Case No. 18-4302

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

NIKOLAI BOSYK,

Defendant-Appellant.

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

On Appeal from the U.S. District Court for the Eastern District of Virginia
The Honorable Leonie M. Brinkema, U.S. District Court Judge
Case No. 1:17-cr-00302-LMB-1

Sophia Cope
Counsel of Record
Stephanie Lacambra
Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
sophia@eff.org

Counsel for Amicus Curiae

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of *amicus*.

Dated: August 30, 2018

Respectfully submitted,

/s/ Sophia Cope

Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel of Record for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization working to protect and promote fundamental liberties in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support free expression, privacy, and transparency in the information society. EFF has over 40,000 dues-paying members, distributes its newsletter to over 400,000 users, and represents technology users' interests in court cases and broader policy debates involving the Fourth Amendment and its relationship to technology.

EFF has served as *amicus* in the U.S. Supreme Court, the Fourth, Seventh, and Ninth Circuits, as well as district courts, and a number of state courts involving the application of the Fourth Amendment to rapidly-developing technology. *See Riley v. State of California*, (No. 13-132 & 13-212) 134 S.Ct 2473 (2014) (warrantless search of a cellphone); *U.S. v. Robert McLamb*, (No. 17-4299) 880 F.3d 685 (4th Cir. 2018) (government hacking of digital devices); *U.S. v. Kolsuz*, (No. 16-4687) 890 F.3d 133 (4th Cir. 2016) (warrantless search of digital devices

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

at the border); *U.S. v. Wanjiku*, (No. 18-1973) (7th Cir. 2018) (same); *U.S. v. Gartenlaub*, (No. 16-50339) (9th Cir. 2017) (overbreadth of domestic FISA search); *State of Maryland v. Andrews*, (No. 1496) 227 Md.App 350 (Md. Ct. Spec. App. 2016) (warrantless use of a cell site simulator); *Massachusetts v. Keown*, (No. SJC-10593) 478 Mass. 232 (Mass. 2017) (ex ante search protocols for digital searches).

INTRODUCTION

This appeal presents an issue of first impression in this Court: whether the act of accessing a website link whose Uniform Resource Locator ("URL") does not reveal that the corresponding website contains contraband material can, by itself, provide probable cause to search the residence of a user alleged to have accessed the link.

Here, the government was investigating a website dedicated to the dissemination of child pornography, described as "Bulletin Board A." During its investigation, the government found a post on Bulletin Board A that contained links to a file-sharing service that it believed was being used to store and exchange password-protected files containing child pornography. The government identified the URLs associated with the links to the file-sharing service that led to several of these password-protected files. It then sought and received a list of IP addresses from the file-sharing service that had accessed the URLs. It is unclear whether those IP addresses had actually downloaded any files, much less been able to access them, as they were password-protected. Having determined that one of these IP addresses was assigned to Mr. Bosyk's residence by his Internet Service Provider, the government obtained a warrant to search his home.

This is far too slender a reed on which to establish probable cause. The affidavit in support of the warrant alleged only that an IP address associated with

Mr. Bosyk's residence "was used to download or attempt to download file content associated with" a target URL – one of the links connecting to the password protected files. *See Affidavit in Support of a Search Warrant filed under seal in Case No. 1:16-SW-191*. It does not allege how the URL was acquired by the user, nor that the user accessed the URL with knowledge of what file content it linked to, nor that he had any reason to know.

Although the government knew that some of the target URLs generated by the file-sharing service were posted by members of Bulletin Board A, nothing in the affidavit shows that Mr. Bosyk knew anything about the connection between the URLs and the website. The affidavit does not allege that Mr. Bosyk was a member of the website, had ever visited the website, or had any reason to know of the posted links on the website. Nor were there any facts from which to allege that the suspect URLs could only have been accessed via Bulletin Board A or that any investigation had been done into whether the URLs could have been encountered elsewhere on the Internet. In sum, the affidavit "relies upon one click of a mouse" to establish probable cause. *U.S. v. Reece*, No. 2:16-cr-00104-AWA-DEM (E.D. Va. Mar. 1, 2017), Document 44: Order at 10.

The mere association of an IP address with access or an attempt to access a particular URL alone does not amount to probable cause to search an individual's home and/or digital devices because of the limited probative inferences that can be

drawn from a single click. The limited information URLs provide about the underlying resources they connect to are why technologists refer to them as "opaque identifiers."[2] URLs may be accessed in any number of ways, and probable cause will be particularly lacking where the URL itself does not provide any indicia that it links to contraband material.

The evidentiary limitations inherent in URLs have important consequences in this case and demonstrate why probable cause was lacking to search Mr. Bosyk's residence. Indeed, the Second Circuit has held that even where the text of the URL appears to link to contraband on a child pornography website, there is no substantial basis for probable cause in a warrant that alleged only that it "appear[ed]" that the defendant "gained access or attempted to gain access" to the site. *U.S. v. Falso*, 544 F.3d 110, 121 (2d Cir. 2008). And in an earlier case, where the defendant was alleged to have sought membership to a group sharing child pornography, the Second Circuit wrote: "The notion that, by this act of clicking a button, [the defendant] 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." *U.S. v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005).

---

[2] *See URI and URL*, Enterprise and Economic Development Glossary (last visited Aug. 30, 2018) http://www.findmehere.com/search/dictionary/u/url.htm; *URL Living Standard*, Section 3.1: Host representation (last updated Aug. 21, 2018) https://url.spec.whatwg.org/.

EFF urges this Court to follow the Second Circuit and hold that mere access or attempt to access a link that may lead to suspected contraband material falls short of the probable cause required by the Fourth Amendment, particularly when the context of how the URL was encountered by the user is completely unknown and the URL itself provides no information directly linking it to contraband.

ARGUMENT

The Fourth Amendment does not permit the search of an individual's home based solely on an allegation that an IP address connected to the residence accessed or attempted to access a link to a file-sharing website suspected as being used to distribute child pornography.

I. URL Links on the World Wide Web are "opaque identifiers" that do not necessarily reveal the content they locate or the context in which they are shared.

The mere fact that an individual accessed an Internet link associated with contraband will generally be insufficient to establish probable cause for a search warrant because those links may not identify the underlying content they connect to. These links are known as Uniform Resource Locators, or "URLs", and they provide Internet users with the ability to access web addresses on the World Wide Web. A URL 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. Absolute URLs contain (1) a protocol designation, (2) a root domain or host name or address, and (3) a file path or resource location.[3]

For example, a webpage giving the history of EFF can be found at: https://www.eff.org/about/history. Its absolute URL breaks down as follows:

[3] Bradley Mitchell, *URL – Uniform Resource Locator*, Lifewire, https://www.lifewire.com/definition-of-uniform-resource-locator-817778 (last visited Aug. 28, 2018)

(1) Protocol designation—https—which stands for Hypertext Transfer Protocol Secure and is a secure form of the foundational HTTP protocol that allows users to fetch data and resources from the World Wide Web.[4]

(2) Domain or host name—www.eff.org—identifies the particular destination website a user accesses.

(3) Path or resource location—/about/history—directs users to a particular webpage or file, functioning much like the directory file system in most personal computers.

In the case of the above absolute URL, clicking on it sends web users to a page describing EFF's founding and mission.

An Internet user can navigate to a URL by clicking on a link in a webpage, bookmark or email, or by typing or pasting the URL directly into the browser's address bar.[5] Some URLs may support an obvious inference about the content of the webpage or file they locate, as with the EFF history page, but some may not. "Dynamic" URLs, for example, can be generated from specific queries to a site's database, such as in response to a search on Google or Amazon.[6] For example, the district court docket for this case on PACER can be found, after logging in, at

---

[4] *An Overview of HTTP*, Mozilla, https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview.

[5] *Anatomy of a URL*, Doepud (March 6, 2010), https://doepud.co.uk/blog/anatomy-of-a-url.

[6] Vangie Beal, *dynamic URL*, Webopedia, https://www.webopedia.com/TERM/D/dynamic_URL.html.

https://ecf.vaed.uscourts.gov/cgi-bin/DktRpt.pl?996144810667108-L_1_0-1.

The content in the PACER link above does not provide any details about the source of the content it locates. Although the top-level domain seems to indicate the file is part of the U.S. District Court for the District of Eastern Virginia's website, the URL does not contain the case number or the party names, much less anything that would indicate that it is a docket for a case before the court. So although someone encountering the URL may recognize that the content is from the court's website, there is no further information in the URL that would allow anyone to know what resources it locates before they access it. Further, as described below, there are circumstances under which the URLs provide even less information about the underlying website, files or resources they locate.

URLs that obscure or otherwise fail to explicitly identify the content they locate can be generated in a variety of ways and for a variety of purposes. Some examples are discussed below.

A. Random or algorithmically generated URLs

File-sharing services, for example, will often generate URL identifiers randomly. Some users and services rely on randomized URLs as a security measure to restrict access to content to those who have been given the URL because it is harder for unauthorized users to guess long, computer-generated URLs. Randomly generated URLs are how many Internet companies, such as

Google, limit access to a range of files, such as photos, that users want to share with family and friends or simply access from a different computer.[7] As the article describes, Google randomly generates URLs for photos that are 40 characters long. *Id*. The randomness of the URL generated for a photo makes it very difficult for someone to guess. Other services, such as the file-sharing service Dropbox, also allow users to generate random URLs to share files while simultaneously allowing users to actually password-protect the underlying content.[8]

Similarly, the video hosting service YouTube also generates random URLs that provide no information about the underlying content they reference. For example, the URL https://www.youtube.com/watch?v=fkniySdHQdc links to a recording of the Court's Constitution Day Program on September 14, 2017.[9] Yet there is nothing in the character string "fkniySdHQdc" that tells anyone anything about the content of the video. Thus, a randomized URL link does not necessarily alert users as to the content of its destination.[10] Furthermore, nothing stops a

---

[7] Russell Brandom, *Google Photos and the unguessable URL*, The Verge (June 23, 2015), https://www.theverge.com/2015/6/23/8830977/google-photos-security-public-url-privacy-protected.

[8] *How Dropbox keeps your files secure*, Dropbox, https://www.dropbox.com/help/sign-in/how-security-works (last visited Aug. 27, 2018).

[9] United States Court of Appeals for the Fourth Circuit, *Constitution Day Program – September 14, 2017*, Youtube (Sep. 27, 2017).

[10] For example, someone who received these two Youtube URLs wouldn't know from inspection which one was by the Fourth Circuit and which one was not: https://www.youtube.com/watch?v=fkniySdHQdc

randomly generated URL from being shared with unintended users. And in some cases, the algorithm used to generate URLs can be susceptible to cracking.[11]

B. Link shorteners and their use in URL spoofing

Since full URLs that link to a particular webpage, file, or other resource tend to be long, and sharing them can become cumbersome, it has become common to use link shorteners[12] that convert a full (absolute) URL into shorter ones. These services facilitate easier transmission of the underlying resource located at the much larger URLs, whether it be via email or some social media platform. For example, this Court's website contains URLs to its local rules of federal appellate procedure, including this link to Local Rule 29 concerning *amicus curiae* briefs: http://www.ca4.uscourts.gov/LocalRules/LocalRules.3.19.html#pID0E0CT0HA. Because the URL is long, a link shortener such as Bitly can provide a more compact URL that provides access to the same webpage: https://bit.ly/2LbBIie. Of course, because the shorter URL does not include the Court's domain – www.ca4.uscourts.gov – in the link, it is not clear on the face of the shorter URL that it links back to the Court's website or to the particular page detailing Local

---

https://www.youtube.com/watch?v=dQw4w9WgXcQ

[11] Andy Greenberg, *Researchers Crack Microsoft and Google's Shortened URLs to Spy on People*, Wired (Apr. 14, 2016), https://www.wired.com/2016/04/researchers-cracked-microsoft-googles-shortened-urls-spy-people/.

[12] For example, see https://tinyurl.com/ or https://bitly.com/

Rule 29.

By obscuring the underlying absolute URL, link shortening also enables a practice known as URL spoofing. A spoofed URL poses as the hyperlink to a particular website, but then directs the user to a different website.[13] Spoofing often takes advantage of the social context around the transmission of links. A common comedic example of spoofing is the practice of "rickrolling"[14] – a type of bait and switch prank involving the unexpected appearance of the music video for the 1987 Rick Astley song "Never Gonna Give You Up" using a disguised or shortened hyperlink URL that leads to the music video. The victims, believing that they are accessing some unrelated material, are said to have been "*rickrolled*."[15]

URL spoofing can also involve more technologically sophisticated techniques, such as exploiting bugs in web browser technology or opening surreptitious pop-up windows. These techniques can enable relatively benign misdirection, as with rickrolling, or more malicious attacks as with phishing.[16] During a phishing attack, a computer user is directed via email or text to visit a

---

[13] *Spoofed URL*, Wikipedia, https://en.wikipedia.org/wiki/Spoofed_URL (last visited Aug. 28, 2018).
[14] *Rickrolling*, Wikipedia, https://en.wikipedia.org/wiki/Rickrolling (last visited Aug. 28, 2018).
[15] For instance, a reader of this brief could not readily determine which of https://bit.ly/IqT6zt and https://bit.ly/2giFEmn leads to the Fourth Circuit's own website without loading these URLs in a web browser.
[16] *Phishing*, Wikipedia at https://en.wikipedia.org/wiki/Phishing (last visited Aug. 28, 2018).

spoofed website with a familiar URL that may look and feel similar to a legitimate website but is, in reality, sending information to an entirely different location that would typically be monitored by an information thief. *Id.*

C. The opacity of URLs means that web users often cannot tell what content any given URL locates.

For these reasons, URLs are referred to as "opaque identifiers,"[17] meaning that a user cannot necessarily determine what kind of content or resource is located at the other end of a URL. This opacity was built into the World Wide Web as a feature. An article published in 1996 by the inventor of the World Wide Web describes the opacity of URLs as axiomatic and warns against ascribing meaning to the content of URLs themselves beyond the fact that they reference a particular object or file on the web.[18] Although the article addresses concerns about creating computer software that would make assumptions based on the content of URLs, its logic extends to the fact that people, including law enforcement, cannot draw conclusions about the underlying material URLs locate based solely on the content within those URLs. Thus it remains true today that "[t]he only thing you use an identifier [URL] for is to refer to an object," and that "you should not look at the contents of the [URL] string to gain other information." *Id*.

---

[17] *Opaque*, Indie Web Camp at https://indieweb.org/opaque (last visited Aug. 28, 2018).

[18] Tim Berners-Lee, *Universal Resource Identifiers – Axioms of Web Architecture*, W3C (Dec. 19, 1996), https://www.w3.org/DesignIssues/Axioms.html

In isolation, a user's connection to a specific URL typically reveals little about the user's actions, knowledge, or intentions. Users may not have intentionally navigated to, or been aware of the content of, the destination web address; they could have clicked on the link accidentally, encountered it with no context or misleading context, had a site load it automatically via a pop-up with no user interaction, or otherwise been the victim of a spoofed URL or phishing attack.

Particularly when URLs can serve as completely opaque identifiers with randomized text, an Internet user frequently cannot tell what content will be hosted at the destination web address just by reading or examining the URL's content.

D. How users encounter URLs varies.

The probative value of a user's connection to a URL is further limited by the fact that links can be posted anywhere on the Internet by anyone. The context of how one user may have encountered the link may be totally different from another user's encounter. For example, journalists and bloggers will routinely post links to past articles and blogs within newer posts, acting as digital references in much the same way as footnotes that reference supporting material. But if a reader chooses to share one of these digital reference links in the body of an email or a text, the recipient won't know anything about the context in which the sender originally encountered the link or that it was used as a digital reference in another article.

Another common example is file-sharing applications, which routinely allow users to copy and share links to hosted materials, such as family photos or shared work documents. And anyone who has ever received a chain email letter knows that users can disseminate links to material via email.

Link shorteners also enable sharing content via Instagram, Twitter, Snapchat, Facebook, and other social media platforms, which allow them to quickly and easily "go viral."[19] Since URLs are repeatedly posted and re-posted by parties unrelated to the host of the URL's content, there is often no way to reliably determine a URL's original source or divine anything about how a particular user may have initially encountered the link.

II. Because URLs are opaque identifiers, an IP address's access or attempt to access a specific URL is, without more, insufficient to support probable cause to search.

Given that URLs are opaque identifiers of the underlying content that they locate on the World Wide Web and provide little to no insight into the context of how a particular user may encounter them, the mere fact that an IP address is alleged to have accessed or "attempted to download" file content associated with a specific URL is not enough to support probable cause to search an individual's home and electronic devices.

[19] *Go Viral* definition, Urban Dictionary, https://www.urbandictionary.com/define.php?term=go%20viral (last visited Aug. 29, 2018).

While law enforcement may have determined that a particular URL was shared in a forum for illicit content and itself points to illicit content, this in and of itself is not proof that a person who received or accessed the URL had any knowledge of its contents, particularly if the URL on its face provided no indication of the underlying content it locates. Moreover, as described above, because URLs can be shared broadly, the mere accessing of the URL says little about whether the individual had found it in the same channel or location through which law enforcement agents did, especially where there is no evidence of how the URL was conveyed to or encountered by the user.

The hazard of reading too much into URLs is apparent in this case. It is misleading for the government to suggest that a particular URL can only have been shared through one medium or channel (like the website identified as "Bulletin Board A") or that no one would re-share a URL link to a file-sharing site. As noted above, URLs can easily be, and frequently are, copied and re-posted outside of their original context; users also routinely share links to hosted material from DropBox, Google Drive, or Apple's iCloud, which are identified as some of the top file-sharing services.[20]

[20] *Top 12 Most Popular File-Sharing Software*, Finances Online, https://file-sharing-software.financesonline.com/ (last visited Aug. 28, 2018).

A. Only limited evidentiary inferences can be drawn from an individual's connection to a specific URL.

As described in Section I.A., there is often no reliable way to tell what content is located at the destination web address of a particular URL link. Thus, just because an IP address is alleged to have accessed or attempted to access a URL that directs to a file-sharing website suspected to distribute child pornography, that fact alone does not necessarily mean that the user intentionally clicked on it to gain access to the content of the URL's destination.

The Second Circuit addressed this same issue in *U.S. v. Falso*, 544 F.3d 110, 121 (2d Cir. 2008). There, the defendant was not alleged to have actually accessed or subscribed to any child pornography website. Rather, the affidavit alleged only "that Falso was perhaps one of several hundred possible subscribers to the cpfreedom.com website, who *appeared* either to have gained *or* attempted to gain access to the site." *Falso*, 544 F.3d at 120.

The Second Circuit reasoned that:

> In Falso's case, there is no allegation that he subscribed to CP Freedom's paying-membership site; only that it "appear[ed]" that he "gained access or attempted to gain access" to the non-member cpfreedom.com website. Even if one assumes (or infers) that Falso accessed the cpfreedom.com site, there is no specific allegation that Falso accessed, viewed or downloaded child pornography. While the non-member site contained approximately eleven images of child pornography, the affidavit lacks any information about whether the images were prominently displayed or required an additional click of the mouse; whether the images were downloadable; or what other types of services and images were available on the site.

Id. at 121.

The affidavit in this case provides even less incriminating evidence than what the Second Circuit found to be a lack of probable cause in *Falso*. Here, the affidavit fails to allege that Bosyk accessed, viewed, or downloaded child pornography. There are no allegations that Bosyk ever connected to Bulletin Board A, that he had access to the password required to open the file containing the suspected child pornography images located by the target URL, or where or how he encountered the URL that led to the file-sharing service suspected of hosting the child pornography. Further, there was no evidence in the affidavit from which to infer that Bosyk was even aware of the destination content of the suspect URL, much less that the URL itself provided indicia of criminality, unlike the link at issue in *Falso* that included the domain name cpfreedom.com in the URL.

In a case involving the same investigation, a more developed record, and an identical search warrant save for its different target suspect, another district court came to the correct conclusion that there was insufficient probable cause to support the search warrant and that the good faith exception did not apply. *See U.S.* v. *Reece*, 2:14-cr- 104, Doc. No. 44 (E.D. Va. March 1, 2017). In *Reece,* the district court determined that the affidavit lacked factual assertions that the defendant subscribed to or accessed a child pornography website (Bulletin Board A). *Id.* at 10. The affidavit supported only an inference that the defendant clicked on a link to

an illicit video that *could be accessed* through a child pornography website, but that such an inference was insufficient to support the resulting search without the court making the "inferential leap" that the defendant *must have accessed* the child pornography website to navigate to the illicit material. *Id.* (emphasis in original).

Relying on *Coreas,* 419 F.3d at 156, the *Reece* court held that an affidavit that similarly relies upon one click of a mouse absent any evidence that the defendant ever actually accessed any website containing child pornography fails to establish probable cause because "it is possible that the link could have been accessed through innocent means." *Id.* at 11. Additionally, the *Reece* court also concluded that there was no evidence to support the inclusion of "collector language" in the affidavit. *Id.* at 11–14.

Likewise here, this Court should find that a single incident of access or attempt to access a specific URL—absent any indicia how the suspect encountered the URL, had ever accessed the child pornography website known as Bulletin Board A, was a collector of child pornography, or had any reason to know the substance of the content of the URL's destination—falls woefully short of the probable cause requirement of the Fourth Amendment.

B. The Good Faith Exception does not apply.

The Good Faith Exception does not apply here because the warrant was so lacking in any indicia of probable cause that no reasonable officer could have

relied upon it. As explained above, the government's proffered justification that a mere attempt to access a particular URL without any further explanation or evidence about how the user encountered the URL is patently unreasonable and falls short of the necessary probable cause to search a user's home or digital devices.

As the Supreme Court recognized in *U.S. v. Leon*, there can be no objective good faith in relying on a warrant based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. 897, 923 (1984); *U.S. v. Doyle*, 650 F.3d 460, 466 (4th Cir. 2011). Suppression remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth. *Leon*, 468 U.S. at 923 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)).

Because the inferences that can be drawn from a specific IP address's connection to a particular URL are so limited, no reasonable officer could believe that the sparse information contained in the affidavit could support probable cause to search Mr. Bosyk's home. As discussed in Section I.B.i. above, dealing with the same template warrant application, the *Reece* court found that "the process undertaken in this warrant application reflects a reckless disregard for accuracy that was material to the probable cause determination" and held the good faith

exception inapplicable "because the flaws existing in the warrant and supporting affidavit go beyond nonrecurring or attenuated negligence and are not the result of an officer's reasonable reliance on faulty information." *Reece* at 23.

Accordingly, the Court should likewise find that mere connection to a suspect URL is such minimal evidence that it cannot justify good faith reliance here.

CONCLUSION

This Court should side with the Second Circuit and hold that merely accessing or attempting to access a URL link that may lead to suspected illicit material falls short of establishing probable cause as required by the Fourth Amendment.

Dated: August 30, 2018

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Counsel of Record
Stephanie Lacambra
Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
sophia@eff.org

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amicus Curiae* in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,552 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: August 30, 2018

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on August 30, 2018.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: August 30, 2018

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amicus Curiae