective beliefs *nor information gleaned post-hoc* bear on this inquiry." (emphasis added)); *McColley v. Cty. of Rensselaer*, 740 F.3d 817, 841 n.3 (2d Cir. 2014) ("Probable cause is not backward looking. Thus, the results of a search are immaterial to a determination of whether the search was supported by probable cause."); *United States v. Sims*, 553 F.3d 580, 583 (7th Cir. 2009) ("[T]here is a practical reason for requiring warrants where feasible: it forces the police to make a record before the search, rather than allowing them to conduct the search without prior investigation in the expectation that if the search is fruitful a rationalization for it will not be difficult to construct, working backwards." (citation omitted)).

On October 17, 2017, the government filed a criminal complaint against Defendant, alleging one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2). Homeland Security Investigations

Special Agent Kristina Eyler submitted an affidavit in support of the complaint, averring that Defendant's IP address was "associated with a user attempting to download child pornography on Bulletin Board A." J.A. 11. Put differently, Special Agent Eyler's affidavit represented, without qualification, that someone using Defendant's IP address "attempt[ed] to download child pornography on *Bulletin Board A*," *id.* (emphasis added), not File Sharing Site.

On December 14, 2017, a grand jury issued an indictment charging Defendant with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). On January 3, 2018, Defendant filed a motion to suppress all evidence seized during the April 12, 2016, search as well as the fruits of that search. Defendant's motion to suppress argued, in part, that the affidavit provided insufficient evidence to establish probable cause to search Defendant's residence because it failed to establish a fair probability that someone using Defendant's IP address navigated through the URL posted on Bulletin Board A to the contraband stored on File Sharing Site. *See, e.g.*, J.A. 27 ("The instant affidavit contains no information or contentions as to [Defendant]'s involvement, access, or membership to Bulletin Board A. In fact, the affidavit makes no contention that the subject URL, purportedly containing child pornography, could have only been accessed through Bulletin Board A.").

In its opposition to Defendant's motion to suppress, the government claimed that the affidavit did, in fact, connect Defendant's IP address to the

Bulletin Board A post given "the close proximity in time between the posting at Bulletin Board A and attempt to download *its* child pornographic content." J.A. 45 (emphasis added). By characterizing the content as the property of Bulletin Board A—not as content stored by File Sharing Site—the government invited the district court to not draw a distinction between Bulletin Board A and File Sharing Site, notwithstanding that the affidavit connected Defendant's IP address with *only* File Sharing Site, not Bulletin Board A.

Additionally, an unstated, but essential, premise of the government's temporal proximity argument was that someone using Defendant's IP address attempted to download the child pornography from File Sharing Site *after* the Bulletin Board A post prompting the investigation—a premise that the government invited the district court to indulge by relying on a case in which a district court found probable cause to issue a warrant when the allegations in the affidavit established that the download of contraband occurred soon *after* a link to the contraband was posted to a child pornography message board. *See* J.A. 45 (citing *United States v. Evans*, 2:16-cr-20292, Doc. No. 69, report and recommendation, at 14 (E.D. Mich. Nov. 20, 2017). The government further rejected Defendant's argument that the File Sharing Site URL "could have been accessed through innocent means" because "there was no reason for the agent to believe the link was available anywhere other than on Bulletin Board A." J.A. 44–45.

On February 2, 2018, the district court denied Defendant's suppression motion. Ruling from the

bench, the district court accepted the key factual premises relied on by the government to connect Defendant's IP address with Bulletin Board A:

> What is clearly in the affidavit is that Bulletin Board A is a dedicated bulletin board to advertising distribution and production of child pornography and that it therefore, already anybody who might be on that site, there would be a reasonable belief that that person was interested in accessing that kind of information.
>
> Then there was the posting of that particular section [of Bulletin Board A] that was clearly advertising video clips of what would absolutely be unequivocally child pornography, and the critical fact . . . is that the same day that posting went up, the URL that is linked—or the IP address that is linked to a computer in the defendant's home . . . attempts to or at least shows an interest in [Bulletin Board A]. In my view, that's enough for probable cause to believe that there would be a computer in that residence that would have child pornography on it.

J.A. 76–77. In other words, in accordance with the government's invitation, the district court drew no distinction between Bulletin Board A and File Sharing Site and presumed that someone using Defendant's IP address clicked on the URL navigating to the child pornography stored on File Sharing Site *after* seeing the URL posted on Bulletin Board A.

But the majority maintains that it is "unclear" whether the district court was referring to Bulletin Board A or File Sharing Site because the district court could have been referring to File Sharing Site, rather than Bulletin Board A when it referred to "both the 'posting' and 'the URL that is linked.'" *Id.* That reading is simply implausible. Clearly, the district court did not refer to the Bulletin A Board "posting" and the "URL that is linked" as two separate websites, *i.e.*, Bulletin Board A and File Sharing Site. Instead, the district court stated that on the "same day that *posting* went up, the *URL that is linked*—or the IP address that is linked to a computer in the defendant's home . . . attempts to or at least shows an interest in *that particular site*." J.A. 76–77 (emphases added). The district court therefore considered both the "posting" and the "URL that is linked," *on Bulletin Board A*, to be referencing a single website: Bulletin Board A. The district court discussed the URL only in the context of it being *linked* on Bulletin Board A, rather than it being *hosted* by File Sharing Site. Accordingly, the district court incorrectly assumed that Defendant's IP address demonstrated an interest in Bulletin Board A.

In short, the district court did not expressly contemplate the possibility that someone using Defendant's IP address navigated to the URL by any means other than the Bulletin Board A post. Defendant timely appealed the denial of his suppression motion.

II.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses,

papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. It represents the Framers' "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014).

Recognizing that the advent of new technology—like the Internet and the ability to store vast amounts of information in small electronic devices—"enhance[s] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court has rejected "'mechanical interpretation[s]'" of the Fourth Amendment that would allow the government to "capitalize" on such technology to invade the reasonable expectations of privacy and security protected by that Amendment. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001)). Rather, when applying the Fourth Amendment in the context of new or advancing technology—like the URL click at issue in this case—courts must seek to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* (quoting *Kyllo*, 533 U.S. at 34).

In doing so, courts must keep in mind at least two basic Fourth Amendment "guideposts"—that the Amendment seeks "to secure the privacies of life against arbitrary power" and "to place obstacles in the way of a too permeating police surveillance." *Id.* (internal quotation marks and citations omitted).

That is particularly true when, as here, the government seeks authority to search a home because, "when it comes to the Fourth Amendment, the home is first among equals." *Florida v. Jardines*, 569 U.S. 1, 6 (2013).

"Although the text of the Fourth Amendment does not specify when a search warrant must be obtained," the Supreme Court repeatedly has recognized that "'[i]t is a basic principle of Fourth Amendment law . . . that searches and seizures inside a home without a warrant are presumptively unreasonable.'" *Kentucky v. King*, 563 U.S. 452, 459 (2011) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). Warrants are "constitutionally sound when issued by a neutral magistrate and supported by probable cause." *United States v. Montieth*, 662 F.3d 660, 664 (4th Cir. 2011); *see* U.S. Const. amend. IV. The government bears the burden of demonstrating probable cause to support a search warrant. *See, e.g.*, *id.* at 665; *Walczyk v. Rio*, 496 F.3d 139, 161 (2d Cir. 2007); *United States v. Abboud*, 438 F.3d 554, 569 (6th Cir. 2006).

To determine whether a warrant is supported by probable cause, a magistrate must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit[,] . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 231, 238 (1983). When a magistrate judge issues the challenged warrant, this Court must determine "whether the magistrate judge had a 'substantial basis' for finding probable cause." *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018). Accordingly, the question before this Court is

whether, based on the information set forth in the affidavit, the magistrate judge had a "substantial basis" for finding that there was a "fair probability" that contraband or evidence of a crime would be found within Defendant's residence.

A.

The majority opinion concludes—and I agree—that even a "single click" of an internet link to download[3] child pornography can provide probable cause to support a search warrant *if* the facts set forth in the warrant application establish that "the person behind that click plausibly knew about and sought out that content." *Ante* at 11. According to the majority opinion, the affidavit established that someone using Defendant's IP address "plausibly knew" that the URL linked to child pornography because the November 2, 2015, post on Bulletin Board A, in which a copy of the URL appeared, "contain[ed] text and images that unequivocally identified its contents as child pornography." *Id*. at 8. The majority opinion's finding of probable cause, therefore, rests entirely on the premise that the affidavit established a fair probability that someone using Defendant's IP address "clicked the link having encountered it on [Bulletin Board A]." *Id*. at 9.

That factual premise finds no direct support in the materials considered by the magistrate judge in

[3] I take no position on whether evidence that someone using a particular IP address clicked on a link navigating to a website that *displays* child pornography—as opposed to a link to *download* child pornography—can provide probable cause to search a residence associated with that IP. *See United States v. Falso*, 544 F.3d 110, 124 (2d Cir. 2008).

granting the warrant. The affidavit does not assert that Defendant, or someone likely to be using Defendant's IP address, was a member of Bulletin Board A. Indeed, the government conceded that it could not establish whether Defendant or someone using his IP address was a member of Bulletin Board A. Gov't Br. at 30.

The affidavit also does not provide any direct evidence that Defendant or someone using Defendant's IP address had ever visited Bulletin Board A. On the contrary, the government conceded before the district court that because Bulletin Board A "was only accessible on the dark web via a special web-browser called TOR," it could not provide an electronic record establishing whether Defendant's IP address ever visited Bulletin Board A. J.A. 37–38.

Instead of relying on direct evidence, the government contends, as it did before the district court, that circumstantial evidence makes it fairly probable that someone using Defendant's IP address navigated through the Bulletin Board A post to attempt to download the child pornography hosted by File Sharing Site. In support of that argument, the government's brief makes several representations.

First, the government repeatedly represents that the post appeared on Bulletin Board A *before* someone using Defendant's IP address sought to access the child pornography stored by File Sharing Site. Gov't Br. at 4 ("On November 2, an IP address that resolved back to [Defendant]'s residence was recorded to trying to access a link containing child pornography that had been posted on Bulletin Board A *less than 24 hours earlier*." (emphasis added)); *id.* at

30 ("The short duration *from* when the link appeared on Bulletin Board A *until* someone at the defendant's residence clicked on the link established a fair probability that the link had been accessed through Bulletin Board A." (emphases added)).

Second, the government represents that the "link . . . *originated* on a dark web forum dedicated to sharing child sexual abuse content," *id.* at 10–11 (emphasis added), meaning Bulletin Board A. *See also id*. at 9 ("Probable cause existed to search [Defendant]'s home on April 12, 2016, because law enforcement determined that a computer at [Defendant]'s residence accessed a link to downloadable child pornography, *which originated on a website that caters to individuals seeking child pornography*." (emphasis added)). That "originat[ion]" contention serves to reinforce the government's assertion that someone using Defendant's IP address attempted to download the child pornography from File Sharing Site *after* encountering the URL on Bulletin Board A—if the URL "originated" on Bulletin Board A, then someone using Defendant's IP address had to have clicked on the URL *after* it appeared on Bulletin Board A.

For two principal reasons, the government's temporal proximity argument fails to establish a fair probability that someone using Defendant's IP address navigated to the URL via the post in Bulletin Board A. First, the government's temporal proximity argument rests on the "critical fact" that someone using Defendant's IP address clicked on the URL *after* the post containing the URL appeared on Bulletin Board A—a premise that the government repeatedly asserted in its briefing and argument to the district

court and this Court. But if that "critical fact" lacks support—if the click on the URL occurred before the post on Bulletin Board A—then the person using Defendant's IP address could not have encountered the URL on Bulletin Board A, and therefore could not have viewed the text and images in the Bulletin Board A post indicating the URL linked to child pornography.

That is the case. Contrary to the government's repeated representations in its briefing, the affidavit does not assert, much less establish, that someone using Defendant's IP address clicked the URL *after* the post containing the URL appeared on Bulletin Board A. On the contrary, whereas the affidavit reports the time someone using Defendant's IP address clicked on the File Sharing Site URL—3:23 pm on November 2, 2015—it does not report at what time that day the post first appeared on Bulletin Board A. Rather, it simply states that the post appeared on Bulletin Board A sometime on November 2, 2015. Accordingly, the post could have appeared on Bulletin Board A anytime within a window of 8 hours, 37 minutes *after* someone using Defendant's IP address downloaded or attempted to download the child pornography from File Sharing Site.

Significantly, notwithstanding that the government represented to both this Court and the district court that—as a matter of fact, not inference—the Bulletin Board A post appeared *before* someone using Defendant's IP address attempted to download the child pornography from File Sharing Site, the affidavit nowhere addressed whether the government knew, or could have known, the time of the Bulletin Board A post as a result of its ongoing

observation and capturing of content on Bulletin Board A. Gov't Br. at 13. Indeed, the government never has explained to this Court or the district court why the repeated representations in its briefing as to the sequence of events does not find direct support in the facts set forth in the affidavit it submitted with the warrant application. Of course, in assessing probable cause, we do not look to the representations the government makes after the fact, but the facts the government presented to the magistrate.

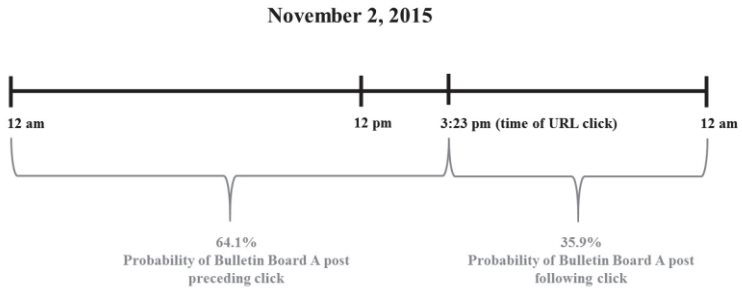
Because the government's circumstantial causation argument rests on the attempted download from File Sharing Site occurring after the post appeared on Bulletin Board A, the government's failure to establish that sequence of events fatally undermines its effort to rely on temporal proximity as a circumstantial basis for proving that someone using Defendant's IP address navigated to the URL through Bulletin Board A.

Notwithstanding this fatal flaw, the majority opinion accepts the government's temporal proximity argument—and the government's crucial factual representations underlying that argument—hook, line, and sinker. Although the majority recognizes that the affidavit does not establish whether the Bulletin Board A post preceded the "attempted download" by someone using Defendant's IP address, it nevertheless contends that the "critical *fact*" supporting probable cause is "[t]he close timing between the link's appearance on Bulletin Board A and the click by a user's IP address." *Ante* at 8–9 (emphasis added). According to the majority, "because the link was accessed on the same day it appeared on Bulletin Board A, it is at least reasonably probable

that the user clicked the link having encountered it on that website." *Id*. at 9. Yet, even as it acknowledges that the affidavit failed to establish the "critical fact" supporting its theory of probable cause, the majority opinion nevertheless accepts that theory wholesale. *See id*. at 10 ("That chronology [of the URL click following the Bulletin Board A post] sets in motion the series of plausible inferences described above.").

Notably, the majority opinion distinguishes that "critical fact"—that the click occurred *after* the appearance of the Bulletin Board A post—from the "inferences" it draws from that fact—most notably, that someone using Defendant's IP address encountered the link in the Bulletin Board A post, not via some other electronic pathway. *Ante* at 8–9, 12 (reasoning that "it's fairly probable, given the temporal proximity, that the person clicked on the link *because he saw it on Bulletin Board A and wanted to view child pornography*" (emphasis added)). Put differently, rather than relying on an inference from an established fact, the majority opinion impermissibly draws inferences on inferences to uphold the warrant. *See Rosencranz v. United States*, 356 F.2d 310, 317 (1st Cir. 1966) (noting that a magistrate may not "reach for external facts and . . . build inference upon inference in order to create a reasonable basis for his belief that a crime is presently being committed"). The majority opinion therefore improperly draws an inference of causality based on a sequence of events the government failed to establish. *See* Figure A (illustrating the 35.9% probability that the Bulletin Board A post followed the IP address's click of the URL).

Figure A



But that is not the only flaw with the temporal proximity argument advanced by the government and embraced by the majority opinion. The government's temporal proximity argument also rests on the wholly unsupported premise that—even if someone using Defendant's IP address had clicked on the File Sharing Site URL after the post appeared on Bulletin Board A (which, again, the affidavit does not establish)—the user navigated to the URL through the post appearing on Bulletin Board A. Indeed, the facts set forth in the affidavit fail to address, much less rule out, a multitude of ways someone using Defendant's IP address could have navigated to the File Sharing Site URL without encountering the URL on Bulletin Board A, and therefore without observing the text and images that would have put that person on notice of the download link's content. The majority nowhere meaningfully contemplates the significance of this internet technology in our role to assess probable cause.

To begin, users can *encounter* URLs, or hyperlinks to URLs,[4] in myriad ways— including through websites, emails, chats, text messages, comment threads, discussion boards, File Sharing Sites (such as DropBox, Google Drive, or Apple iCloud), tweets, Facebook posts, Instagram captions, Snapchat messages, embedded images or videos, unwanted pop-up windows, any combination thereof, or by any other digital means. And because a URL, or a hyperlink to a URL, can be copied with only a click of a button, a single URL can be copied and further disseminated through any or all of these ways millions of additional times, often in a matter of seconds.

Thus, it is no exaggeration to state that URLs, or hyperlinks to URLs, can be posted and disseminated millions of times anywhere by anyone. Take for example, the trailer for the movie *Avengers: Endgame*—which was shared through multiple online platforms such as YouTube, Facebook, and Twitter—was viewed 289 million times in the first 24 hours after it was posted online. Todd Spangler, *'Avengers: Endgame' Trailer Smashes 24-Hour Video Views Record*, Variety (Dec. 8, 2018, 11:02 a.m.), https://variety.com/2018/digital/news/avengers-endgame-record-trailer-worldwide-24-hour-views-1203085074; *see also Crosby v. Twitter, Inc.*, 921 F.3d 617, 625 (6th Cir. 2019) (citing sources

[4] "The definition of a hyperlink is text or an image within a file on your computer that you can click on that gives access to another document or image. Words on a website that are underlined and highlighted in blue and that you can click on in order to open a new web page are an example of a hyperlink." *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 373 n.2 (E.D.N.Y. 2015) (citation omitted).

observing that "third parties upload 300 hours of content to YouTube every minute" and Twitter "boasts hundreds of millions of users . . . with over 500 million tweets per day . . . [or] 6,000 tweets per second" (citations omitted)); Chloe Taylor, *A Japanese Billionaire Now Has Most Retweeted Tweet Ever After Offering a $923,000 Prize*, CNBC (Jan. 7, 2019) (reporting that a single tweet—only one of the numerous online vehicles for sharing a URL—was retweeted nearly five million times in a two-day period), https://www.cnbc.com/2019/01/07/yusaku-maezawa-has-most-retweeted-tweet-ever-after-offering-923000.html. In this matter, none of the facts alleged in the affidavit rule out any of these potentially millions of alternative paths—wholly unconnected to the Bulletin Board A post—through which someone using Defendant's IP address could have encountered the URL navigating to the child pornography on File Sharing Site.[5]

---

[5] Relatedly, the *content* to which a URL navigates and the *link* itself could "originate[]" in numerous places. Because electronic content often can be easily duplicated and stored, content that first appears at one URL may appear, in short order or over a longer time horizon, at numerous other URLs and may be stored on numerous other servers. Therefore, just because a URL, or a hyperlink to a URL, appears on one webpage, like Bulletin Board A, does not mean that the content associated with that URL first appeared on the webpage. For this reason, the government's repeated representation that the child pornography hosted on File Sharing Site "originated" on Bulletin Board A finds no support in the affidavit, which establishes only that a URL navigating to at least one website hosting the content, File Sharing Site, appeared on Bulletin Board A. It is entirely consistent with the facts set forth in the affidavit that the child pornography originated some place other than Bulletin Board A, meaning that the affidavit provides little factual support for the government's theory of causation—that someone

Additionally, users can *navigate* to a URL in numerous ways beyond clicking on a link included in a post on a particular webpage, like Bulletin Board A. For example, a user could click on a copy of the URL posted to another website, click on a bookmark, type the URL directly into a browser's navigation bar, or click a hyperlink in an email or a news article, to name only a few. *See generally* Amicus Br. at 8. That is particularly true when the URL navigates to a site on the normal Internet, like File Sharing Site, as opposed to a site, like Bulletin Board A, that can only be reached using a specialty browser, like Tor.

The majority opinion maintains that the "randomness of the URL" in this case— which contains a string of letters and numbers with no discernible pattern or meaning— "helps the government, as internet users aren't likely to type a truly random string of numbers and letters into their web browser by mistake." *Ante* at 15 n.7. That assertion— that someone using Defendant's address *typed* the URL into a web browser—contradicts the probable cause theory advanced by the government and otherwise relied on in the majority opinion—that someone using Defendant's IP address intentionally *clicked* on the URL in the Bulletin Board A post because they believed it led to child pornography.

Additionally, the randomness of the URL weighs against a finding of probable cause because it

---

using Defendant's IP address likely learned of the child pornography through Bulletin Board A. Indeed, that the child pornography videos at issue were hosted on File Sharing Site—not Bulletin Board A—provides evidence that the child pornography—a link to that child pornography—*did not* "originate[]"] on Bulletin Board A.

increases the likelihood that someone using Defendant's IP address clicked on the URL without knowing the content to which it navigated. Even assuming the user actually saw the URL—which, as explained below, is not necessarily the case— the random sequence of letters and numbers would provide a user with no indication that the URL navigated to child pornography. And most significantly, the majority opinion's myopic focus on one method of navigating to a URL—typing the URL into a browser— again ignores the multitude of other equally plausible—and likely far more plausible—ways someone using Defendant's IP address could have navigated to URL, none of which ways the facts set forth in the affidavit rule out.

Importantly, users can *unintentionally navigate* to URLs because—as is the case with the URL clicked by someone using Defendant's IP address—URLs frequently do not provide any external indication of the content to which they navigate. For example, services like YouTube and DropBox generate random URLs that provide no information about their underlying content. Amicus Br. at 10. Other services, like Bitly, TinyURL, and Perma shorten URLs, which may otherwise provide external indicators of their content, to generic URLs that include a standard URL base, such as "https://bit.ly/," "https://tinyurl.com/," or "https://perma.cc/," followed by a random string of alphanumeric characters. *See generally* Robin Camille Davis, *The Future of Web Citation Practices*, 35 Behav. & Soc. Sci. Libr. 128–34 (2016) (explaining different URL shortening services). Such generic URLs offer no indication of the content to which they navigate.

Link shortening and disguising often serve beneficial purposes by, for example, permitting distribution of password-protected files, facilitating the sharing of less clunky links, or permitting simpler citation styles. And link shortening and disguising can serve other innocuous purposes. URL spoofing, for example, permits one user to disguise a hyperlink as directing to specific content or a particular website, while in reality directing the unwitting user to a distinct website altogether. *See* Amicus Br. at 12.

One humorous form of URL spoofing is "rickrolling," one of the "Internet's oldest memes," in which individuals click on a link "expecting one thing" but are instead led to "a video of Rick Astley singing 'Never Gonna Give You Up.'" Abby Ohlheiser, *I Can't Believe This Is Why People Are Tweeting Fake Celebrity News*, Wash. Post (Oct. 18, 2018), https://www.washingtonpost.com/technology/2018/10/18/i-cant-believe-this-is-why- people-are-tweeting-fake-celebrity-news/?utm_term=.e9c493b7234d. The unsuspecting individual who follows the disguised URL is said to be "rickrolled." In fact, "rickrolling" has become such a mainstream online practice that in the lead-up to the 2018 midterm elections, an online campaign aimed to "rick roll" unregistered voters into registering to vote. *Id.*

As the *Washington Post* described, doing so was easy:

> First, create a link to vote.org (or whatever else you want to trick people into visiting) using a link shortener such as bit.ly. Bit.ly works pretty simply: You enter in a URL, and the site spits out a

> shorter version. It's a relic from a time when URL length counted toward characters on Twitter but is now used to hide the original source of links.

Id. Then, "choose the right piece of gossip," such as news of a celebrity couple split, and tweet out an attention-grabbing headline alongside the disguised Bit.ly link leading to the voter registration website. *Id*. Thus, with a few clicks, anyone—even users with no advanced computational skills—can disguise a link and lure an unsuspecting user to click that link. In such circumstances, the user would learn of the content to which the URL navigates only *after* clicking on the link.

But link shortening and disguising are also used for malicious purposes. URL spoofing can enable "phishing," which redirects a user to a facially legitimate, but fake, website in order to steal the user's personal information. A "decent fake website," which a "phisher" can set up with little difficulty, provides the phisher with complete access to the user's information and computer without "expensive and detectable malware." Quinn Norton, *Phishing Is the Internet's Most Successful Con*, Atlantic (Sept. 12, 2018), https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-successful-con/569920; *see also* Jonnelle Marte, *Can You Tell the Real TurboTax Email from the Scam?*, Wash. Post (Mar. 1, 2016), https://www.washingtonpost.com/news/get- there/wp/2016/03/01/can-you-tell-which-of-these-turbotax-emails-is-real-and-which-one-is-from-a-scam-artist/?utm_term=.7ba2976355cb.

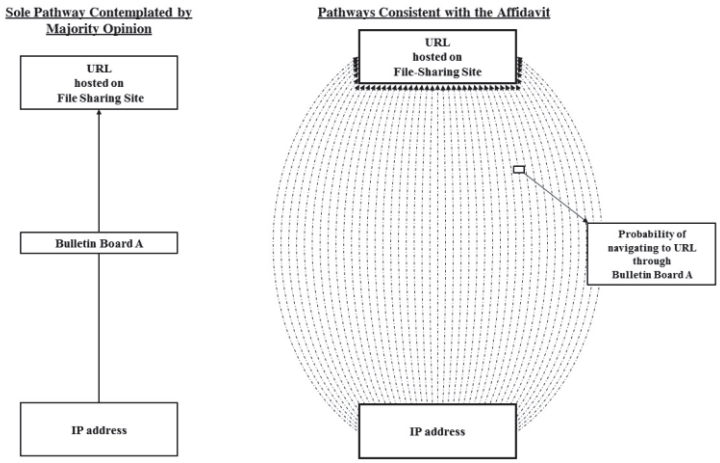
Of particular relevance, bad actors can, and have, innocuously disguised links to child pornography and then sought to extort internet users who inadvertently navigate to the child pornography by clicking on the disguised links. *See, e.g.*, Adam Levin, *The 5 Deadly Clicks: The Links You Should Never Touch*, ABC News (Oct. 6, 2013), https://abcnews.go.com/Business/links-click/story?id=20461918 (detailing a Russia-based extortion scheme in which unsuspecting users clicked a link to child pornography). Again, none of the facts in the affidavit address, much less rule out, the numerous possible ways in which someone using Defendant's IP address could have unintentionally navigated to the File Sharing Site URL hosting the child pornography.

The majority opinion adverts to one of the many alternative paths through which someone using Defendant's IP address could have navigated—intentionally or unintentionally—to the File Sharing Site URL, acknowledging that Defendant's IP address may have "received [the link] knowingly from a member of [Bulletin Board A]," rather than "f[i]nd[ing] the link through Bulletin Board A." *Ante* at 13. But the majority opinion fails to recognize that this alternative path, by itself, materially undermines its theory of probable cause. If someone using Defendant's IP address did not encounter and navigate to the File Sharing Site URL through the Bulletin Board A post, then that person did not have an opportunity to observe the text and pictures in the post indicating the nature of the content to which the URL navigated. As the majority opinion concedes, absent a fair probability that someone using Defendant's IP address "clicked the link knowing that

it contained child pornography"—which would not necessarily be the case if Defendant "received [the link] knowingly from a member of [Bulletin Board A]"—then there is no basis to find probable cause. *Ante* at 8, 14.

In sum, there are myriad ways users can encounter and navigate to a URL— including unintentionally, particularly when, as here, the text of the URL provides no indication as to the nature of the content to which it navigates. Accordingly, even if the Bulletin Board A post preceded the attempt by someone using Defendant's IP address to download child pornography from File Sharing Site—again, a fact not established by the affidavit—there are potentially millions of paths through which someone using Defendant's IP address could have encountered and navigated to the File Sharing Site URL hosting the child pornography other than through Bulletin Board A. Put simply, the affidavit does not establish the probability of the single sequence of events upon which the majority opinion relies—that someone using Defendant's IP address navigated to the File Sharing Site URL after encountering it on Bulletin Board A. *See* Figure B (contrasting the majority opinion's myopic focus on one pathway between Defendant's IP address and the File Sharing Site URL with the myriad pathways, only some of which are reflected by the dashed lines, consistent with the affidavit).

Figure B



The majority acknowledges that the probability of the IP address accessing the URL through Bulletin Board A "depends on the link being clicked *after* it was posted on Bulletin Board A" and that the affidavit does not specify the timing of the Bulletin Board A post. *Ante* at 10. But, in the majority's view, the "ambiguity" regarding the timing of the Bulletin Board A post is not fatal to a probable cause finding because it "was still almost twice as likely that the post preceded the click as the other way around." *Id*. (citing Figure A). Therefore, the majority opinion maintains, "the much likelier scenario" was that the Bulletin Board A post preceded the URL click and was therefore accessed by Defendant's IP address through Bulletin Board A. *Id*. at 10.

However, the majority's analysis ignores that the probability that the Bulletin Board A post preceded the File Sharing Site URL click is only one of several layers of uncertainty governing the

likelihood that someone using Defendant's IP address accessed the File Sharing Site URL through the Bulletin Board A post. Put simply, assessing whether it is fairly probable that Defendant's IP address navigated to the URL via Bulletin Board A involves a compound probability,[6] governed by the probabilities of at least two independent events: first, whether the Bulletin Board A post preceded the URL click, *and* second, whether Defendant's IP address encountered the URL through the Bulletin Board A post. Stated formulaically,

P{Navigated to URL via Bulletin Board A}	=	*P{Bulletin Board A Post Preceded Click} * P{Encountered Link on Bulletin Board A}*
$0.641x$	=	$.641 * x$

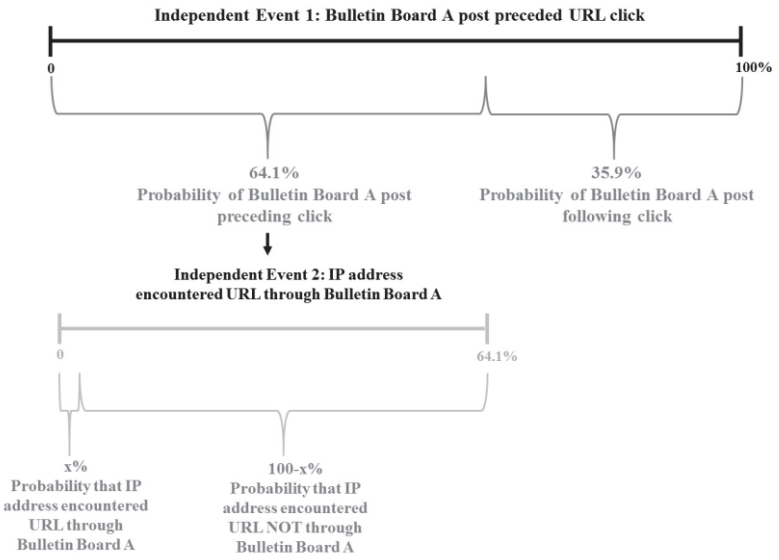
$x \leq 1$

As to the first event, there is a 64 percent chance that the Bulletin Board A post temporally preceded the URL click. *See supra* Figure A. And as to the second event— whether Defendant's IP address accessed the File Sharing Site URL through the Bulletin Board A post—the affidavit provides no facts that in any way circumscribe the massive universe of paths someone using Defendant's IP address could have taken to the URL, meaning that that

[6] Compound probability is a "mathematical term relating to the likeliness of two independent events occurring" and is "equal to the probability of the first event multiplied by the probability of the second event." *Compound Probability*, Investopedia (Apr. 29, 2019), http://www.investopedia.com/terms/c/compound-probability.asp.

probability, under the facts set forth in the affidavit, is necessarily vanishingly small. *See* Figure C.

Figure C



Without additional facts further limiting the universe of possibilities, we cannot know whether it is fairly probable that the IP address encountered the URL through Bulletin Board A. All but one of these potentially millions of the paths to the File Sharing Site URL do not involve the factual scenario that the majority opinion, at the government's urging, credulously accepts—that someone using Defendant's IP address encountered the URL in the November 2, 2015, post on Bulletin Board A and, using the link in that post, sought to download the child pornography shared on File Sharing Site.

The majority opinion glosses over these myriad alternative paths of accessing the URL because in its

view, these "aren't of equal probability; rather, the likelier avenues incriminate [Defendant]." *Ante* at 13. The majority opinion claims that the "avenue[]" advanced by the government—that someone using Defendant's IP address clicked on the File Sharing Site URL after encountering it in the Bulletin Board A post—is "likelier" because the "likelihood that a specific filesharing page containing child pornography would find its way to somebody uninterested in such contraband . . . is probably quite low." *Id.*

But the majority opinion identifies no facts in the affidavit supporting its bald assertion that it is unlikely that a user would innocently access child pornography. Instead, it first cites to the affidavit's boilerplate language regarding the characteristics of individuals who "collect" child pornography. The Fourth Amendment permits courts to rely on "the affiant-officer's experience" and knowledge regarding given crimes only when the affidavit contains sufficient evidence linking an individual to that crime. Wayne R. LaFave, 2 Search & Seizure § 3.7(d) (5th ed. 2018). For example, because it is "merely common sense that a drug supplier will keep evidence of his crimes at his home," at least one court has found that informant statements, as well as corroborating record evidence, setting forth "sufficient evidence" that a defendant was a drug supplier supported probable cause to search the supplier's home. *United States v. Sanchez*, 555 F.3d 910, 914 (10th Cir. 2009). But when individualized information connecting an individual to a crime is absent, an affiant—much less a court—cannot rely on generalized, boilerplate assumptions about criminal habits. *See United States v. Underwood*, 725 F.3d 1076, 1082–83 (9th Cir. 2013)

(concluding that a trio of facts—a detective's observation of a personal-use sized baggie of marijuana at a suspect's home, the suspect's one-time delivery of two crates to drug traffickers, and the affiant's claims based on "experience and training" regarding the general habits of drug traffickers—could not support a finding of fair probability that drug trafficking evidence would be found at defendant's home).

Here, like *Underwood*, the majority opinion relies on the affidavit's explanation of the generalized habits of collectors of child pornography but points to no individualized facts in this case demonstrating that someone using Defendant's IP address was, in fact, a collector of child pornography. *Ante* at 13. For example, the affidavit does not allege that someone using Defendant's IP address viewed or possessed child pornography—or even successfully downloaded the illicit content associated with the URL—let alone that the IP address had ever accessed Bulletin Board A.

Ultimately, the majority's reasoning is circular: the IP address must have accessed the URL through Bulletin Board A because the IP address was associated with a collector of child pornography, and in turn, the IP address must be associated with a collector of child pornography because the IP address accessed the URL through Bulletin Board A. But without any affidavit evidence suggesting that the IP address in fact accessed the URL through Bulletin Board A or any evidence demonstrating that the IP address belonged to a collector of child pornography, the majority opinion cannot permissibly rely on the generalized habits of those who view and possess child pornography.

Moreover, even if the majority could permissibly rely on the affidavit's boilerplate language in this case, that language does not describe the sharing habits of child pornography collectors or the "complex measures" used to conceal their online activities, and therefore that language has no bearing on the likelihood of an innocent user accessing child pornography inadvertently. *Ante* at 13. Indeed, the fact that the government elected not to include such language is telling. The template for search warrants in child pornography cases used by law enforcement officers in the Bulletin Board A investigation directs affiants that they should include boilerplate "collector" information in an affidavit "ONLY if" the affiant can "tie [collector] characteristics to the specific offender." *United States v. Reece*, No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176, at 22 (E.D.Va. Mar. 1, 2017). Accordingly, the government's decision not to include boilerplate language related to the "complex" sharing habits of child pornography collectors indicates that even it did not believe the evidence supported inclusion of those boilerplate facts and therefore the inferences drawn by the majority opinion. *Ante* at 13.

In support of its assertion that the "likelihood that a specific filesharing page containing child pornography would find its way to somebody uninterested in such contraband . . . is probably quite low," *id.*, the majority opinion further relies on two out-of-circuit cases to show that "consumers of child pornography frequently employ complex measures to keep their online activities secret," and therefore that it is unlikely that someone uninterested in child pornography could, or would, access the URL in question. *Ante* at 12–13 (citing *United States v.*

McGarity, 669 F.3d 1218, 1230–31 (11th Cir. 2012), *abrogated on other grounds by Paroline v. United States*, 572 U.S. 434 (2014); *United States v. Vosburgh*, 602 F.3d 512, 516–17 (3d Cir. 2010)).

But both of these cases—neither of which was referenced by the government in the affidavit—involve materially different facts from those at issue here. *McGarity* dealt with a complex online ring of child pornography users, which used codenames, encryption, and other methods of subterfuge to conceal their activities. 669 F.3d at 1229–31. And *Vosburgh* involved an online message board that directed users to child pornography using constantly changing gateway websites, complicated access instructions, and "cumbersome URLs." 602 F.3d at 516–17.

Unlike *McGarity* and *Vosburgh*, the affidavit in this case contains no analogous case-specific evidence of a complex child pornography network relying on complicated electronic concealment and security measures. Instead, it documents a single click by an unspecified user of a particular IP address of a URL containing illicit content. And even if the facts of those cases were in any way analogous to the facts set forth the affidavit— which they were not—the government elected not to reference those cases, or even the type of conduct at issue in those cases, in its warrant application. Warrant applications do not implicitly incorporate, without reference, the entire Federal Reporter. Rather, the government is obligated to put the relevant, case-specific facts in the affidavit to support probable cause. It simply failed to do so here.

Additionally, the approach taken in the majority opinion—relying on factually dissimilar cases not referenced in the warrant affidavit as evidence that there is a fair probability that a suspect committed a crime in the same manner as those earlier cases— eviscerates the Fourth Amendment's probable cause requirement. The majority opinion's reasoning rests on the unsupported, and unsupportable, premise that if a defendant commited a crime in a certain way in one case—like, for example, the *McGarity* defendants' use of codenames and encryption methods—then there is a fair probability that every other individual suspected of the same crime committed that crime in the same manner as the defendant in the first case.

Consider, for example, a case in which the government suspected a physician's involvement in an alleged health care fraud scheme. In an earlier health care fraud case, the government filed affidavits and obtained three search warrants, for the physician's two medical offices and his personal residence. *See United States v. Srivastava*, 540 F.3d 277, 280–81 (4th Cir. 2008). In addressing the physician's motion to suppress evidence seized from his residence, among other challenges, this Court concluded that the affidavit "made compelling assertions that documents and records relating to [the physician's] medical practice—and that may constitute evidence of health care fraud—would be found in [his] residence." *Id*. at 289. In particular, the affidavit demonstrated that the physician "conducted a substantial part of his medical practice from [his] residence." *Id*. For example, the insurance billing for the physician's medical practice was conducted from his house, and his personal residence

was listed as a billing address. *Id*. at 281. Therefore, the affidavit demonstrated probable cause that evidence of health care fraud would be found at his residence. *Id*. at 289. In so doing, this Court emphasized that the affidavit included case-specific facts demonstrating a nexus between the physician's residence and the evidence of health care fraud.

Under the majority opinion's analytical approach—in which one defendant's conduct may be imputed to all future individuals suspected of committing the same crime—there is a fair probability that every future health care fraud suspect conducted health care fraud in the same way as the defendant in *Srivastava*—namely, from their personal residence as well as their medical offices, even if the affidavit alleges no facts to support such a finding. Accordingly, under the majority opinion's flawed analysis, law enforcement would be able to procure a search warrant for a future health care fraud suspect's home, even if the affidavit does not demonstrate a nexus between her home and health care fraud, simply because health care fraud has been previously conducted in that manner. *But see United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) ("If the affidavit does not present sufficient facts demonstrating why the police officer expects to find evidence in the residence rather than in some other place, a judge may not find probable cause to issue a search warrant.").

Such an analytical approach violates the Fourth Amendment's requirement that the "affidavit supporting the search warrant . . . demonstrate a nexus between the evidence sought and the place to be searched." *Id*. Contrary to the majority opinion's

reasoning, we cannot rely on factually unrelated cases to ascertain probable cause merely because they implicate the same crime. Rather, determining if an affidavit properly establishes a nexus is a "fact-intensive question resolved by examining the totality of circumstances presented." *Id.* (citations omitted).

In further support of its conclusion that Defendant's IP address is unlikely to have innocently encountered the URL in question, the majority points to the "suspiciously short interval *between*" the Bulletin Board A post and the URL click. *Ante* at 14 (emphasis added). In the majority's view, this temporal proximity is based "on the contents of the affidavit, the magistrate judge's likely familiarity with online child pornography crimes, and his ability to reach 'common-sense conclusions about human behavior.'" *Id.* (citations omitted).

But as explained previously, the simple fact that the Bulletin Board A post and the alleged accessing of the File Sharing Site URL took place on the same day does not support the majority opinion's inferential leap. The naked click of a URL provides very little information about how a particular IP address—or individual using that IP address—actually encountered or navigated to a URL. Simply because *law enforcement officers* navigated the URL through one particular pathway—clicking the URL included in the Bulletin Board A post—does not establish, in the absence of additional circumstantial evidence, a fair probability that *Defendant's IP address* also accessed the URL using the same pathway through the Bulletin Board A post. Because the affidavit lacks facts to circumscribe the multitude of potential paths someone using Defendant's IP

address could have taken to encounter and navigate to the File Sharing Site URL, the probability that the person in fact reached the URL through the Bulletin Board A post—the foundation of the probable cause theory embraced by the majority opinion—necessarily approaches zero. This is not the "fair probability" the Fourth Amendment demands.

On the contrary, the inference advanced by the government and made up out of whole cloth by the majority opinion—that someone using Defendant's IP address navigated to the File Sharing Site URL after encountering the URL on Bulletin Board A—amounts to the type of "improbable leap" that the Fourth Amendment does not countenance. *Lyles*, 910 F.3d at 795. Put differently, that inference is not the "usual inference [from] which reasonable men draw from evidence" and therefore does not constitute a "substantial basis" for issuing a warrant. *Johnson v. United States*, 333 U.S. 10, 14 (1948).[7]

---

[7] The majority opinion—like the district court—distinguished this case from an analogous case, *United States v. Reece*, No. 2:16cr104, 2017 U.S. Dist. LEXIS 220176 (E.D.Va. Mar. 1, 2017). In *Reece*, the defendant challenged a search warrant supported by an affidavit nearly identical to the affidavit at issue here—the key difference being that the *Reece* affidavit unambiguously established that the Bulletin Board A post at issue appeared *before* someone using the suspect's IP address clicked on the URL included in the post. The *Reece* court held that the government failed to establish probable cause to support issuance of a warrant to search the suspect's home. *Id.* at *36.

The majority opinion attempts to distinguish *Reece* on the basis that the time between the Bulletin Board A post and the click on the File Sharing Site URL is shorter in this case than in *Reece* (on the same day versus two days apart), thereby rendering "the connection between the suspect and Bulletin

B.

The most troubling aspect of the majority opinion—most clearly evidenced by its reliance on the government's unsupported factual theory—is its failure to grapple with the complex and novel questions courts face when assessing probable cause premised on conduct on the Internet.

1.

Probable cause is not a "[f]inely-tuned standard[]" but rather "turn[s] on the assessment of probabilities in particular factual contexts." *Gates*, 462 U.S. at 232, 235. These probabilities are "incapable of precise definition or quantification into percentages" because they depend on the "totality of the circumstances." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Nevertheless, the term "probabilities" necessarily contemplates that courts try to estimate (at least) outer bounds on the likelihood that contraband or evidence will be found in a particular location at a particular time. Otherwise, the probable cause inquiry would be devoid of guardrails, opening the door to the general warrants the Framers feared. To estimate those outer bounds, courts rely on facts—facts that

---

Board A . . . much closer." *Ante* at 16. Again, however, the majority opinion underplays that the affidavit does not establish that the Bulletin Board A post preceded the click, materially weakening the purported "connection" between Defendant's IP address and Bulletin Board A. That stands in sharp contrast to the affidavit in *Reece*, which unambiguously established that the IP address attempted to download content from the URL *after* the Bulletin Board A post, meaning that the still- insufficient facts in *Reece* provided a stronger basis for finding a "connection" between the suspect and the Bulletin Board A post.

circumscribe the universe of potential explanations and therefore allow the court to make an estimate as to the numerator and denominator determining the probability. *See Lyles*, 910 F.3d at 793 ("The question, as so often in Fourth Amendment cases, is what precisely the facts show."); *see generally* Richard Posner, *Against Constitutional Theory*, 73 N.Y.U. L. Rev. 1, 3 (1998) (observing that "the greatest need of constitutional adjudicators" is "empirical knowledge").

For instance, courts often must decide whether to issue a warrant to authorize the search of a home of a suspect known to sell drugs. In determining whether a warrant should issue—whether there is a fair probability that contraband or evidence will be found at the suspect's home—courts rely on numerous circumstantial facts to guide their determination. Thus, for example, courts upholding warrants issued in such circumstances have emphasized that a recent drug sale took place within a close vicinity of the suspect's home, *United States v. Jones*, 159 F.3d 969, 974 (6th Cir. 1998); that officers had a reasonable belief that a suspect had just left his home and was en route to a drug sale, *United States v. Aguirre*, 664 F.3d 606, 611 (5th Cir. 2011); or that the suspect attempted to hide his residence from the police by driving "erratically" on the way back from a sale, *United States v. Dessesaure*, 429 F.3d 359, 368 (1st Cir. 2005). *See generally* LaFave § 3.7(d) (collecting cases). By geographically and temporally tying the suspect's conduct to his residence, these additional facts—over and above the suspect's history as a drug dealer— make it more likely that the contraband or evidence will be found in the place the government seeks to search.

By contrast, when insufficient information "links the criminal [drug] activity to the defendant's residence"—for example, when the affidavit fails to describe the storage of drugs at the residence, the "geographic relationship" between the area of drug sales and the residence, or temporal proximity between evidence of drug activity at the residence and the proposed search—then the affidavit is "devoid of any basis from which the magistrate could infer that evidence of drug activity would be found at [the residence]." *United States v. Lalor*, 996 F.2d 1578, 1582–83 (4th Cir. 1993). Even when a magistrate "might have been able to draw an inference from the proximity of the drug sales to the [the defendant's] residence," if the government fails to include proximity evidence in a warrant application, then the magistrate has "no basis" for finding probable cause. *Id*. at 1583.

Additional facts circumscribing the universe of possible explanations for potentially unlawful conduct prove especially important when, as here, the facts are consistent with an innocent explanation for the conduct. Although the Fourth Amendment's probable cause requirement "does not depend on the elimination of all innocent explanations for a situation," courts must consider the "existence of countervailing probabilities" as part of their probable cause analysis. *United States v. Jackson*, 415 F.3d 88, 94 (D.C. Cir. 2005). Otherwise, nothing would prevent the government from presenting only the "most incriminating interpretation of the circumstances" and thereby depriving the magistrate of the opportunity to weigh the likelihood that contraband or evidence will be found against the likelihood that contraband is absent. *Id*. at 94–95.

For example, in *United States v. Gary*—an opinion the government relied on in its briefing to the district court, J.A. 44–45—this Court upheld a search warrant for a home that had its genesis in an anonymous tip that someone was selling drugs from that home. 528 F.3d 324, 328 (4th Cir. 2008). Following the tip, the police removed several tied trash bags from two cans "directly behind" the home. *Id*. at 326. The bags contained drugs and drug distribution paraphernalia, including foil and baggies with cut corners. *Id*. at 326. This Court recognized the innocent possibilities that "another person placed the offending bags [containing drugs] in the trash cans, or that some other person moved the unmarked can from its correct spot behind someone else's home to a place behind [the individual's] home." *Id*. at 327. Nevertheless, those "mere possibilit[ies]" did not defeat probable cause to search the home. *Id.*

In reaching that conclusion, we emphasized several case-specific facts that rendered those innocent alternative explanations unlikely. The proximity between the trash cans and the home—the police found the trash cans directly behind the house—reduced the likelihood that contraband in the trash can was unconnected to the adjacent home because generally "trash cans placed directly behind a home are used by those who live there" and trash inside those trash cans is "usually generated *by the house closest to those cans*." *Id*. at 327–28 (emphasis added). Other evidence further tightened the connection between the trash can and the home—a letter addressed to the house was found inside one of the trash cans, and one of the cans bore the house's street number. *Id*. These facts, considered together, established probable cause because they rendered

"too slight" the possibility that the tied trash bags did not come from the house. *Id*. at 328. Importantly, unlike the majority opinion's failure to meaningfully consider the myriad ways someone using Defendant's IP address could have clicked on the File Sharing Site URL without encountering the Bulletin Board A post, the *Gary* Court did not dismiss out of hand potential "innocent reasons" weighing against the likelihood that drug evidence would be found in the home. Instead, this Court looked at the totality of the circumstances and cited specific facts that made those possibilities unlikely.

By contrast, in *United States v. Lyles*, we held that a single trash pull "revealing evidence of three marijuana stems, three empty packs of rolling papers, and a piece of mail, standing alone" did not justify a search warrant for an adjacent home. 910 F.3d at 793. In reaching that conclusion, we highlighted several case-specific facts that rendered the case distinguishable from *Gary*. Whereas in *Gary* the trash pull revealed drug distribution paraphernalia—evidence consistent with recurrent or ongoing activity within the residence, meaning that contraband was likely still at the residence—the single trash pull in *Lyles* revealed only a "tiny quantity of discarded [marijuana] residue" that provided no evidence of recurrent or ongoing activity, rendering it possible, but "not probabl[e]," that drugs would be found in the home. *Id*. at 793–94 (citations omitted). Additionally, whereas in *Gary* law enforcement officers received a tip that drug distribution activities were taking place at the residence, in *Lyles* the affidavit submitted by the government in support of the warrant provided no evidence, beyond the evidence in the trash bag, that

the residence, or individuals living therein, was involved in drug distribution activities. *Id.*

The types of corroborative facts present in *Gary*—and absent in *Lyles*—are especially important in cases, like the instant case, in which the government seeks to obtain a warrant based on online conduct, as the Internet significantly expands the universe of "countervailing probabilities" that courts must consider in weighing whether the government has met its burden to show that there is a fair probability that contraband will be found in the place it seeks to search. *Jackson*, 415 F.3d at 94. In other words, many of the physical, spatial, and temporal limitations that historically proved invaluable in assessing probable cause do not apply in the digital context or apply in meaningfully different ways.

For example, whereas this Court could rely on geographic proximity in *Gary* to conclude that there was a fair probability that contraband would be found in the residence adjacent to the trash cans, geographic proximity has little or no relevance in the context of conduct on the Internet—like the alleged download of child pornography—because the Internet allows for rapid dissemination of electronically stored content throughout the world. That is to say, whereas the limited number of homes within the physical proximity of a trash can means that the probability contraband will be found at any one house near the trash can is fairly large (because the limited number of homes renders the denominator of the probability relatively small), geographic proximity does not serve to increase the probability that contraband will be found at a particular location in the Internet context.

2.

That certain facts courts historically have relied on to assess probable cause lack, or have diminished, probative value in the Internet context does not mean that the government will never be able to surmount its evidentiary burden to obtain a warrant based on Internet conduct. "Technology is both a threat and a promise." *Vieth v. Jubelirer*, 541 U.S. 267, 312 (2004) (Kennedy, J., concurring in the judgment). Although new technologies can foreclose certain avenues for the government to show probable cause—such as through geographic proximity—"new technologies [also] may produce new methods" of demonstrating probable cause. *Id.* at 312–13. For example, the ease with which Internet and telecommunications companies can capture and store information regarding an IP address's browsing behavior and online activities provides a wealth of additional information for the government to rely on in seeking to obtain a search warrant for a residence associated with the IP address. In the child pornography context, in particular, courts routinely rely on such evidence—or the absence of such evidence—to determine whether the government has met its burden to show a fair probability that evidence related to child pornography offenses will be found at a residence associated with a particular IP address.

For instance, in *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc), the Ninth Circuit found probable cause to search a defendant's residence based on facts set forth in affidavit establishing a fair probability that the suspect "inten[ded] and desire[d] to obtain illegal images," *id.* at 1070. Those facts included that (1) the suspect

paid for a subscription to a website, Lolitagirls.com, that "was a child pornography site whose primary content was in the form of images"; (2) electronic records from a credit card processing service revealed that in order to subscribe to the website the suspect "submitt[ed] his home address, email address and credit card data, and he consented to have $19.95 deducted from his credit card every month"; and (3) the suspect "became a member [of the website] and never looked back—his membership ended because the FBI shut down the site" several months later. *Id.* at 1070–71. The Court reasoned that these facts established that the defendant "could not have become a member by accident or by *a mere click of a button*[.]" *Id.* (emphasis added). The Court relied on the circumstantial evidence regarding the defendant's Internet conduct to determine that the "countervailing probabilit[y]" that the defendant innocently visited the website was low. *Jackson*, 415 F.3d at 94; *see also, e.g.*, *United States v. Martin*, 426 F.3d 68, 78 (2d Cir. 2005) (finding probable cause to search a residence when electronic records revealed that an individual with a particular email address "joined . . . voluntarily and never cancelled his membership" to a child pornography website and that the user of the email address lived at the residence for which the warrant was sought).

In contrast, courts have declined to find probable cause when the government fails to put forward supporting facts that diminish the likelihood that a child pornography website was accessed innocently or unintentionally. For example, in *United States v. Falso*, the Second Circuit held that a forensic analysis of a child pornography site's server revealing that a suspect—who the affidavit reported

had been charged 18 years earlier for sexually abusing a seven-year-old girl—had "either gained access or attempted to gain access" to a child pornography website did not establish probable cause to search the suspect's home, 544 F.3d at 114. Writing for the court, then-Judge, now-Justice Sotomayor held that those facts were insufficient to establish probable cause because, unlike *Martin*, the affidavit included "no allegation that [the suspect] in fact gained access to the [child pornography] website, much less that he was a member or subscriber of any child- pornography site." *Id.* at 124.

The Second Circuit pointed to several types of information that the government could have—but did not—adduce in preparing its warrant application that may have allowed it to satisfy the "fair probability" standard, including that the suspect (1) took actions "tend[ing] to negate the possibility that his membership or subscription was unintended," such as being a member of multiple child pornography sites or having provided personal information to join a child pornography site; (2) used an "e-mail address[] or screen name[] suggestive of an interest in collecting child pornography"; or (3) had a "criminal history relating to child pornography." *Id.* at 120 (collecting cases). The court further suggested that, to show it was more likely that contraband would be found at the suspect's residence, the government "could have monitored the traffic of [the child pornography] website and ascertained whether [the suspect] (and others) actually downloaded pornography from the site." *Id.* at 124 n.20.

The majority opinion's resolution of this case puts this Court at odds with *Gourde*, *Martin*, and

Falso[8] and other circuit decisions requiring the government to adduce additional facts—over and above the single click of a URL that provides for download of child pornography—to establish probable cause to search a residence associated with the IP address responsible for the click. Unlike in *Gourde*, *Martin*, and *Falso*—and notwithstanding that the warrant application had its genesis in the government's monitoring of Bulletin Board A—the government concedes that its warrant application never established that someone using Defendant's IP address ever had visited Bulletin Board A, let alone consciously joined that site.

Nor does the affidavit establish any of the other types of facts *Falso* recognized courts use to

---

[8] The majority opinion attempts to distinguish *Falso* on grounds that "there, the affidavit contained no allegation that the defendant in fact gained access to a website containing child pornography, nor any allegation that images of child pornography were downloadable from the site." *Ante* at 17 (internal quotation marks and alterations omitted). According to the majority opinion, the affidavit in this case is materially different because it "alleged that [Defendant]'s IP address accessed a URL" containing child pornography. *Id*.

But under the majority's reasoning, that difference is irrelevant. The majority opinion holds—and I agree—that to establish probable cause based on a "single click," the affidavit must establish a fair probability that "someone using [Defendant]'s IP address clicked the link knowing that it contained child pornography." *Ante* at 8. Under that rule, the "access[ing of] a URL" containing child pornography does not, by itself, establish probable cause. Rather, there must be "knowing" accessing of illicit content. *Id.* at 8–9. As explained above, the affidavit failed to establish that someone using Defendant's IP address navigated to the URL through the Bulletin Board A post, and therefore failed to establish that the person "knowing[ly]" sought to access child pornography.

circumscribe the universe of potential explanations for an IP address clicking on a URL linked to child pornography. The affidavit did not aver that Defendant, or someone likely to be using his IP address, used an email address or Internet screenname suggestive of an interest in child pornography; had a criminal history relating to child pornography; or ever had visited or joined other child pornography sites. Put another way, the affidavit establishes solely that someone using Defendant's IP address clicked on a URL hosted on File Sharing Site—in short, the "mere click of a button" rejected by the Ninth Circuit in *Gourde*. *See also United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005) (Rakoff, J.) (rejecting the theory that the naked "clicking [of] a button" was sufficient to establish probable cause).

The majority opinion nevertheless contends that its decision is consistent with these out-of-circuit decisions because here, the "abbreviated time frame" alone suffices as an additional fact "lessen[ing] the likelihood that [Defendant's] IP address accessed the link independently of Bulletin Board A." *Ante* at 18. But, as explained above, the affidavit does not establish that someone using Defendant's IP address accessed the File Sharing Site URL after the Bulletin Board A post. And the additional facts relied upon by other circuits—such as whether the IP address paid for a child pornography website subscription; submitted personal information to a child pornography website; or was a member of a child pornography website—establish a much closer nexus between the suspect's IP address and a child pornography website than the purported relationship by the facts set forth in the affidavit here, which show only that the *Bulletin Board A* post appeared on the

same day that someone using Defendant's IP address clicked on a URL to a *different website*.

3.

Comparing this case to *Gourde, Martin*, and *Falso* also puts in sharp relief the types of information omitted from the affidavit, but which the government may have been able to include in the affidavit to reduce the "countervailing probabilit[y]" that someone using Defendant's IP address navigated to the File Sharing Site URL via some pathway other than the Bulletin Board A post. For instance, the affidavit may have been able to provide the timestamp of the Bulletin Board A post, and thereby rule out the possibility that someone using Defendant's IP address clicked on the URL before the post appeared on Bulletin Board A. Or, the affidavit may have been able to state whether Defendant's IP address actually downloaded the child pornography hosted by File Sharing Site—meaning that the contraband was more likely stored on a computer in Defendant's residence—rather than simply "attempt[ing]" to do so. Or, the affidavit may have been able to state, based on the government's monitoring of Bulleting Board A, whether Defendant, or someone using his IP address, ever had posted to Bulletin Board A. Or, the affidavit may have addressed whether someone using Defendant's IP address had clicked the File Sharing Site URL another time. Or, the affidavit could have stated whether the IP address had clicked *another* URL on File Sharing Site or some other website containing child pornography. Or, the affidavit may have been able to state whether Defendant, or someone likely to be using his IP address, had committed prior offenses

indicative of a potential interest in child pornography. Or, the affidavit may have been able to state, based on the records the government obtained from File Sharing Site, how many different IP addresses downloaded or attempted to download the content accessible through the URL, thereby providing some indication as to how widely the URL was disseminated.

Any one of these facts would have provided the magistrate with greater clarity as to whether there was a fair probability that someone using Defendant's IP address clicked on the URL knowing that it would likely lead to the download of child pornography, and therefore that contraband was likely to be found in Defendant's residence. Importantly, the government never has stated, either in the affidavit or in briefing, that it could not have learned of some or all of these facts before submitting the warrant request.

By allowing the government to obtain a warrant to rummage through Defendant's residence and effects based on the single click of a URL navigating to a website not devoted to child pornography, File Sharing Site, the majority opinion invites the government to submit similar bare-bones affidavits in the future. That is to say, the approach taken by the majority opinion—which relies on those representations in the government's briefing that do not find support in the affidavit submitted in support of the warrant—sends a message to government that any ambiguities or omissions in the evidence it submits in support of a warrant application will inure to its benefit.

That is precisely the wrong message for the judiciary to send to the government. As explained above, in order to assess whether there is a fair probability that contraband or evidence in a place the government seeks to search, courts need facts—we need to know "what precisely the facts show." *Lyles*, 910 F.3d at 793. And it is the government's burden to put forward those facts necessary for courts to make that determination. Accordingly, rather than rewarding the government for submitting a warrant application with glaring inadequacies and omissions—like the time of the Bulletin Board A post—this Court should require the government "to comply with the well-known duty to spell out the *complete factual basis* for a finding of probable cause within the affidavit's four corners" and thereby advance the "preeminently worth goal" of "deterring police from submitting (and magistrates from accepting) affidavits that completely omit crucial factual allegations." *Virgin Islands v. John*, 654 F.3d 412, 420 (3d Cir. 2011).

4.

The conspicuous absence of facts circumscribing the universe of countervailing probabilities also fatally undermines the efforts by my colleagues in the majority to analogize the online conduct at issue to analytical frameworks developed by courts prior to the advent of the Internet. Analogical reasoning follows a familiar four-step framework: "(1) Some fact pattern *A* has a certain characteristic *X,* or characteristics *X, Y,* and *Z*; (2) Fact pattern *B* differs from *A* in some respects but shares characteristics *X,* or characteristics *X, Y,* and *Z*; (3) The law treats *A* in a certain way; (4) Because *B* shares certain

characteristics with *A,* the law should treat *B* the same way." Cass R. Sunstein, *On Analogical Reasoning*, 106 Harv. L. Rev. 741, 745 (1993). It is "readily app[arent]" from this framework that "analogical reasoning does not guarantee good outcomes or truth." *Id.* Rather, "[f]or analogical reasoning to operate properly, we have to know that *A* and *B* are 'relevantly' similar, and that there are not 'relevant' differences between them." *Id.* at 745. In cases involving new technology like the Internet, therefore, analogical reasoning is valid only if the new technology is "'relevantly' similar" to the technology employed in the cases in which the rule or framework was developed or previously applied.

To be sure, there are cases in which new technology is "'relevantly' similar" to technology considered in earlier cases, rendering analogies between cases involving the two types of technology valid. For instance, in determining whether social media websites constitute public forums for purposes of the First Amendment, the Supreme Court has described such sites as "the modern public square." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1737 (2017). That analogy is "'relevant[ly]' similar" because, at least in certain circumstances, social media sites "bear the hallmarks of a public forum" by constituting a space for unfettered "public discourse." *Davison v. Randall*, 912 F.3d 666, 682 (4th Cir. 2019); *see also, e.g.*, *City of Richmond v. S. Bell Tel. & Tel. Co.*, 174 U.S. 761, 776–77 (1899) (analogizing the telephone to the telegraph in deciding whether a telephone company's business was within the purview of a congressional act relating to telegraph companies).

But there are also cases in which analogical reasoning has proved faulty as a result of "'relevant' differences" between the facts at issue and the cases to which courts seek to draw an analogy. For example, several courts once held that law enforcement officers could conduct a warrantless search of an arrestee's cell phone on grounds that cell phones are analogous to "container[s]"—like cigarette packs, wallets, or purses—which may be searched incident to arrest. *See, e.g.*, *United States v. Wurie*, 612 F. Supp. 2d 104, 109–110 (D. Mass. 2009) (collecting cases), *rev'd* 728 F.3d 1 (1st Cir. 2013). In *Riley v. California*, the Supreme Court rejected that reasoning, highlighting the numerous ways in which cell phones differ from other objects arrestees keep on their person, rendering the analogy between cell phones and containers inapt. 573 U.S. at 393 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."). According to the Supreme Court, one crucial "'relevant' difference" between cell phones and the type of "containers" law enforcement officers may search incident to arrest is the "immense storage capacity" of modern cell phones, which allows for the storage of a vast trove of highly personal information that, prior to the advent of modern electronic storage, could not be stored in "a container the size of [a] cigarette package." *Id.* at 393–95. *Riley*, therefore, stands for the general proposition that because "[c]yberspace is different from the physical world," courts "should proceed circumspectly" in analogizing analog case law to the digital context. *Packingham*, 137 S. Ct. at 1743–44 (Alito, J., concurring in the judgment).

Here, in appealing to the purported "temporal proximity" between the Bulletin Board A post and the click on the URL hosted by File Sharing Site, the government advances—and the majority opinion embraces—an unstated analogy to the evidentiary rule providing for authentication of a writing, communication, or other form of evidence based on "[a]ppearance, contents, substance, internal matters, or other distinctive characteristics, taken in conjunction with circumstances." Fed. R. Evid. 901(b)(4). Rule 901(b)(4) codifies and generalizes the common-law "reply-letter doctrine," which provides for authentication of a writing or communication "where it can be show that the [writing or communication] was sent in reply to a previous communication." *Winel v. United States*, 365 F.2d 646, 648 (8th Cir. 1966); *see also* Charles Alan Wright & Victor James Gold, Federal Practice & Procedure: Evidence § 7109, at 83 (2000).

The majority opinion reasons that because the click (possibly) occurred soon after the Bulletin Board A post—and because the URL was composed of a distinctive string of letters and numbers—the person using Defendant's IP address who made the click *must* have encountered the URL on Bulletin Board A. In a nutshell, the majority opinion rests on the determination that due to temporal proximity and the unique content of the URL there is a fair probability that the click was made "in reply to" the Bulletin Board A post.

But there are "'relevant' differences" between the factual scenario in which courts have applied the reply rule and the Internet context to which the majority opinion seeks to extend it. Most

significantly, unlike with the items typically authenticated under Rule 901(b)(4)—letters, telephone calls, or even emails—URLs can be easily copied, disguised, and shared rapidly and widely—preserving no indication of their provenance—meaning that there are potentially millions of pathways through which someone using Defendant's IP address could have encountered and navigated to the File Sharing Site URL. *See supra* Part II.A.

That difference materially undermines the analogy to authentication under Rule 901(b)(4), which is premised on the notion that the "*distinctive characteristics*" of a writing make it sufficiently likely that an item of evidence is what a proponent purports it to be. Wright & Gold, Fed. Prac. & Proc.: Evid. § 7109, at 74–87 (emphasis added); *see also McQueeney v. Wilmington Trust Co.*, 779 F.2d 916, 930 (3d Cir. 1985) (authenticating record based on distinctiveness of information contained therein because "[a]lthough we do not know precisely how many people had the information contained in the proffered evidence, we suspect . . . that *the number is small*" (emphasis added)). When *thousands or even millions* of copies of a URL can exist on the Internet—and the government provides no factual basis for circumscribing that universe to a "small" number of relevant copies, *McQueeney*, 779 F.2d at 930—one cannot reasonably determine that someone using Defendant's IP address clicked on that URL in reply to *one* posted copy of the URL—here, the Bulletin Board A post.

Notably, commentators have recognized that new technology allowing for easy replication and duplication of documents—akin to the easy

duplication of URLs—has forced courts to reconsider which characteristics of a writing render it sufficiently distinctive to establish its provenance. Wright & Gold, Fed. Prac. & Proc.: Evid. § 7109, at 80–81 ("[W]hile earlier cases often assumed that the use of letterhead paper is sufficient to establish authenticity, that conclusion is now undermined by the current widespread availability of photocopy machines, scanners, and computer software capable of forging any letterhead."). Accordingly, the ease with which URLs can be copied and shared renders inapt the analogy upon which the majority opinion implicitly relies.

Or consider another proposed analogy advanced by one of my colleagues in the majority during oral argument:

> If a package is being sent through the mail to a residence and that package contains cocaine . . . and [law enforcement officers] go and say they want a search warrant for that house because the package is being delivered there, there is probable cause to search that house, right. We recognize though that it could well be and, in fact, we actually know that often . . . drug dealers will send packages to their next door neighbor, for example, and try to pick them up before they are gathered. So there are always possibilities that that package could be sent to an innocent neighbor instead of the actual drug dealer. But throughout the case law we say that that may well be true—that is a possible explanation—

> that the receiver doesn't know that it was coming, but that doesn't destroy probable cause.

Oral Argument at 41:40–43:46; *see also, e.g.*, *United States v. Lawson*, 999 F.2d 985, 988 (6th Cir. 1993) (reasoning that the possibility that the addressee of package containing drugs was an "innocent receiver[]" was "extremely remote, especially in the context of a controlled delivery of a quantity of drugs presumptively sufficient to constitute possession for resale."). Again, several aspects of this analog analogy do not map well onto the digital context.

To begin, as in the trash pull example at issue in *Gary*, *see supra* Part II.B.1, the limited number of houses "neighbor[ing]" the house to which the package of cocaine is delivered allows courts to place a lower bound on the probability that the house to which the package was delivered was, in fact, the package's intended recipient. By contrast, because URLs can be copied myriad times and rapidly disseminated to an infinite number of IP addresses around the world, geographic proximity provides no assistance to courts in assessing the probability that electronically disseminated contraband will be found in any particular location.

Second, contraband disseminated over the Internet is not subject to the same physical constraints as the package of cocaine in my colleague's hypothetical. A URL, and the content to which it navigates, can be replicated, stored, and reposted with little or no cost or effort. By contrast, a package of cocaine cannot be replicated and obtaining additional packages of cocaine is costly. Due to the

cost and complexity of obtaining packages of cocaine, someone is not likely, for example, to send a package of cocaine to a large swath of innocent persons as part of an extortion scheme, as has occurred with child pornography disseminated electronically. *See* Levin, *supra*.

Third, there are more ways to disguise the content to which a URL navigates than a package of cocaine. As explained above, there are virtually an infinite number of ways that one can mask a URL, through methods such as link shortening or disguising. To be sure, there also are ways to disguise a package of cocaine—the sender, for example, can use a false return address or use a box that suggests the contents of the package are innocuous. But the methods for disguising cocaine are more limited—a given quantity of cocaine takes up a certain amount of space and has a certain weight, meaning any effort to mask a package of that quantity of cocaine is necessarily subject to certain physical limitations.

Fourth, the cocaine package can be delivered by limited means—the postal service, a commercial service like FedEx or UPS, or a private individual or group. By contrast, as explained above, the IP address could have encountered and navigated to the URL in myriad ways, only some of which provide any indication of the nature or origin of the content to which the URL navigates.

That the bare-bones facts provided in the affidavit—a single click of a random alphanumeric URL leading to a widely used file sharing website hosting downloadable child pornography on the same day as a copy of the URL appeared on a different website devoted to child pornography—render the

analogies my colleagues in the majority seek to draw inapt does not mean, however, that courts can never rely on analogical reasoning to assess probable cause in the Internet context. Rather, it means that the government must put forward sufficient facts in an affidavit to establish that the online conduct at issue is "'relevant[ly] similar" to the facts of prior cases such that the analogy the government wishes the court to draw is valid. The government simply failed to do that here.

5.

The majority opinion's resolution of this case also opens the door to the government obtaining the general warrants the Framers feared. In particular, it opens the home—"first among equals" when it "comes to the Fourth Amendment"—to sweeping governmental searches based on a single click of a URL by an Internet user, regardless of whether the government adduces facts indicating that the user intended to navigate to the URL's illicit content. *Jardines*, 569 U.S. at 6. Several hypotheticals illustrate the dangerous scope of the majority opinion's holding.

Suppose, for example, that a businessperson is conducting Internet research related to her business when a pop-up suddenly appears stating that her computer has a virus and that she should "Click here" to start the computer's clean-up process. Thinking the pop- up window was generated by her computer's anti-virus program, she clicks the link and navigates to a URL hosted by a widely used file sharing service, like File Sharing Site, where, upon entry of a password, a user can download child pornography.

Or consider that Grandma receives an email from what appears to be a close friend. The email contains the following sentence "Click HERE for my favorite knitting website." The word "HERE" is a hyperlink, appearing to direct Grandma to that knitting website. Grandma hovers her mouse over the word "HERE," which reveals the URL. But given the URL's random alphanumeric string, it reveals nothing about its content. Believing that the URL navigates to the knitting website, Grandma clicks "HERE" and is redirected to the same file sharing service URL encountered by the businessperson.

Or consider a teenager who clicks an online post that purportedly links to the latest viral YouTube video. Unbeknownst to the teenager, the link has been spoofed to appear to look like a YouTube link. Clicking the link in fact takes the teenager to the same file sharing service URL encountered by the businessperson and Grandma.

Or consider a college student who regularly visits a popular website devoted to adult pornography. A post in a discussion forum on the website includes a random alphanumeric URL, which the post says navigates to additional free pornographic images. The student clicks the link, which navigates the student's browser to the same file sharing URL encountered by the businessperson, Grandma, and the teenager.

In each of these hypotheticals, also suppose that the same day, independently of each individual's innocent navigation to the URL, a post on a known child pornography site, like Bulletin Board A, included that same URL. The timing of the post on

the child pornography site is irrelevant—it could have appeared before or after the businessperson, Grandma, the teenager, or the college student navigated to the File Sharing Site URL.

Under the majority's opinion, in each of these hypothetical scenarios, the government would be able to obtain a search warrant to conduct an invasive search of each individual's home and electronic devices for evidence of wrongdoing. Like the instant case, *no additional fact* in these hypotheticals demonstrates the businessperson's, Grandma's, the teenager's, or the college student's intention either to access the child pornography site or child pornography, and *no limiting fact* reduces the countervailing innocent probabilities.

Contrary to the majority's wholly unsupported speculation that the "likelihood that a specific filesharing page containing child pornography would find its way to somebody uninterested in such contraband . . . is probably quite low," these hypotheticals are not far-fetched. *Ante* at 13; *see, e.g.*, Robert Siciliano, *Why Is Child Pornography on Your PC?*, HuffPost (Dec. 6, 2017), https://www.huffpost.com/entry/why-is-child-pornography_b_356539? ("When you click a link in an email or a pop up advertisement in your browser, you may inadvertently download one of these viruses, which can then visit child pornography websites and download files onto your hard drive."); *Viruses Frame PC Owners for Child Porn*, CBS News (Nov. 9, 2009, 12:49 PM), https://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn (describing an Associated Press investigation into numerous cases in which child pornography was placed on a

computer through a virus, including one computer that was "programmed to visit as many as 40 child porn sites per minute"). And it takes little imagination to envision corporate competitors, jilted lovers, or other bad actors sending unsuspecting victims disguised links to illicit content, knowing that if their victims click on that link, the government could search their homes or businesses.

*****

In sum, taking seriously the nature of the new and advancing technology at issue, the connection my colleagues in the majority draw between the Bulletin Board A post and the click on the File Sharing Site URL does not find factual support in the government's bare-bones warrant application. A single click of a URL, absent any further factual evidence circumscribing the universe of paths through which someone using Defendant's IP address could have encountered and navigated to that URL—nearly all of which have no relation to Bulletin Board A—is insufficient to establish probable cause. Indeed, the majority opinion concedes that in a "case based purely on an IP address connecting with a URL," probable cause "may be hard to establish absent other incriminating evidence." *Ante* at 15. Contrary to the majority's belief, this is that case.

Physical searches of the home represent the "chief evil against which the wording of the Fourth Amendment is directed." *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972). The majority's unquestioning acceptance of the government's probable cause theory—that, "by [the] act of clicking a button," an individual opens the doors

of his home and the electronic devices stored therein to a sweeping search by government agents—is "utterly repellent to core purposes of the Fourth Amendment." *Coreas*, 419 F.3d at 156. Therefore, I dissent from the majority opinion's conclusion that the magistrate judge had a substantial basis for finding that there was a fair probability that contraband would be found at Defendant's residence.

III.

Defendant next argues that even if probable cause existed to search his residence in November 2015—when someone using Defendant's IP address sought to download child pornography from File Sharing Site—probable cause no longer existed when the government obtained the warrant and searched his residence six months later. I agree.

Defendant's argument rests on the well-established rule that a valid search warrant "may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." *United States v. McCall*, 740 F.2d 1331, 1335–36 (4th Cir. 1984) (internal quotation marks omitted). To that end, the information in the affidavit supporting the warrant must not be "too stale to furnish probable cause." *Id.* at 1336. Staleness is "not resolved by reference to pat formulas or simple rules." *Id.* Rather, "we must look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Id.*

Child pornography cases present "unique" staleness questions. *United States v. Raymonda*, 780

F.3d 105, 114 (2d Cir. 2015) (internal quotation marks). As the majority correctly recognizes, when assessing claims of staleness in child pornography cases, courts distinguish between categories of suspects. The first category encompasses suspects—often referred to as "collectors"—for whom "circumstances suggest[] [they] had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *Id.* at 114–5. The second category encompasses those suspects for whom there is an absence of evidence of willful or deliberate interest in child pornography—suspects who may have encountered child pornography in a "purely negligent or inadvertent" manner. *Id.* at 115.

In cases involving collectors, "courts have largely concluded that a delay—even a substantial delay—between distribution and the issuance of a search warrant does not render the underlying information stale." *United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010) (rejecting that a period of four months between the defendant's email of an image depicting child pornography until the warrant was issued); *see also United States v. Burkhart*, 602 F.3d 1202, 1206 (10th Cir. 2010) (noting that the "'passage of time alone' cannot demonstrate staleness" in child pornography cases). Such an approach is warranted because collectors "value their sexually explicit materials highly, rarely if ever dispose of such material, and store it for long periods in a secure place, typically in their homes." *Richardson*, 607 F.3d at 370 (citations and internal quotation marks omitted); *see also United States v. Sassani*, 139 F.3d 895 (4th Cir. 1998) (unpublished) (collecting cases).

But as the Second Circuit has recognized, "the value of [these] inference[s] in any given case depends on the preliminary finding that the suspect is a person 'interested in' images of child pornography"—that the suspect is, in fact, a collector. *Raymonda*, 780 F.3d at 114. Put simply, "the 'alleged proclivities of collectors of child pornography' . . . 'are only relevant if there is probable cause to believe that [a given defendant] *is* such a collector.'" *Id.* (quoting *Coreas*, 419 F.3d at 156).

In determining whether an affidavit submitted in support of a warrant establishes a fair probability that a child pornography suspect is a collector, courts have looked to "a suspect's admission or other evidence identifying him as a 'pedophile,'" a suspect's paid access or subscription to child pornography, or a suspect's "extended history of possessing or receiving pornographic images." *Raymonda*, 780 F.3d at 114–15 (collecting cases). Here, the affidavit is devoid of evidence that the individual using Defendant's IP address to click on the URL was a "collector," as courts have construed that term. The affidavit presents no evidence: that Defendant, or anyone likely to be using his IP address, was a pedophile; that Defendant's IP address had ever subscribed to or paid for access to child pornography; or that someone likely to be using Defendant's IP address had ever possessed or received child pornography. The affidavit does not even aver that a device connected to Defendant's IP address downloaded—let alone opened—the child pornography stored on File Sharing Site prompting the warrant request.

In certain cases, courts have inferred that a suspect was a collector "on the basis of a *single*

incident of possession or receipt"—when, "for example, the suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files" or when the defendant "subsequently redistributed that [single] file to other users." *Id*. at 115 (emphasis added). But in such cases the inference that the suspect was a "collector" "did not proceed merely from evidence of [] access to child pornography at a single time in the past." *Id.* Rather, the inference rested on "circumstances suggesting that [the individual] had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *Id.*

The government argues—and the majority opinion agrees—that the circumstances described in the affidavit surrounding the attempt to download child pornography from File Sharing Site on November 2, 2015, established a "fair probability" that "whoever clicked on the link did so willfully and deliberately because he was interested in images of child pornography." *Ante* at 21. In support of that conclusion, the majority opinion relies entirely on its determination that the information set forth in the affidavit established that it was fairly probable "that somebody saw the description and video thumbnails on a website devoted to child pornography, Bulletin Board A, and then deliberately sought out the video by clicking that link." *Id*.

But the affidavit fails to establish a fair probability that someone using Defendant's IP address ever visited Bulletin Board A, let alone navigated through the November 2, 2015, post on Bulletin Board A to the child pornography stored by

File Sharing Site. *See supra* Part II. And the affidavit's averments bearing on whether Defendant's IP address was used by a collector materially differ from the cases in which this Court and other courts have rejected staleness arguments in child pornography cases.

In *Richardson*, for example, this Court concluded that a delay of four months did not render the probable cause finding stale "*in light of the other information* supplied by [the federal agent], including the previous instance in which [the defendant] used an AOL account to send such images [.]" 607 F.3d at 370 (emphasis added); *see also United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997) (holding that ten-month-old information is not stale where the affidavit provided evidence that the defendant downloaded at least two GIFs depicting minors engaged in sexual activity); *United States v. Ramsburg*, 114 F. App'x 78, 82 (4th Cir. 2004) (unpublished) (concluding that evidence was not stale when it showed the defendant had previously transmitted an image of child pornography was a member of two e-groups that regularly distributed child pornography). Accordingly, the majority errs in rejecting Defendant's staleness argument.

IV.

Finally, the majority holds that even if the search warrant was constitutionally deficient—either due to lack of probable cause or staleness—the district court did not reversibly err in refusing to suppress the evidence obtained during the search because the officers reasonably relied on the warrant in executing the search. *Ante* at 18. Again, I disagree.

Under the so-called "good faith" exception to the exclusionary rule, "evidence obtained pursuant to a search warrant issued by a neutral magistrate does not need to be excluded if the officer's reliance on the warrant was 'objectively reasonable.'" *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011) (citing *United States v. Leon*, 468 U.S. 897, 922 (1984)). Defendant argues that the government is not entitled to invoke the good faith exception for two reasons: the materials submitted to the magistrate in support of the warrant application were (1) materially misleading and (2) "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* (quoting *Leon*, 468 U.S. at 922–23).

As to the first reason, the government may not seek relief under the good faith exception if "the magistrate or judge [] issuing the warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for [her] reckless disregard of the truth." *Id.* (citation omitted). One situation in which this Court has found an affidavit is sufficiently misleading to establish an absence of good faith is when the affidavit includes "puffing"—i.e., irrelevant or inapplicable information—in an apparent "attempt[] to endue the affidavit with the appearance of genuine substance." *United States v. Perez*, 393 F.3d 457, 465 (4th Cir. 2004) (quoting *United States v. Wilhelm*, 80 F.3d 116, 123 (4th Cir. 1996)).

Here, whereas only two paragraphs of the affidavit address allegedly unlawful conduct of someone using Defendant's IP address—attempting to download child pornography from File Sharing Site—the vast majority of the content in the

affidavit— nearly twenty paragraphs—relates to the government's investigation into Bulletin Board A and the behavioral characteristics of "collectors" of child pornography. By including that information, the government sought to paint a picture of Defendant as a collector of child pornography who downloaded child pornography from a website, Bulletin Board A, devoted to child pornography. Yet, none of the evidence set forth in the affidavit establishes a fair probability that Defendant ever visited Bulletin Board A, let alone navigated through the Bulletin Board A post to the File Sharing Site URL. *See supra* Part II. And, the affidavit fails to establish a fair probability that Defendant was a "collector" of child pornography. *See supra* Part III. Accordingly, unless the affidavit established any nexus between Bulletin Board A and Defendant's IP address—which it did not—the affidavit's description of Bulletin Board A and the contents of the post is not at all "crucial to understanding why the government believed [Defendant's] home would contain evidence of criminal activity." *Ante* at 23.

By devoting the vast majority of the affidavit to information untethered from Defendant—or even Defendant's IP address—the government made the affidavit appear as if it had "genuine substance," *Wilhelm*, 80 F.3d at 123, when in fact the information in the affidavit pertaining to Defendant established only that someone using Defendant's IP address clicked on a link to a widely used File Sharing Site around the same time, but not necessarily after, a post regarding the content of the link appeared on a wholly unrelated website devoted to child pornography. Accordingly, the inclusion of the Bulletin Board A and collector information was

materially misleading. *See Raymonda*, 780 F.3d at 124 (Chin, J., concurring in part and dissenting in part) ("Without any evidence that [the suspect] was a collector of child pornography, it was inappropriate—and heedlessly indifferent—for [the affiant] to rely on boilerplate language regarding the proclivities of collectors."); *Reece*, 2017 U.S. Dist. LEXIS 220176, at *28–30 (finding misleading an affidavit's inclusion of extensive information regarding the Bulletin Board A investigation and "the general characteristics shared by collectors of child pornography" when the affidavit failed to establish a fair probability that the suspect ever visited Bulletin Board A or was a collector of child pornography); *cf. Coreas*, 419 F.3d at 156 (rejecting the use of "unparticularized allegations" to justify an otherwise inadequate warrant application).

Importantly, evidence indicates that the government knew that the inclusion of "boilerplate" language regarding collectors, in particular, is materially misleading when, as here, the affidavit does not establish that a suspect is a collector: the template for search warrants in child pornography cases used by law enforcement officers in the Bulletin Board A investigation directs affiants that they should include boilerplate "collector" information in an affidavit "ONLY if" the affiant can "tie [collector] characteristics to the specific offender." *Reece*, 2017 U.S. Dist. LEXIS 220176, at 22.

An affidavit also is misleading when affiants "omit material facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading." *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990) (citations and internal quotation marks omitted). In seeking to avoid

application of the good faith exception on the basis of a material omission, a defendant must show "(1) that the officer deliberately or recklessly omitted the information at issue and (2) that the inclusion of this information would have defeated probable cause." *United States v. Andrews*, 577 F.3d 231, 238–39 (4th Cir. 2009).

Here, the affidavit includes at least one material omission—evidence regarding the time of the Bulletin Board A post. Although the district court denied Defendant's request for a *Franks* hearing—meaning the record is largely devoid of evidence regarding what information the government chose to leave out of the affidavit—the affidavit provides some indication that the affiant knew when the post occurred. In particular, the affidavit states law enforcement officers began "observ[ing] various postings" and "captur[ing] content" on Bulletin Board A in October 2015, before the November 2, 2015, Bulletin Board A post at issue. J.A. 164. Given that the government was engaged in ongoing monitoring of Bulletin Board A, one can reasonably infer that the government knew—or at least should have known—the time of the November 2, 2015, post. In short, the omission of the time of the Bulletin Board A post from the affidavit was at least reckless, if not deliberate. *See United States v. Jacobs*, 986 F.2d 1231, 1234–35 (8th Cir. 1993) (concluding that an "omission occurred at least with reckless disregard with its effect upon the affidavit" when "[a]ny reasonable person would have known that this was the kind of thing the [magistrate] judge would wish to know").

Because the government's probable cause theory—which the majority opinion embraces—relies

exclusively on the temporal relationship between the Bulletin Board A post and the click on the File Sharing Site URL, the conspicuous omission of the time of the Bulletin Board A post from the affidavit "casts substantial doubt on the probability" that the click in fact occurred *after* the Bulletin Board A post. *Gourde*, 440 F.3d at 1076 (Reinhardt, J., dissenting). That the government repeatedly has represented in briefing to both the district court and this Court that the click occurred *after* the post—notwithstanding the absence of evidence to that effect in the affidavit, *see supra* Parts I, II.A—renders the omission of the timestamp all the more problematic. And if the click in fact occurred *before* the Bulletin Board A post—and the government had disclosed that information in the warrant application—the government could not have established probable cause. In such circumstances, the warrant application would lack the "critical fact" upon which the majority opinion largely relies. *Ante* at 8.

Second, the good faith exception does not apply because the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Doyle*, 650 F.3d at 467. Although "[m]ere insufficiency of the affidavit to support probable cause" will not preclude application of the good faith exception, when the "deficiencies in the affidavit . . . [are] so great as to render it objectively unreasonable" to rely on the warrant, it will. *Id*. at 470.

Here, it was objectively unreasonable for the law enforcement officers conducting the search to rely on the warrant application because, at the time of the search, it was well- established that a magistrate

could not issue a warrant based on evidence "too stale to furnish probable cause." *McCall*, 740 F.2d at 1336 (internal quotation marks omitted). And it was well-established at that time that in cases involving child pornography, months- old evidence that a suspect sought to access or download child pornography—like the click of the File Sharing Site URL—is too stale to establish probable cause, absent evidence that the suspect is a "collector." *See Doyle*, 650 F.3d at 474 & n.15; *see also Raymonda*, 780 F.3d at 117 (holding that evidence that suspect had "accessed thumbnails of child pornography" nine-months earlier was too stale to establish probable cause when affidavit failed to establish suspect was a collector). And it was likewise well-established at that time that an affidavit establishes a fair probability that a suspect is a collector child pornography only if the affidavit sets forth "circumstances suggesting that [the suspect] had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *Raymonda*, 780 F.3d at 115.

As explained above, the bare-bones facts set forth in the affidavit failed to establish that someone using Defendant's IP address had sought the File Sharing Site URL "willfully and deliberately" in an effort to "satisfy a preexisting predilection." *See supra* Part III. That deficiency rendered it objectively unreasonable for a law enforcement officer to believe that the otherwise stale facts set forth in the affidavit were sufficient "to justify a finding of probable cause at that time." *McCall*, 740 F.2d at 1335–36. That is particularly true given that the government's warrant template should have put the affiant on notice that it is improper to include boilerplate collector information absent evidence in the affidavit

"t[ying] [collector] characteristics to the specific offender." *Reece*, 2017 U.S. Dist. LEXIS 220176, at 22.

Other deficiencies in the affidavit also rendered any belief in the existence of probable cause unreasonable. Most glaringly, given that the government's theory of probable cause relied entirely on the "crucial fact" that the click on the File Sharing Site URL occurred soon *after* the Bulletin Board A post, it was objectively unreasonable to rely on the affidavit when it failed to even establish that sequence of events. *See,e.g.*, J.A. 61.

V.

When, as here, an unlawful search reveals evidence of suspected criminality, we must not apply unsupported inferences to bend the law to ensure that a guilty person does not go free. And though the vileness of the crime in child pornography cases often presents a strong incentive to take liberties with the protections the Constitution affords to criminal defendants, we must guard our roles as judges to resist even that temptation. *See Coreas*, 419 F.3d at 151 ("Child pornography is so repulsive of a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules."). Because when courts give in to that temptation, "they endanger the freedom of all of us." *Id.*; *cf. United States v. Clayton*, 68 M.J. 419, 428 (C.A.A.F. 2010) (Ryan, J., dissenting) (lamenting that the majority opinion "appears to champion the idea that there is something *de minimis* about the Fourth Amendment's requirements when the thing sought by a search authorization or warrant is child pornography"). Because our Constitution does not

provide individuals suspected of committing certain crimes with less fulsome protections than individuals suspected of committing other crimes, the majority opinion's approach to analyzing the contours of constitutional rights in the digital context extends beyond cases that involve suspected distribution of child pornography. That's because cases involving alleged malfeasance committed electronically—which test the boundaries of our Fourth Amendment jurisprudence—will only increase in the coming years, as it is irrefutable that "[t]ime works changes, brings into existence new conditions and purposes." *Olmstead v. United States*, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting). "Therefore a princip[le] to be vital must be capable of wider application than the mischief which gave it birth. This is peculiarly true of Constitutions." *Id*.

With great respect for my colleagues in the majority, I must conclude that today's holding belies its claim to be "sensitive to the privacy interests at stake here." *Ante* at 25. Instead, it clings to analog technology from the internet dark age, uses unsupported inferences, and eviscerates constitutional rights for this brave new world of digital technology.

In sum, the majority's closing statements best illustrate why our disagreement is a matter of "judicial choice" rather than "judicial duty." Surely, we all agree that we "cannot ignore that many crimes are committed with just a few clicks of a mouse." *Ante* at 25. We also agree that the download of child pornography presents a particularly troubling result that can arise from a "single click."

But we disagree with the "judicial choice" that confronts us. That much is revealed in Part IV of the majority opinion:

> In cases like this, our job is to ask precisely what "a single click" reveals under the circumstances presented, and whether that information justifies searching a person's most private places for evidence of a crime.

Id. Here, the majority says that the "circumstances presented" indicate temporal proximity between the Bulletin Board A post and the URL click. Based on that circumstance alone, the majority claims that the "single click" of a URL demonstrates an intent to navigate to the URL's illicit content. But in this brave new world of digital technology, it's just not that simple.

Instead, our "judicial duty" is to guard against infringements on our constitutional rights. Unfortunately, the majority's "judicial choice" to use layers of unsupported inferences that do not meaningfully grapple with the technology at issue diminishes the constitutional rights of those who use the Internet—I say woe unto all users of the Internet.

Respectfully, I dissent.

HOME > DIGITAL > NEWS

DECEMBER 8, 2018 11:02AM PT

‘Avengers: Endgame’ Trailer Smashes 24-Hour Video Views Record

By **TODD SPANGLER**

CREDIT: COURTESY OF MARVEL STUDIOS

With the Marvel fandom’s anticipation leading up to “Avengers: Endgame,” it’s no surprise that the trailer drop set a new record for most views in its first 24 hours.

The “Avengers: Endgame” trailer was viewed 289 million times in its first 24 hours, after it was released around 5 a.m. PT Friday, according to Marvel Studios. That blasted past the previous record of 230 million views, set a little over a year ago by the studio’s “Avengers: Infinity War.” Behind that was Disney’s “The Lion King” teaser, which racked up 224.6 million views.

The views for the "Avengers: Endgame" trailer were tabulated across multiple platforms, including YouTube, Facebook and Twitter.

"Avengers: Endgame," the fourth Avengers movie and the sequel to "Infinity War," is set to hit theaters April 26, 2019.

Marvel announced the record on social media Saturday, extending thanks to "the greatest fans in the world":

> **To the greatest fans in the world, thank you for being there from the beginning til the endgame and making Marvel Studios' #AvengersEndgame the most viewed trailer in history with 289M views in 24 hours! Pic.twitter.com/Fe0MA2Gfqy**
>
> **— Marvel Entertainment (@Marvel) December 8, 2018**

"To the greatest fans in the world, thank you for being there from the beginning til the endgame and making Marvel Studios' #AvengersEndgame the most viewed trailer in history with 289M views in 24 hours!" the studio said.

The trailer also set a record for Twitter conversation for a movie trailer in the first 24 hours — with 549,000 mentions — soaring past previous record holder "Avengers: Infinity War" (389,000) and "Black Panther" (349,000).

The upcoming "Avengers: Endgame" picks up where "Infinity War" left off: Thanos has just wiped out half of all life in the universe. Seemingly facing certain

doom, Iron Man (Robert Downey Jr.) joins forces with Captain America (Chris Evans) and Black Widow (Scarlett Johansson) — and other members of the superhero crew — to rise up and fight Thanos.

Watch the "Avengers: Endgame" trailer:

https://variety.com/2018/digital/news/avengers-endgame-record-trailer-worldwide-24-hour-views-1203085074

TECH

A Japanese billionaire now has most retweeted tweet ever after offering a $923,000 prize

PUBLISHED MON, JAN 7 2019 • 7:36 AM EST

Choe Taylor SHARE □ □ □ □ □

KEY POINTS

- A tweet from Japanese billionaire Yusaku Maezawa has become the most retweeted message in history.
- Maezawa offered followers an incentive of almost $1 million to share his tweet.
- He is the founder of Japanese online clothing retailer Zozo Inc.

Japanese billionaire entrepreneur Yusaku Maezawa speaks at SpaceX's headquarters in Hawthorne, California.

Michael Sheetz | CNBC

A message from Japanese billionaire Yusaku Maezawa has become the most retweeted tweet of all time.

Maezawa took to Twitter on Saturday to give 100 randomly selected retweeters the chance to win a share of 100 million Japanese yen ($923,000).

Twitter users were given until Monday to follow Maezawa's account and retweet the promotion to be in with a chance of scooping the prize. His tweet has now been shared almost 5 million times.

Maezawa, the founder of Japanese online retailer Zozo Inc, sent the tweet after his website Zozotown posted sales of 10 billion yen in its New Year's sale. He previously gained international attention after securing a seat aboard SpaceX's inaugural tourist flight to the moon. The mission from Elon Musk's transportation company is expected to launch in 2023.

Maezawa's tweet overtook a plea from to gain enough retweets to persuade fast food chain Wendy's to award him a year's worth of free chicken nuggets.

A spokesperson for Zozo Inc was not immediately available for comment when contacted by CNBC.

https://www.cnbc.com/2019/01/07/yusaku-maezawa-has-most-retweeted-tweet-ever-after-offering-923000.html

The Intersect • Analysis

I can't believe this is why people are tweeting fake celebrity news

By Abby Ohlheiser

October 18, 2018

This is part of an occasional series in which we explain what's behind a popular meme. We like to call it memesplaining; you might call it meme-ruining. Regardless, if you just chanced upon a joke, tweet, image, app or GIF you don't understand, we have the answers — insofar as answers can be had.

The Meme: Vote Rickrolling

Rickrolling is one of the Internet's oldest memes: Trick people into clicking on a link expecting one thing but instead lead them to a video of Rick Astley singing "Never Gonna Give You Up." That's probably why the official video for the song has more than 487 million YouTube views.

In recent weeks, Rickrolling has been reborn. But instead of tricking people into listening to a song, people are using the bait of celebrity gossip to trick young people into visiting a voter registration site.

Here's an example:

> Wow I can't believe this is why Ariana Grande and Pete Davidson split up https://t.co/WQrbEBV6uD
>
> pic.twitter.com/Dc8b9azhua
>
> **— Tim (@cigelske) October 14, 2018**

How did this meme grow?

The idea of tricking people with link shorteners like bit.ly, as used in this meme, is not at all new. However, this particular version emerged as part of a larger viral campaign to increase voter registration and participation for the 2018 midterms, particularly among younger voters.

The activist and writer Ashlee Marie Preston tweeted an early, super-viral version of the current meme format.

"Welp . . . it's official . . . Kim Kardashian finally decided to divorce Kanye West . . ." she tweeted. The trick went viral: the original tweet has more than 60,000 retweets and 140,000 likes.

> Welp...it's official...Kim Kardashian finally decided to divorce Kanye West... https://t.co/C2p25mxWJO
>
> **— Ashlee Marie Preston (@AshleeMPreston) October 12, 2018**

But that doesn't quite capture the full spread of her tweet. Others, appreciating the trick, quote tweeted her and expanded on the weaponized clickbait.

> This is actually insane. Is this really how she ended it or is this fake?? https://t.co/TT5V27Djnk
>
> **— Chris Kelly (@imchriskelly) October 13, 2018**

Soon, others were making their own versions. Tim Cigelske, whose clickbait tweet about the Ariana Grande and Pete Davidson split is quoted above, was also amplified by a number of big accounts, including some celebrities. Ashton Kutcher, Colin Hanks and

James Corden all retweeted his tweet to their millions of followers.

> I normally don't care for celeb gossip about breakups but this is so sad https://t.co/gwgXXtBkM5
>
> **— Colin Hanks (@ColinHanks) October 16, 2018**

Did it work?

Well, according to data from Bit.ly, the link shortener used for these memes, quite a few people clicked on the links. Cigelske examined the aftermath of his tweet in a Medium post that he's continually updating with data on the tweet's reach. He wrote that "honestly at this point i'm not sure how many more notifications my iphone can take but we're at 1.4 MILLION CLICKS."

The tweet that inspired his clickbait — Preston's fake-out about Kanye West getting divorced — is approaching 3 million clicks.

Obviously, that doesn't necessarily translate into actual registrations, although it appears to have inspired at least a few. Cigelske has been collecting tweets from those who say the viral trick prompted them to register.

> Okay this was smart. You got me. I registered https://t.co/sYG7NkL1S4
>
> **— azari' (@azarian_delaney) October 16, 2018**

We reached out to vote.org for comment on whether this viral meme has resulted in a corresponding spike in registrations through its site. Its answer was inconclusive, but the site is optimistic about the effect of conversations about voter registration in general.

"Since the vote rolling memes started, we have seen more than 100K people under 30 register to vote. While we can't suggest they caused all the registrations, we can say all of the cultural conversations surrounding voting certainly correlate to spikes in young voters engagement," a spokeswoman said in a statement.

How can I use this meme as if I know what I'm doing?

Should you decide to participate — we'll get to the "should" later — setting up a vote rickroll is pretty easy. First, create a link to vote.org (or whatever else you want to trick people into visiting) using a link shortener such as bit.ly. Bit.ly works pretty simply: You enter in a URL, and the site spits out a shorter version. It's a relic from a time when URL length counted toward characters on Twitter but is now used to hide the original source of links. Then, choose the right piece of gossip. Cigelske capitalized on the emerging news of the Grande-Davidson split, while Preston timed her tweet to Kanye West's visit to the White House.

However, there are good reasons not to use this meme.

Please be a buzzkill on this meme for me.

Okay, sure. On Thursday, Elle magazine decided it was their turn to rickroll people into voting.

> Kim Kardashian and Kanye West are splitting up https://t.co/epwKG7aSBg pic.twitter.com/u7qqojWVlR
>
> **— ELLE Magazine (US) (@ELLEmagazine) October 18, 2018**

The tweet is a perfect encapsulation of why this meme, no matter its good intentions, is wading into tricky territory.

First, while this meme certainly is an effective way to get people to click on a link that leads to a call for civic engagement, the meme seems to promote an assumption that the people who are interested in celebrity gossip — particularly young people — are not interested in voting or democracy. Just months after a bunch of teens responded to mass shooting at their high school by launching into full-time political activism, this seems like a bit of a cynical and outdated way of viewing how younger voters understand their role in democracy.

In 2015, the Atlantic's Megan Garber identified this phenomenon as attention policing — the idea of shaming someone for liking a frivolous or unimportant topic or meme (as, in her example, #TheDress) when the world is full of tragic or important moments. But attention spent on, say, celebrity gossip is not necessarily at the expense of an important story. Giving attention and amplification to each serves different purposes in building online community,

Garber argues. Getout-the-vote efforts can go viral because of the interconnectedness of Internet culture that was built, in part, by a bunch of people caring about dumb gossip or arguments for an hour.

And, some celebrities — Ariana Grande specifically, to use one of the names taken for this meme — are already aware of the power they have to drive people's attention to important topics and movements. Grande, whose 2017 show in Manchester, England, was the target of a bombing that killed 22 people, was one of several celebrities who participated in the March for Our Lives in Washington, D.C., earlier this year.

In conclusion, fake news for a good cause is still fake news. Particularly in this Elle tweet, which comes from a publication that covers both celebrity news and politics, the virality of this meme is dependent on saying that sometimes it's okay to spread misinformation on purpose — a weird thing to assert in 2018. Plus, creating and spreading a deceptive link, and encouraging people to click through to a hidden domain of unknown safety or ownership, is not a good online hygiene practice.

more reading:

Welcome to the online search for a cursed sarcophagus that will finally end it all

By age 35, you should have saved up enough despair to understand this meme

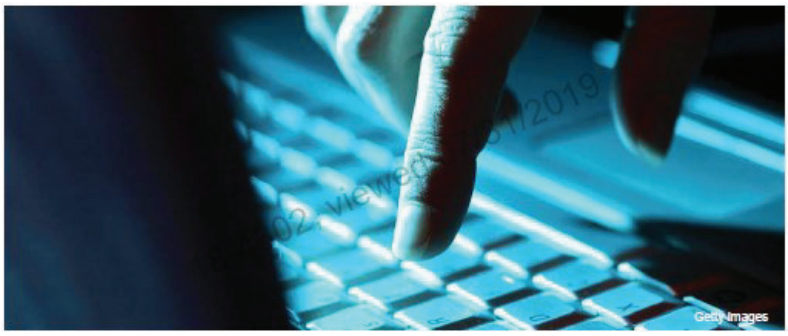
How a man's viral Instagram ode to his 'curvy' wife went from 'required reading' to mocking meme

Abby Ohlheiser Abby Ohlheiser covers digital culture for The Washington Post. She was previously a general assignment reporter for The Post, focusing on national breaking news and religion. Follow

https://www.washingtonpost.com/technology/2018/10/18/i-cant-believe-this-is-why-people-are-tweeting-fake-celebrity-news/?utm_term=.e9c493b7234d

The 5 Deadly Clicks: The Links You Should Never Touch

By **COLUMN BY ADAM LEVIN, CREDIT.COM**
Oct. 6, 2013



Here are some links to be wary of when surfing the internet.

intro: Here's a scary scenario. You're innocently surfing the Web, maybe on an unfamiliar site, not paying close attention. Suddenly your computer screen fills with illegal pornographic images of minors. You try to navigate away, but a warning screen branded by the National Security Administration's Internet Surveillance Program pops up with the message: "Your computer has been locked due to suspicion of illegal content downloading and distribution."

You are then offered a sort of Hobson's choice: Pay a fine immediately, or face prosecution for downloading child pornography.

The folks behind that scam were actually based in Russia, SC Magazine reported, not NSA headquarters. The number of people entrapped by this type of scam has been increasing exponentially. In a recent report

from McAfee, an Internet security company, there were fewer than 25,000 samples of ransomware catalogued per quarter in the first half of 2011. In the second quarter of 2013 alone, the number of new samples multiplied to more than 320,000, (which was double the number in the first quarter of this year).

“During the past two quarters we have catalogued more ransomware than in all previous periods combined,” MacAfee found. “This trend is also reflected by warnings from law enforcement and federal agencies around the globe.”

If you think the most common cyber scam still involves deposed Nigerian royalty eliciting your help to extract fortunes from African banks, your time machine has stalled. Cyber ninjas have become far more creative, sophisticated and inscrutable. With that in mind, here are five links you should never, ever click.

quicklist: title: Mobile Apps That Are Unfamiliar to You text:

It's easy to think of spam and phishing as email-based scams. But with the rise of mobile devices, scammers have added mobile apps to their repertoire. Malware attacks on Android phones grew by 35 percent to nearly 18,000 new samples in the second quarter of 2013, according to McAfee.

11 Dumb Things You do With Your Emails

It appears the onslaught will only grow worse. While the number of attempted mobile device hacks increased by just over a third, the total number of new malware applications discovered by McAfee researchers in the second quarter was double the

number found in the first. This trend suggests that cyber scam artists are honing their craft.

Mobile malware takes many forms. It could purport to come from your bank. It could trick you into paying for a fake dating app. Some scammers even "weaponize" legitimate apps, turning real programs into spying machines that siphon your location, contact and other data away from legal enterprises and funnel it into the black market.

How to Avoid It: Control the impulse! Don't just click on any app no matter how cool it seems at first blush. And just because you see it in the app store doesn't mean it's safe. Do the research to make sure it's the real deal before you download.

quicklist: title: Remote Access text:

In the latest and most popular iteration of this scam, con men pose as employees of Microsoft. They send emails, instant messages or texts with warnings that your computer has contracted a virus, and provide a link that you can click so a "Microsoft employee" can fix the problem. The thieves claim to work for different divisions of Microsoft such as Windows Helpdesk and the Microsoft Research and Development Team.

What's a Bad Credit Score?

Once the scammers gain access, they "can install malicious software, steal personal information, take control of the computer remotely or direct consumers to fraudulent websites where they are asked to enter their credit card information," according to the Better Business Bureau.

How to Avoid It: Never trust an unsolicited contact. Only provide personal information or agree to a remote access session when you initiate communication. If, for some reason, you are contacted by anyone representing an institution with which you have a relationship, always confirm the authenticity and contact information of the organization before you respond and then only to the appropriate department.

quicklist: title: Porn text:

While you mindlessly surf the Internet, you may accidentally click on sketchy ads or spam. Or perhaps you get an email with a tantalizing picture or link, which ultimately sends you to a site rife with illegal pornographic images. Such despicable lures are just one part of the larger epidemic of ransomware.

9 Things You Need to Do When Your Email Is Hacked

How to Avoid It: Pay attention! Absentminded clicking can land you in a world of pain. Also, deal with businesses that are security minded. These businesses have their websites tested at least annually for vulnerabilities, then fix the security gaps before you get trapped in them. Intentionally clicking on illegal sites, however, will (and should) entitle you to a one-way ticket to a federal sleep-away camp for a not inconsequential period of time.

quicklist: title: Authority Scams text:

Email, texts or phone calls alerting us to issues with our checking accounts, tax returns and credit cards tend to elicit knee-jerk instant responses (and are designed to do so). A natural tendency is to immediately provide whatever personal information

is required to identify ourselves and make the problem go away.

This is not lost on scammers, which is what makes "authority scams" so appealing to those on the dark side. From May 2012 through April 2013, 102,100 Internet users globally received phishing attacks every day, twice the number of recipients the previous two years, according to a report by Kapersky Lab, an Internet security company. Of those attempts, 20% involved scammers impersonating banks. Of all fake and deceptive websites, 50% of those discovered by Kapersky attempted to impersonate banks, credit card companies and other financial services such as PayPal.

How to Avoid It: Before clicking any links, entering any username or password information or flinging any kind of precious personal information into the ether, stop, take a breath and think. No reputable financial institution, or government entity, would ever ask you to provide such data via email; nor would they cold-call potential victims of fraud and request sensitive personal data. If you receive an email alerting you to fraud and requesting that you verify by email your account username and password, it is – by definition – a scam.

quicklist: title: Drug Spam text:

For nearly as long as there's been email, there's been spam. Creative criminals have used lures of all stripes to entice people into clicking on links in their emails. Email has become the "carrier" for malware. The email subject may be about a job, travel, shopping discounts, sex, news, or, the most popular, drugs. McAfee's research team has found that about 20

percent of all spam emails sent to recipients in the U.S. referenced drugs in the subject line. It's no wonder with the cost of healthcare in the U.S. that this is a particularly effective subject line. Delivery service notification, in which fraudsters claiming to be from UPS or FedEx say they could not deliver a package, came in a distant second.

How to Avoid It: Don't take the bait. Why would you buy drugs from anyone who contacts you blindly over the Internet? Your health, your bank account, or both will suffer. And, if you're expecting a package, contact the shipper directly.

These scams will continue as long as people will fall for them. It's all about fear, carelessness, curiosity or distraction -- any of which can lead to financial issues, health implications or being labeled a criminal — even a sexual predator. The convenience and access of the Internet creates vulnerabilities, opportunities and also requires personal responsibility. Before you click, weigh each against the other and do the smart thing.

This work is the opinion of the columnist and in no way reflects the opinion of ABC News.

Adam Levin is chairman and cofounder of Credit.com and Identity Theft 911. His experience as former director of the New Jersey Division of Consumer Affairs gives him unique insight into consumer privacy, legislation and financial advocacy. He is a nationally recognized expert on identity theft and credit.

https://abcnews.go.com/Business/links-click/story?id=20461918

Successful Con

Tricking people out of sensitive information online is far too easy.

QUINN NORTON

SEP 12, 2018

In *The Sting*, Robert Redford plays a con artist who built a fake reality to get his mark. On the internet, phishing attacks are a similar kind of trickery. (GETTY)

In the classic 1973 heist movie *The Sting*, two con men—played by Robert Redford and Paul Newman—build a fictitious world in a Depression-era Chicago basement to defraud a corrupt banker. They make an offtrack-betting the finest movies in the genre, well written and funny, but also because the duo's work is so meticulously detailed.

The con has changed since then, both short and long. In this age, the online equivalent of *The Sting* is a phishing site: a fake reality that lives online, set up to capture precious information such as logins and

passwords, bank-account numbers, and the other functional secrets of modern life. You don't get to see these spaces being built, but—like *The Sting*'s betting room—they can be perfect in every detail. Or they can be thrown together at the last minute like a clapboard set.

This might be the best way to think about phishing: a set built for you, to trick information out of you; built either by con men or, in the case of the recent spear-phishing attack caught and shut down by Microsoft, by spies and agents working for (or with) interfering governments, which seems a bit more sinister than Paul Newman with a jaunty smile and a straw hat.

But perhaps it should not seem so sinister, because phishing is profoundly easy to do. So easy, and comparatively cheap, that any country that isn't using it as part of its espionage strategy should probably fire its intelligence agency.

Computer security often focuses on malware: software that attacks faults in your computer to take control of it and give that control to someone else. Malware is often sophisticated software that can quietly take over a computer without being detected—from there, it can do anything, from copying every keystroke you type, to watching every page you open, to turning your camera and microphone on and recording you, to encrypting your hard drive and ransoming your computer's contents back to you. But novel malware is difficult to write, and can take many paid hours for some of the most talented programmers, in addition to finding or buying a security flaw that allows you to get your malware onto someone's computer undetected. It's painfully

expensive, and often ends up leaving a trail back to the authors.

Phishing doesn't attack computers. It attacks the people using computers.

Setting up a phishing website is something a summer intern can do in a couple of weeks, and it works. If you were to try to create a phishing version of this article, you could start by saving the complete webpage from your browser—that would get you the picture, text, and code that makes the page you're reading now. If this article contained an account login, you could put it on a server you control, and maybe register another domain, something like http://tehatlantic.com. If you enticed someone to try to use their TheAtlantic.com username and password on tehatlantic.com, you would then have that information.

This kind of phishing started out mainly as a money-stealing scheme, delivered en masse. "Phishing has changed a lot. A decade or so ago it was a mass

phenomenon of people looking for passwords to bank accounts, PayPal, eBay … anything they thought would be easily monetizable," says Cormac Herley, a principal researcher at Microsoft Research. "I think that threat has largely been beaten back: Spam filters have become better at detecting it, browsers have warning mechanisms built in, banks have become good at detecting fraud."

But that's the untargeted stuff. Enticing someone to click on a phishing link, in an email or elsewhere, is where a targeted attack, also known as spear-phishing, comes in: learning about someone's life and habits to know just what email would get them

unthinkingly to click. A reality built for one person, or one cohort of people. The con is on, the set is built, and the actors are hired to make the sting, all from a web browser.

In early 2016 a phishing email requesting an urgent payment as part of what's known as a "fake president" scam landed on the Austrian aviation-parts maker FACC's email servers. The "fake president" is generally an urgent message from an authority figure that needs Accounts Payable to send money to a foreign account at once. In the case of FACC, a dubious wire transfer followed the email, and the company lost more than 40 million euros and fired its CEO.

[Email hackers are winning.]

John Podesta, the chairman of the Hillary Clinton campaign, was famously spear-phished in 2016 by an email saying someone in Ukraine was attempting to log into his Gmail account. When he clicked the link and entered his username and password (instead of using the Google domain passed along by his own help-desk person), his account was actually captured. His emails, along with Democratic National Committee emails harvested the same way, were later leaked online, creating chaos in the run-up to the 2016 election. Most recently, Microsoft found and shut down six domains it believed were created by a group known as the Main Intelligence Directorate of the Russian army, or GRU, targeting conservative think tanks (the International Republican Institute and the Hudson Institute) and the U.S. Senate. It's not clear what exactly these phishing sites looked like, or how they worked. As far as Microsoft knows,

no one was compromised by these sites, but they also don't know how many more are out there, waiting for just the right spear-phishing email or bogus phone call to get someone to click the link.

"The phishing that persists as a real problem today is the spear-phishing for … credentials," Herley says. He has studied the economics of phishing as well as the efficacy of security advice. "This is still a very successful vector in getting a toehold on enterprise networks. It's low volume, so it's much harder to detect." In the case of political and industrial espionage, each potential victim is worth researching and getting to know—building just the right room for their own personal sting.

Phishing and malware aren't exclusive options. Blending phishing with malware can be the most potent approach, usually in the form of a well-crafted email with an important, often urgent, document attached. But it's not a document, or not just a document. It's malware, and when you click on that attachment you're telling your computer that you want to install the software, which you don't know is software. The computer obeys you, and in doing so, invisibly hands itself over to the person who sent you the software. This approach uses you to get to your computer. It's been used against journalists and activists all over the world, and probably a lot of other people, but it's the journalists and activists we hear about.

More frightening is the fact that, most of the time, a decent fake website gets an attacker whatever they need without expensive and detectable malware. You just followed a link, put in your username and

password, and maybe the page showed an error with a link that goes to the real site. Just one of those hiccups on the net that we see and forget moments later. This can be overwhelming to think about. Someone, you might reasonably say, should fix this, and by someone you mean tech companies.

The most Microsoft, Google, or any of the tech companies can do with their technology is try to detect malware and phishing sites, and stop them from talking to the internet—blocking up the door to the offtrack-betting basement. This is called "blackholing." But because spinning up a hundred basements on the internet isn't much harder than spinning up one, leaving it to tech companies won't work. The victims are the weakest link in phishing, and the tech companies can't put out reliable updates to change or prevent user behavior.

"We do invest a lot in technical fixes like better threat detection, better protection of networks, efforts like AccountGuard and Defending Democracy, and encouraging two-factor authentication for high-value accounts," Herley says. "But there's also an education component; we'd love protection to have zero asks of the user, but that's not always possible."

AccountGuard and Defending Democracy are offerings from Microsoft aimed at its most vulnerable (and political) clients, but even then, most of the offerings consist of recommendations, best practices, webinars, and notifications: attempts to patch the human.

Many security-professional and media recommendations exhort eternal vigilance, paying attention to every detail. This is terrible advice. I'm a professional with years of experience in this space and I don't bother to

inspect my emails or carefully read all my URLs: I have things to do. As a strategy for the constant level of attacks in modern email, this approach has failed, even in dealing with the amateurish mass-phishing attacks we've seen over the past 10 years.

Spear-phishing, especially political spear-phishing, is even harder to catch with vigilance. The inconsistency of security advice has contributed to the disaster with ideas that are hard to implement, don't make sense, and don't work, but that security and IT departments yell at people with all the fury of revivalist preachers. It's exhausting.

Developing a few good habits based on how this computer you're using works is relatively easy and more effective than paranoia. Turn on two-factor authentication where you can, where it's available on sites you use. This includes things such as RSA tokens, Yubikeys, Google Authenticator, and SMS verification codes, which create something needed to log in beyond a password and a username so that if your username and password are stolen or leaked, attackers still can't take over your accounts. Apply software updates. Or, better yet, Herley suggests letting your computer do it for you. "I'd say use automatic updates … We invest heavily in [fixes] as soon as we figure out things are wrong. You want all that goodness working for you."

Set up regular backups that require minimal effort from you. "You don't have to worry as much about ransomware [or theft, or disk crashes] … if you know you can always get your stuff back," Herley says. Use long, complex, and unique passwords, but make it easy on yourself. "Write them down or use a password manager," Herley says.

[How long until the next big ransomware attack?]

I'd strongly recommend the password manager, but not directly for security purposes. Password managers are easy and will autofill your password on sites you've used before—even less effort. There's most likely one built into the browser or operating system you're using now, but if you want to get fancy, you can use an online password-management system that syncs between devices. Don't reuse passwords, and go ahead and change your password on the sites where you know you've reused passwords. This is an hour or two of pain, but only one time. You are not likely to leak your password onto the internet, but a site you use almost certainly will at some point. You can also sign up at Have I Been Pwned to find out which of your passwords have already leaked onto the internet.

Don't follow links you get sent to sites on which you have an account—you have your own bookmarks and browser history, which already go to the right site for sure. If you get an email from your bank or, say, think-tank employer, log in on your web browser. You're going to have to do that anyway, so you might as well follow your own link. One habit that would take some work to change but does the most to secure you from malware is not opening email attachments on your own computer. Have people put files in a file-locker site, something like Dropbox, and open documents in a remote service like Google Docs. Make it someone else's IT department's problem.

Don't try to be perfect. Just try to be expensive for the con artist. Make them work hard enough, and you're not worth the bother. Right now, most computer

users, whether they are political consultants, CEOs, scientists, or researchers, aren't very hard to con.

Understanding all of this, the news of phishing campaigns takes on a different tone. Rather than asking why there are groups linked to Russia phishing our politics, the question is: Why aren't more governments phishing U.S. companies and agencies? Perhaps they are, and we just don't notice. Whatever the reason, people need to talk about phishing, as much as they need to update their software. Because striving to understand complex phenomena is how humans are updated over time, and it's how we make it as expensive and difficult to hack humans as it is to hack computers.

We want to hear what you think about this article. Submit a letter to the editor or write to letters@theatlantic.com.

https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-successful-con/569920

The Washington Post

Personal Finance

Can you tell the real TurboTax email from the scam?

By Jonnelle Marte

March 1, 2016

TurboTax and other tax software companies told customers this year that they would be sending more emails and other alerts in an effort to fight tax fraud.

But they aren't the only ones sending more emails — scammers are, too. And in many cases, it's nearly impossible to tell the phony emails from the real ones.

The Internal Revenue Service said the number of reported phishing scams from fraudsters pretending to be from the IRS or a tax company surged by 400 percent this year from the same time last year. The 1,389 scams reported as of mid-February added up to about half of the email scams reported for all of last year, the agency said.

Julie Miller, a spokeswoman for Intuit, the maker of TurboTax, said the company has seen a spike in the number of phishing scams from fraudsters pretending to be TurboTax. The scams generally try to persuade people to click on malicious links by saying the action is needed to help users confirm their accounts or verify the taxpayer's identity. Others say users could be blocked from their accounts if they don't take action or could pretend to remind people to get started on their tax returns.

For taxpayers, it can be difficult to tell fact from fiction. Although some of the emails are barren and easy to question, some are more sophisticated, including company logos or other design traits that look similar to the emails being sent by TurboTax and other companies.

Take this fraudulent email that TurboTax is warning people about on its website. It looks strikingly similar to the reminders taxpayers might receive from TurboTax, encouraging them to sign in and start working on their tax returns. The colors and logos are nearly identical, as is the layout of the page.

Although there are some minor stylistic differences in font color, they are pretty difficult to notice. And just because an email has some personal information, such as your name or employer, doesn't mean that it's legitimate, Miller says.

Some people may be tempted to ignore the emails altogether, but that could have consequences if it means missing out on a real warning sign. This year, for instance, Intuit started alerting customers after their password or bank account information was changed — red flags that someone else may have accessed their account. Intuit is also alerting customers if a second account is opened with their Social Security number, which could point to a criminal using TurboTax to file a fraudulent return in their name.

For most taxpayers, the best line of defense is to do research before opening emails and to avoid clicking on links. Users can hover over a link to see what URL they are being directed to, Miller says. If the link isn't to the website for the company you're trying to reach,

don't click on it, she says. The smarter move may be to go directly to the website of the company you're trying to contact by typing its URL (not the one in the email) into the browser and to look there for a customer service number.

TurboTax customers can check Intuit's website to see if the email matches one of scams that Intuit already knows about. It's a pretty long list, but if the email you received isn't there, you can also forward the email to spoof@intuit.com and the company will let you know whether the email is legitimate.

You might also like:

The IRS says hackers stole data for twice as many taxpayers as initially expected

Criminals want your tax returns. Here's what you can do about it.

Tax Day is coming fast. Test your knowledge here.

Jonnelle Marte

Jonnelle Marte is a reporter covering personal finance. She was previously a writer for MarketWatch and the Wall Street Journal. Follow

https://www.washingtonpost.com/news/get-there/wp/2016/03/01/can-you-tell-which-of-these-turbotax-emails-is-real-and-which-one-is-from-a-scam-artist/?utm_term=.7ba2976355cb

BUSINESS CORPORATE FINANCE & ACCOUNTING

Compound Probability

REVIEWED BY JULIA KAGAN | Updated Apr 29, 2019

What is Compound Probability?

Compound probability is a mathematical term relating to the likeliness of two independent events occurring. Compound probability is equal to the probability of the first event multiplied by the probability of the second event. Compound probabilities are used by insurance underwriters to assess risks and assign premiums to various insurance products.

Understanding Compound Probability

The most basic example of compound probability is flipping a coin twice. If the probability of getting heads is 50 percent, then the chances of getting heads twice in a row would be (.50 X .50), or .25 (25 percent). A compound probability combines at least two simple events, also known as a compound event. The probability that a coin will show heads when you toss only one coin is a simple event.

As it relates to insurance, underwriters may wish to know, for example, if both members of a married couple will reach the age of 75, given their independent probabilities. Or, the underwriter may want to know the odds that two major hurricanes hit a given geographical region within a certain time frame. The results of their math will determine how much to charge for insuring people or property.

KEY TAKEAWAYS

- Compound probability is the product of probabilities of occurrences for two independent events known as compound events.
- The formula for calculation of compound probabilities differs based on the type of compound event, whether it is mutually exclusive or mutually inclusive.

Compound Events and Compound Probability

There are two types of compound events: mutually exclusive compound events and mutually inclusive compound events. A mutually exclusive compound event is when two events cannot happen at the same time. If two events, A and B, are mutually exclusive, then the probability that either A or B occurs is the sum of their probabilities. Meanwhile, mutually inclusive compound events are situations where one event cannot occur with the other. If two events (A and B) are inclusive, then the probability that either A or B occurs is the sum of their probabilities, subtracting the probability of both events occurring.

Compound Probability Formulas

There are different formulas for calculating the two types of compound events: Say A and B are two events, then for mutually exclusive events: *P(A or B) = P (A) + P(B).* For mutually inclusive events, *P (A or B) = P(A) + P(B) - P(A and B).*

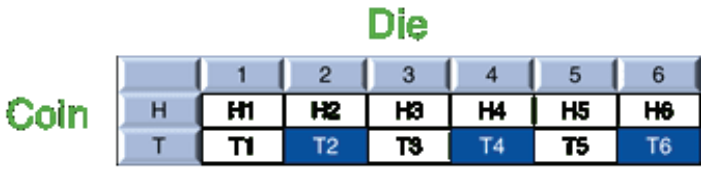
Using the organized list method, you would list all the different possible outcomes that could occur. For example, if you flip a coin and roll a die, what is the

probability of getting tails and an even number? First, we need to start by listing all the possible outcomes we could get. (H1 means flipping heads and rolling a 1.)

H1	T1
H2	T2
H3	T3
H4	T4
H5	T5
H6	T6

The other method is the area model. To illustrate, consider again the coin flip and roll of the die. What is the compound probability of getting tails and an even number?

Start by making a table with the outcomes of one event listed on the top and the outcomes of the second event listed on the side. Fill in the cells of the table with the corresponding outcomes for each event. Shade in the cells that fit the probability.



In this example, there are twelve cells and three are shaded. So the probability is: P = 3/12 = 1/4 = 25 percent.

These Are Your 3 Fiduciary Financial Advisor Matches

Finding the right financial advisor that fits your needs doesn't have to be hard. SmartAsset's free tool matches you with fiduciary financial advisors in your

area in 5 minutes. Each advisor has been vetted by SmartAsset and is legally bound to act in your best interests. If you're ready to be matched with local advisors that will help you achieve your financial goals, get started now.

Compare Investment Accounts

PROVIDER	E*TRADE	MERRILL A BANK OF AMERICA COMPANY	charles SCHWAB
NAME	E*TRADE	Merrill Edge	Charles Schwab
DESCRIPTION	E*TRADE has $0 commissions for online stock, ETF and options trades. Start trading today!	300 $0 online stock and ETF trades, no minimum deposit required	$0 online stock, ETF, and options commissions. It's time to trade up.
	LEARN MORE	**LEARN MORE**	**LEARN MORE**

http://www.investopedia.com/terms/c/compound-probability.asp

Viruses Frame PC Owners for Child Porn

NOVEMBER 9, 2009 / 12:49 PM / CBS / AP

Of all the sinister things that Internet viruses do, this might be the worst: They can make you an unsuspecting collector of child pornography.

Heinous pictures and videos can be deposited on computers by viruses – the malicious programs better known for swiping your credit card numbers. In this twist, it's your reputation that's stolen.

Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught. Pranksters or someone trying to frame you can tap viruses to make it appear that you surf illegal Web sites.

Whatever the motivation, you get child porn on your computer – and might not realize it until police knock at your door.

An Associated Press investigation found cases in which innocent people have been branded as pedophiles after their co-workers or loved ones stumbled upon child porn placed on a PC through a virus. It can cost victims hundreds of thousands of dollars to prove their innocence.

Their situations are complicated by the fact that actual pedophiles often blame viruses – a defense rightfully viewed with skepticism by law enforcement.

"It's an example of the old 'dog ate my homework' excuse," says Phil Malone, director of the **Cyberlaw Clinic at Harvard's Berkman Center for**

Internet & Society. "The problem is, sometimes the dog does eat your homework."

The AP's investigation included interviewing people who had been found with child porn on their computers. The AP reviewed court records and spoke to prosecutors, police and computer examiners.

One case involved Michael Fiola, a former investigator with the Massachusetts agency that oversees workers' compensation.

In 2007, Fiola's bosses became suspicious after the Internet bill for his state-issued laptop showed that he used 4½ times more data than his colleagues. A technician found child porn in the PC folder that stores images viewed online.

Fiola was fired and charged with possession of child pornography, which carries up to five years in prison. He endured death threats, his car tires were slashed and he was shunned by friends.

Fiola and his wife fought the case, spending $250,000 on legal fees. They liquidated their savings, took a second mortgage and sold their car.

An inspection for his defense revealed the laptop was severely infected. It was programmed to visit as many as 40 child porn sites per minute – an inhuman feat. While Fiola and his wife were out to dinner one night, someone logged on to the computer and porn flowed in for an hour and a half.

Prosecutors performed another test and confirmed the defense findings. The charge was dropped – 11 months after it was filed.

The Fiolas say they have health problems from the stress of the case. They say they've talked to dozens of lawyers but can't get one to sue the state, because of a cap on the amount they can recover.

"It ruined my life, my wife's life and my family's life," he says.

The **Massachusetts attorney general's office**, which charged Fiola, declined interview requests.

At any moment, about 20 million of the estimated 1 billion Internet-connected PCs worldwide are infected with viruses that could give hackers full control, according to security software maker F-Secure Corp. Computers often get infected when people open e-mail attachments from unknown sources or visit a malicious Web page.

Pedophiles can tap viruses in several ways. The simplest is to force someone else's computer to surf child porn sites, collecting images along the way. Or a computer can be made into a warehouse for pictures and videos that can be viewed remotely when the PC is online.

"They're kind of like locusts that descend on a cornfield: They eat up everything in sight and they move on to the next cornfield," says Eric Goldman, academic director of the **High Tech Law Institute at Santa Clara University**. Goldman has represented Web companies that discovered child pornographers were abusing their legitimate services.

But pedophiles need not be involved: Child porn can land on a computer in a sick prank or an attempt to frame the PC's owner.

In the first publicly known cases of individuals being victimized, two men in the United Kingdom were cleared in 2003 after viruses were shown to have been responsible for the child porn on their PCs.

In one case, an infected e-mail or pop-up ad poisoned a defense contractor's PC and downloaded the offensive pictures.

In the other, a virus changed the home page on a man's Web browser to display child porn, a discovery made by his 7-year-old daughter. The man spent more than a week in jail and three months in a halfway house, and lost custody of his daughter.

Chris Watts, a computer examiner in Britain, says he helped clear a hotel manager whose co-workers found child porn on the PC they shared with him.

Watts found that while surfing the Internet for ways to play computer games without paying for them, the manager had visited a site for pirated software. It redirected visitors to child porn sites if they were inactive for a certain period.

In all these cases, the central evidence wasn't in dispute: Pornography was on a computer. But proving how it got there was difficult.

Tami Loehrs, who inspected Fiola's computer, recalls a case in Arizona in which a computer was so "extensively infected" that it would be "virtually impossible" to prove what an indictment alleged: that a 16-year-old who used the PC had uploaded child pornography to a Yahoo group.

Prosecutors dropped the charge and let the boy plead guilty to a separate crime that kept him out of jail,

though they say they did it only because of his age and lack of a criminal record.

Many prosecutors say blaming a computer virus for child porn is a new version of an old ploy.

"We call it the SODDI defense: Some Other Dude Did It," says James Anderson, a federal prosecutor in Wyoming.

However, forensic examiners say it would be hard for a pedophile to get away with his crime by using a bogus virus defense.

"I personally would feel more comfortable investing my retirement in the lottery before trying to defend myself with that," says forensics specialist Jeff Fischbach.

Even careful child porn collectors tend to leave incriminating e-mails, DVDs or other clues. Virus defenses are no match for such evidence, says Damon King, trial attorney for the U.S. Justice Department's **Child Exploitation and Obscenity Section**.

But while the virus defense does not appear to be letting real pedophiles out of trouble, there have been cases in which forensic examiners insist that legitimate claims did not get completely aired.

Loehrs points to Ned Solon of Casper, Wyo., who is serving six years for child porn found in a folder used by a file-sharing program on his computer.

Solon admits he used the program to download video games and adult porn – but not child porn. So what could explain that material?

Loehrs testified that Solon's antivirus software wasn't working properly and appeared to have shut off for long stretches, a sign of an infection. She found no evidence the five child porn videos on Solon's computer had been viewed or downloaded fully. The porn was in a folder the file-sharing program labeled as "incomplete" because the downloads were canceled or generated an error.

This defense was curtailed, however, when Loehrs ended her investigation in a dispute with the judge over her fees. Computer exams can cost tens of thousands of dollars. Defendants can ask the courts to pay, but sometimes judges balk at the price. Although Loehrs stopped working for Solon, she argues he is innocent.

"I don't think it was him, I really don't," Loehrs says. "There was too much evidence that it wasn't him."

The prosecution's forensics expert, Randy Huff, maintains that Solon's antivirus software was working properly. And he says he ran other antivirus programs on the computer and didn't find an infection – although security experts say antivirus scans frequently miss things.

"He actually had a very clean computer compared to some of the other cases I do," Huff says.

The jury took two hours to convict Solon.

"Everybody feels they're innocent in prison. Nobody believes me because that's what everybody says," says Solon, whose case is being appealed. "All I know is I did not do it. I never put the stuff on there. I never

saw the stuff on there. I can only hope that someday the truth will come out."

But can it? It can be impossible to tell with certainty how a file got onto a PC.

"Computers are not to be trusted," says Jeremiah Grossman, founder of WhiteHat Security Inc. He describes it as "painfully simple" to get a computer to download something the owner doesn't want – whether it's a program that displays ads or one that stores illegal pictures.

It's possible, Grossman says, that more illicit material is waiting to be discovered.

"Just because it's there doesn't mean the person intended for it to be there – whatever it is, child porn included."

First published on November 9, 2009 / 12:49 PM

https://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn

Robert Siciliano CSP, Contributor
Personal Security, Privacy, Cyber Safety and Identity Theft Expert

Why Is Child Pornography on Your PC?

03/18/2010 05:12 am ET | **Updated** Dec 06, 2017

Anti-virus protection, critical security patches, and a secure wireless connection have always been essential processes on my networks. My main concern has always been to protect my bank account by keeping the bad guy out.

In my presentations, I've always stressed the importance of making sure your wireless connection is secured to prevent skeevy sex offender neighbors or wackos parked in front of your business from surfing for child porn and downloading it to your PC.

Once a predator uses your Internet connection to go to into the bowels of the web, your Internet Protocol address, which is connected to your ISP billing address, is now considered one that is owned by a criminal. If law enforcement happens to be chatting with that a person who is using your Internet connection to trade lurid child porn, then someone may eventually knock on your door at 3 AM with a

battering ram. And in another freakish and relatively new twist, hackers can use a virus to crack your network and gain remote control access, and then store child porn on your hard drive.

An AP investigation found plenty of people who have been victimized in this way. Maybe their PCs were being used as a virtual server, or maybe they were being framed by someone with a vendetta against them, but either way, they had child pornography planted on their computers. Once that porn is discovered by a friend, family member, or computer technician, the victim is arrested.

This is the kind of "breach" that can cost you thousands in legal fees, your marriage, relationships, your job, and your standing in society. In one case, a virus changed the default home page on a man's PC, and his seven year old daughter discovered it. The guy was arrested and eventually lost custody of his daughter. And you think you've got problems.

When you click a link in an email or a pop up advertisement in your browser, you may inadvertently download one of these viruses, which can then visit child pornography websites and download files onto your hard drive.

It also important to point out that most criminal investigators will say that "a virus put the child porn on my PC" is a bunch of hooey and a common defense used by the presumed innocent until proven guilty. Simply don't give anyone a chance to doubt by doing the following:

Dont be a scumbag child pornographer. Where there's smoke there's usually fire.

Make sure your anti virus up to date and set to run automatically.

Update your web browser to the latest version. An out of date web browser is often riddled with holes worms can crawl through.

Update your operating systems critical security patches automatically

Lock down your wireless internet connection with the WPA security protocol.

Invest in Intelius Identity Theft Protection. While not all forms of identity theft can be prevented, you can effectively manage your personal identifying information by knowing what's buzzing out there in regards to YOU. "Disclosures"

Robert Siciliano Identity Theft Speaker discussing viruses on Fox News.

https://www.huffpost.com/entry/why-is-child-pornography_b_356539?

[ENTERED: August 1, 2019]

FILED: August 1, 2019

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-4302
(1:17-cr-00302-LMB-1)

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

NIKOLAI BOSYK

Defendant - Appellant

ELECTRONIC FRONTIER FOUNDATION

Amicus Supporting Appellant

J U D G M E N T

In accordance with the decision of this court, the judgment of the district court is affirmed.

This judgment shall take effect upon issuance of this court's mandate in accordance with Fed. R. App. P. 41.

/s/ PATRICIA S. CONNOR, CLERK

[ENTERED: May 7, 2018]

AO 245 S (Rev. 2/99)(EDVA rev. 1) Sheet 1 - Judgment in a Criminal Case

UNITED STATES DISTRICT COURT
Eastern District of Virginia
Alexandria Division

UNITED STATES OF AMERICA

v. Case Number 1:17CR00302-001

NIKOLAI BOSYK,

Defendant.

JUDGMENT IN A CRIMINAL CASE

The defendant, NIKOLAI BOYSK, was represented by Mark B. Williams, Esquire.

The defendant pleaded guilty to Count 1 of the Indictment. Accordingly, the defendant is adjudged guilty of the following count, involving the indicated offense:

Title & Section	Nature of Offense	Date Offense Concluded	Count Number
18 U.S.C. § 2252(a)(2)	**Receipt of Child Pornography (Felony)**	**11/18/2015**	**1**

On motion of the United States, the Court has dismissed Count 2 of the Indictment.

As pronounced on May 7, 2018, the defendant is sentenced as provided in pages 2 through 8** of this Judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

IT IS FURTHER ORDERED that the defendant shall notify the United States Attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid.

Signed this 7th day of May, 2018.

/s/
Leonie M. Brinkema
United States District Judge

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a term of SIXTY (60) MONTHS, with credit for time served.

The Court makes the following recommendations to the Bureau of Prisons:

> The defendant to be designated to F.C.I. Allenwood, Pennsylvania.
>
> The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons as notified by the United States Marshal. Until he self surrenders, the defendant shall remain under the Order

** Page 8 of this document contains sealed information

Setting Conditions of Release entered on October 24, 2017.

RETURN

I have executed this Judgment as follows:

_____

_____

_____

Defendant delivered on _____ to _____ at _____, with a certified copy of this Judgment.

c: P.O. (2) (3)
Mshl. (4) (2)
U.S.Atty.
U.S.Coll.
Dft. Cnsl.
PTS
Financial
Registrar
ob

_____
United States Marshal

By _____
Deputy Marshal

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of TEN (10) YEARS.

The Probation Office shall provide the defendant with a copy of the standard conditions and any special conditions of supervised release.

The defendant shall report to the probation office in the district to which the defendant is

released within 72 hours of release from the custody of the Bureau of Prisons.

While on supervised release, the defendant shall not commit another federal, state, or local crime.

While on supervised release, the defendant shall not illegally possess a controlled substance.

While on supervised release, the defendant shall not possess a firearm or destructive device.

If this judgment imposes a fine or a restitution obligation, it shall be a condition of supervised release that the defendant pay any such fine or restitution in accordance with the Schedule of Payments set forth in the Criminal Monetary Penalties sheet of this judgment.

STANDARD CONDITIONS OF SUPERVISED RELEASE

The defendant shall comply with the standard conditions that have been adopted by this Court (set forth below):

1) The defendant shall not leave the judicial district without the permission of the Court or probation officer.

2) The defendant shall report to the probation officer and shall submit a truthful and complete written report within the first five days of each month.

3) The defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer.

4) The defendant shall support his or her dependents and meet other family responsibilities.

5) The defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other acceptable reasons.

6) The defendant shall notify the Probation Officer within 72 hours, or earlier if so directed, of any change in residence.

7) The defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any narcotic or other controlled substance, or any paraphernalia related to such substances, except as prescribed by physician.

8) The defendant shall not frequent places where controlled substances are illegally sold, used, distributed or administered.

9) The defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer.

10) The defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer.

11) The defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer.

12) The defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the Court.

13) As directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

SPECIAL CONDITIONS OF SUPERVISION

While on supervised release, pursuant to this Judgment, the defendant shall also comply with the following additional conditions:

1. The defendant shall undergo a mental health evaluation and, if recommended, participate in a program approved by the United States Probation Office for mental health treatment with an emphasis on sex offender treatment. The defendant shall take all medications as prescribed and waive all rights of confidentiality regarding mental health treatment to allow the release of information to the United States Probation Office and authorize communication between the probation officer and the treatment provider. The defendant to pay all costs as able as directed by the probation officer.

2. Pursuant to the Adam Walsh Child Protection and Safety Act of 2006, the defendant shall register with the State Sex Offender Registration Agency in any state where the defendant resides, is employed, carries on a vocation, or is a student, according to federal and state Law and as directed by the probation officer.

3. The defendant shall have no contact with minors unless supervised by a competent, informed adult, and approved in advance by the probation officer.

4. The defendant shall not engage in employment or volunteer services that allow him access to minors.

5. The defendant shall comply with the requirements of the Computer Monitoring Program as administered by the Probation Office. The defendant shall consent to the installation of computer monitoring software on any computer to which the defendant has access. Installation shall be performed by the probation officer. The software may restrict and/or record any and all activity on the computer, including the capture of keystrokes, application information, internet use history, email correspondence, and chat conversations. A notice will be placed on the computer at the time of installation to warn others of the existence of the monitoring software. The defendant shall also notify others of the existence of the monitoring software. The defendant shall not remove, tamper with, reverse engineer, or in any way circumvent the software. **Costs are waived.**

6. The defendant shall not use a computer to access any kind of pornography at any location, including employment, internet service providers, bulletin board systems, or any other public or private computer network.

7. The defendant shall make a good faith effort to pay his full restitution obligation during supervised release with minimum monthly payments of $200.00, to begin 60 days after release from custody.

8. The defendant shall waive all rights of confidentiality and provide the probation officer access to any requested financial information.

9. As directed by the probation officer, the defendant shall apply all monies received from tax refunds, lottery winnings, inheritances, judgments, and any anticipated or unexpected financial gains, to the outstanding court ordered financial obligation.

10. Although mandatory drug testing is waived pursuant to 18 U.S.C §3564 (a)(4), the defendant must remain drug free and his probation officer may require random drug testing at any time. Should a test indicate drug use, then the defendant must satisfactorily participate in, and complete, any inpatient or outpatient drug treatment to which defendant is directed by the probation officer.

CRIMINAL MONETARY PENALTIES

The defendant shall pay the following total monetary penalties in accordance with the schedule of payments set out below.

Count	Special Assessment	Fine
1	$100.00	0.00
Total	**$100.00**	**0.00**

FINE

No fines have been imposed in this case.

SCHEDULE OF PAYMENTS

Payments shall be applied in the following order: (1) assessment; (2) restitution; (3) fine principal; (4) cost of prosecution; (5) interest; (6) penalties.

The special assessment is due in full immediately. If not paid immediately, the Court authorizes the deduction of appropriate sums from the defendant's account while in confinement in accordance with the applicable rules and regulations of the Bureau of Prisons.

Any special assessment, restitution, or fine payments may be subject to penalties for default and delinquency.

If this judgment imposes a period of imprisonment, payment of Criminal Monetary penalties shall be due during the period of imprisonment.

All criminal monetary penalty payments are to be made to the Clerk, United States District Court, except those payments made through the Bureau of Prisons' Inmate Financial Responsibility Program.

RESTITUTION AND FORFEITURE

RESTITUTION

TO BE DETERMINED WITHIN 60 DAYS

Payments of restitution are to be made to Clerk, U. S. District Court, 401 Courthouse Square, Alexandria, VA 22314.

Restitution is due and payable immediately and shall be paid in equal monthly payments of at least $200.00 to commence within 60 days of release, until paid in full.

Interest on Restitution has been waived.

If there are multiple payees, any payment not made directly to a payee shall be divided proportionately among the payees named unless otherwise specified here:

FORFEITURE

Forfeiture is directed in accordance with the Consent Order of Forfeiture entered by this Court on May 7, 2018.

[ENTERED: October 9, 2019]

FILED: October 9, 2019

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-4302
(1:17-cr-00302-LMB-1)

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

NIKOLAI BOSYK,

Defendant – Appellant.

ELECTRONIC FRONTIER FOUNDATION,

Amicus Supporting Appellant.

O R D E R

The court denies the petition for rehearing en banc.

A requested poll of the court failed to produce a majority of judges in regular active service and not disqualified who voted in favor of rehearing en banc. Chief Judge Gregory, Judge Wilkinson, Judge Niemeyer, Judge Motz, Judge King, Judge Agee,

Judge Keenan, Judge Diaz, Judge Floyd, Judge Thacker, Judge Harris, Judge Richardson, Judge Quattlebaum, and Judge Rushing voted to deny rehearing en banc. Judge Wynn voted to grant rehearing en banc and filed a separate statement.

Entered at the direction of Judge Diaz.

For the Court

/s/ Patricia S. Connor, Clerk

WYNN, Circuit Judge, statement in the denial of rehearing en banc:

The Government in this matter leads this Court to depart from the wisdom of our sister circuits and endorse an unsustainable approach to evaluating evolving technology. At the core of this matter is the Government's affidavit which states that someone using Defendant's IP address was in the wrong place at a certain time. Not at the wrong time—just at a certain time.

As I discussed in my dissent, reasoning by analogy depends on relevant similarity. To many courts, the internet is abstract and the task of learning what a URL is—or what a dynamic URL is, or what a URL shortener does, and what the implications may be—represents a specialized undertaking unrelated to legal expertise, that is, something to approach with a sense of dread. Tools like analogies that promise to reduce a technical issue to something susceptible to the intuitive logic of the familiar become appealing. And retrospective confirmation, such as when we can look back and see that an affidavit led to a computer filled with child

pornography, builds trust that the logic that found probable cause was sound in the first instance. However, legal commentators have raised the alarm about indiscriminate use of metaphors in the internet context. *See, e.g.,* Mark A. Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 542 (2003) ("The cyberspace as place metaphor can be valuable . . . [but t]he metaphor will serve its purpose only if we understand its limitations—the ways in which the Internet is not like the physical world."). Sometimes, the preference to avoid taking the internet on its own terms, to avoid learning new rules and starting from logical scratch, leads us to not question basic assumptions when we should. This is one of those cases.

I offer a comparison of two analogies to illustrate the problem. Both start with what seems like a reasonable general metaphor that describes how a human user experiences the internet. After that point, however, based on the initial choice of metaphor, each analogy naturally takes a different path, and the two analogies ultimately suggest opposing conclusions. Both conclusions are "right" according to their analogy's logic. But by the time they reach those conclusions, both analogies have become somewhat divorced from reality and in neither case can we go back and "check our work" without reference to the technology that we are trying to describe.

In the first analogy, we begin in a building. This building is the confines of the internet. We are standing in a room and this room is a section of an internet forum, Bulletin Board A. We see a door with a sign that advertises child pornography. The door is

the download link URL that was posted on Bulletin Board A. We open that door and encounter both a cache of child pornography and the Defendant. If we believe the door we used was the only door to that place—indeed, so long as the number of doors into the room is a manageable number, or so long as we speculate on the basis of proximity that only places like Bulletin Board A have doors that lead here—we can reasonably conclude that Defendant is seeking child pornography.

In the second analogy, we begin on a field. That field is the vastness of the internet. The general area where we are standing is Bulletin Board A. We see a sign that points in a direction and advertises child pornography. That sign is the link posted on Bulletin Board A. We follow the sign's instructions and eventually reach a place, where there is a cache of child pornography on the ground. We also encounter Defendant in the immediate vicinity, but we did not see where he came from. Because there are no walls in this environment to direct traffic, we cannot reasonably conclude that Defendant, like us, followed the sign advertising child pornography.

This second analogy does not seek to explain the internet, rather, it seeks to explain how a foundational fault in the Government's logic skewed the Government's conclusion. The Government, the magistrate judge, the district court, and the majority in this case read the affidavit using an inapplicable logic of enclosure. They assumed limitations—represented by walls—that do not exist online. That said, the field analogy is also misleading in its own way. The field's openness suggests that we can and do see exactly where a link will take us, which, as the

amicus curiae in this case explained, is not the case. The field analogy also risks spiraling into a detailed and unhelpful geography if used to explain the role of the File Sharing Site. Every analogy can only go so far. This is why courts depend on *amici curiae* and, more importantly, the parties themselves, to explain technical issues in cases like this one, and to explain them well. *See, e.g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 306 n.1 (3d Cir. 2010) (thanking a group of *amici* led by the Electronic Frontier Foundation for participating in a case involving an *ex parte* application by the government and an issue of first impression related to the Stored Communications Act and cell site location information).

Examining the affidavit in this case, it is technological error to conclude that "the records showed that . . . someone using this IP address clicked *that same link*." *United States v. Bosyk*, 933 F.3d 319, 323 (4th Cir. 2019) (emphasis added). Indeed, the affidavit does not make this direct causal allegation. The affidavit represented that some number of hours before or some number of hours after some anonymous actor posted *a certain* link on *a certain* website, someone using Defendant's IP address came into contact with *some* link that was perhaps found on *some* website.

The affidavit does not say that the Defendant's IP address had ever been associated with any child pornography activity in the past. The affidavit does not say the person using Defendant's IP address actually downloaded any of the password-protected files. The affidavit does not even say that the person

with Defendant's IP address arrived at the URL in question after the suspect link was posted on the monitored website—a bar so low that it is alarming that the affidavit tripped over it. We know from other cases in other circuits that such facts are relevant to finding probable cause. *See, e.g., United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006). These kinds of facts, however, are all missing here.

In the digital age, the ubiquity of link shortening services and randomly generated URLs renders browsing the Internet a great exercise in trusting strangers. The average internet user does not—indeed, cannot—know with certainty that all the links they follow will take them where they expect. The system works because we follow links on faith. What, then, should a court assume when an affidavit alleges nothing more than that a single click occurred? Very little, if anything.