Appeal No. 18-5578

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff/Appellee,

v.

WILLIAM J. MILLER,

Defendant/Appellant.

On Appeal from the United States District Court
for the Eastern District of Kentucky
Case No. 2:16-cr-00047-1
The Hon. David L. Bunning

BRIEF OF DISCORD, INC., DROPBOX, INC., FACEBOOK, INC., GOOGLE LLC, MICROSOFT CORP., PINTEREST, INC., REDDIT, INC., SNAP INC., AND TWITTER, INC. AS AMICI CURIAE SUPPORTING APPELLEE AND AFFIRMANCE

Ryan T. Mrazik
Erin K. Earl
Rachel A.S. Haney
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Telephone: (206) 359-8000

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Discord, Inc.
Name of Party

makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Dropbox, Inc.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

Dropbox, Inc. does not have a financial interest in the outcome.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Facebook, Inc.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Google LLC
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

Google LLC ("Google") is a wholly owned subsidiary of XXVI Holdings Inc., which is a wholly owned subsidiary of Alphabet Inc., a publicly traded company.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

XXVI Holdings Inc. owns 100% of Google and is a wholly owned subsidiary of Alphabet Inc., a publicly traded company.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Microsoft Corp.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Pinterest, Inc.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Reddit, Inc.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Snap Inc.
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 18-5578 Case Name: United States v. Miller

Name of counsel: Ryan T. Mrazik

Pursuant to 6th Cir. R. 26.1, Twitter, Inc.
Name of Party

makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on December 26, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Ryan T. Mrazik

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

Amici offer some of the most widely used Internet- and mobile-based communications, sharing, and storage products and services in the world.

Discord is a communications platform that allows hundreds of millions of people across the world to engage in video, voice, and text-based chat. People use Discord to talk to each other about video games as well as other shared interests. Through Discord, community members can chat, play games together, purchase them, and create lasting relationships.

Dropbox is a global collaboration platform where content is created, accessed, and shared. Dropbox aims to unleash the world's creative energy through its collaboration, synchronization, and cloud storage services.

Facebook's mission is to give people the power to build community and bring the world closer together. Through its services, Facebook enables people to stay connected with friends, family, and colleagues; to discover what's going on in the world; and to share and express what matters to them.

Google is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google

[1] All parties have consented to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no person other than amici or their counsel has made a monetary contribution intended to fund the preparation or submission of the brief.

offers a variety of web-based products and services—including Search, Gmail, Maps, YouTube, and Blogger—used by people everywhere.

Microsoft Corporation is a worldwide leader in software, services, devices, and solutions, including intelligent cloud-based computing. Since its founding in 1975, Microsoft has developed a wide range of software, services, and hardware products, including the flagship Windows operating system, the Office suite of productivity applications, the Surface tablet computer, and the Xbox gaming system. Microsoft serves more than 90 markets worldwide, delivering more than 200 online services and supporting more than one billion customers from more than 100 datacenters across the globe. In 2009, Microsoft partnered with Dartmouth College to develop PhotoDNA, a hash-matching technology that aids in finding and removing known images of child exploitation. Today, PhotoDNA is used by organizations around the world, including by Microsoft, to detect and remove child exploitation images. Microsoft developed, implemented, and distributed PhotoDNA because of its judgment that blocking illegal images of child exploitation is in Microsoft's business interests.

Pinterest is an online visual discovery tool that helps people discover and save creative ideas, and share the things and places they love with others.

Reddit is a network of communities where individuals can find experiences built around their interests, hobbies, and passions. Redditors submit, vote, and

comment on content, stories, and discussions about the topics they care about the most. With over 330 million global users monthly, Reddit is home to the most open and authentic conversations on the Internet.

Snap Inc. operates the mobile application Snapchat, one of the world's leading camera and messaging applications. Snapchat lets users talk with their closest friends via photos and videos that they create on the application. The app also empowers users to learn about what's happening in the world and view original shows and other video content from leading publishers.

Twitter, Inc. is a technology company based in San Francisco, California. Its primary service, Twitter, is a global platform for public self-expression and conversation in real time. Twitter allows people to consume, create, distribute, and discover content and has democratized content creation and distribution. Twitter has more than 300 million monthly active users, spanning nearly every country, and creating approximately 500 million Tweets every day.

Every day, billions of people use amici's services to talk with family and friends, express thoughts and opinions, operate businesses, take and send videos and photos, and discover new content and information from around the world.

Unfortunately, a tiny fraction of users abuse amici's services, in violation of amici's Terms of Service, to offer, store, and transmit child pornography.[2]

For decades, "the exploitive use of children in the production of pornography has [been] a serious national problem." *New York v. Ferber*, 458 U.S. 747, 749 (1982). As use of online communications has increased, the proliferation of child pornography likewise has "grown exponentially." *Paroline v. United States*, 572 U.S. 434, 440 (2014) (internal citation omitted). Amici devote substantial human and technological resources to keeping this material off their services.

One such technological resource is hash matching, an automated computer process that detects duplicates of images previously identified as apparent child pornography. Hash matching enables service providers such as amici to protect their services and users, independent of any reporting requirement, by reliably and efficiently detecting duplicates of files that were previously identified as apparent child pornography and removing those files from their services. Amici report this

[2] Amici and courts sometimes refer to this material using other terms, including "child exploitation material" or "child sexual abuse images." *See, e.g.*, *Paroline v. United States*, 572 U.S. 434, 483 (2014) (Sotomayor, J., dissenting); *United States v. Christman*, 607 F.3d 1110, 1113 (6th Cir. 2010). In this brief, amici use the term "child pornography" for clarity and consistency with the parties' briefs. As noted below, providers have a statutory obligation to report any apparent violation of the federal child pornography statutes, so reportable "child pornography" discussed in this brief includes material that appears to satisfy the definitions in Chapter 110 of Title 18, United States Code.

material to the National Center for Missing and Exploited Children ("NCMEC") to fulfill their duty to report any "apparent violation of" the federal child pornography statutes. 18 U.S.C. § 2258A. If the Fourth Amendment were interpreted to prevent NCMEC or law enforcement from reviewing files that providers identified through hash matching as duplicates of previously-reviewed apparent child pornography, there would be fewer investigations of providers' reports and providers would have to cope with increased recidivism on their platforms.

Because of their interests in safeguarding the integrity of their services, protecting their users, and keeping child pornography off their products and services, amici have a strong interest in the outcome of this case.

SUMMARY OF ARGUMENT

The district court correctly held that the use of hash matching to identify two child pornography images attached to an email in Miller's account did not violate the Fourth Amendment.

The Fourth Amendment applies to searches by the government, not by private actors. Although online service providers like amici share the broad societal interest in combating child pornography, that does not transform them into government agents. In identifying and removing child pornography that appears on their services and platforms, and developing and using technology to increase the

efficiency, accuracy, and effectiveness of that process, providers are private companies acting to fulfill their own business purposes.

One way that providers like amici pursue their private interests in working to stop the spread of child pornography online is through hash matching. Hash matching involves calculating an alphanumeric value (a "hash value") from a specific file—in this context, an image that has previously been viewed by a human and determined to be apparent child pornography—and then identifying duplicates of that file by comparing its hash value with the hash values of unknown files. This process enables service providers like amici to accurately and efficiently identify and remove from their services identical copies of previously-reviewed child pornography images.

And when a provider reports copies of such images identified using hash matching, subsequent viewing of those images by the government does not exceed the scope of the provider's initial private search: the high accuracy of hash matching means that the government's examination of the image will not reveal any information not already revealed by the provider's hash match.

ARGUMENT

The Fourth Amendment generally protects users' reasonable expectations of privacy in the contents of emails held by a third-party service provider from warrantless search and seizure by the government, irrespective of whether the

service provider has terminated that user's account or whether the user violated the terms governing his relationship with the service provider. *See* Miller Br. 9-10; *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010). But the Fourth Amendment applies only to searches by the government and the district court correctly found that Google did not act as a government agent.

Further, Detective Schihl did not expand the scope of Google's initial private review. This Court should join the Fifth Circuit in affirming that law enforcement does not violate the Fourth Amendment by reviewing images identified by private companies as having hash values corresponding to previously-reviewed apparent child pornography. *See United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018), *petition for cert. filed*, No. 18-6734 (Nov. 14, 2018).

A. Service providers do not act as government agents by advancing their private interests in ensuring that child pornography does not proliferate on their services.

The Fourth Amendment's prohibition against unreasonable searches and seizures applies only to governmental action, not to conduct undertaken by private parties. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Because Google is a private entity, its conduct implicates the Fourth Amendment only if Google acted as a government agent. *See United States v. Robinson*, 390 F.3d 853, 871 (6th Cir. 2004). The record here shows that Google did not act as a government

agent, and service providers like amici that undertake similar hash matching to protect their own private business interests remain private actors when doing so.

1. Law enforcement did not instigate, encourage, or participate in Google's identification of offending images, which Google undertook to fulfill its independent private interests.

This Court uses a two-part test to determine whether a private person has conducted a search[3] as an agent of the government: (1) law enforcement "must have instigated, encouraged or participated in the search" and (2) "the individual must have engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985)) (internal quotation marks omitted). The district court correctly held that Google does not qualify as a government agent under this standard.

First, nothing in the record suggests that either NCMEC or law enforcement instigated, encouraged, or participated in Google's identification of the two reported images.[4] To the contrary, Google was not aware of any investigation of Miller by law enforcement and did not review the reported images at law enforcement's request. Declaration of Cathy McGoff, RE 33-1 ("McGoff Decl."),

[3] Amici assume for purposes of this case that hash matching can constitute a "search" under the Fourth Amendment.

[4] Amici take no position on whether NCMEC qualifies as a government entity or agent but, like the district court, assume only for purposes of this analysis that it does. *See* Dist. Ct. Op. Page ID #264.

Page ID #162 ¶¶ 12-13. Google's only interaction with law enforcement occurred *after* the images were reported, when Google responded to "inquiries as to whether images had been viewed by human eyes prior to or concurrently to the submission of CyberTips." *Id.* ¶ 13.

Second, nothing in the record comes close to suggesting that Google identified the reported images with any intent to assist a police investigation. Rather, the district court correctly found that Google acted "for its own business purposes," which are "entirely independent of the government's intent to collect evidence for use in a criminal prosecution." Dist. Ct. Op. Page ID #266-67 (quoting *United States v. Bowers*, 594 F.3d 522, 526 (6th Cir. 2010)) (internal quotation marks omitted).

Google and other service providers, including amici, have strong business interests in enforcing their Terms of Service and ensuring that child pornography is not stored in their products. *See* McGoff Decl. Page ID #161 ¶ 3; Dist. Ct. Op. Page ID #266-67; *see also, e.g.*, *United States v. Rosenow*, No. 17-CR-3430-WQH, 2018 WL 6064949, at *8 (S.D. Cal. Nov. 20, 2018) ("Yahoo has a business interest in enforcing its terms of service and ensuring that its products are free of illegal conduct, in particular, child sexual abuse material."); *Vermont v. Lizotte*, ___ A.3d ___, No. 17-127, 2018 WL 3947971, 2018 VT 92, ¶ 23 (Vt. Aug. 17, 2018) ("AOL monitored defendant's transmissions based on its business interest, not because it

was encouraged or directed to by government . . . ."); *Hearing on Examining the Content Filtering Practices of Social Media Before the H. Comm. on the Judiciary*, 115th Cong., 2018 WL 3440302 (2018) (statement of Juniper Downs, Global Policy Lead, YouTube, LLC) ("Keeping YouTube free from dangerous, illegal or illicit content not only protects our users, it's a business imperative.").

In amici's experience, users stop using services if they are associated with being havens for this content. *See* McGoff Decl. Page ID #161 ¶ 3. Accordingly, as the district court reasoned, "[e]ven without a statutory obligation to report its findings to NCMEC, it seems likely that Google would screen its platform for images of child pornography because doing so is good business practice." Dist. Ct. Op. Page ID #267. That is what amici do: they work to ensure their services are free from child pornography because it protects their users and services.

Service providers like amici also share the "general societal consensus that images of child pornography are harmful." *Id.* Amici do not want their products and services to be used to perpetuate that harm. *See, e.g.*, Technology Coalition, *Our Mission*, http://www.technologycoalition.org/our-mission/ (explaining its "vision is to eradicate online child sexual exploitation" by "sponsor[ing] the development of technology solutions that disrupt the ability to use the Internet to exploit children or distribute child pornography"); Thorn, *About Us*, http://www.wearethorn.org/about-our-fight-against-sexual-exploitation-of-

children/ (explaining that Thorn partners "with the sharpest minds from tech, non-profit, government and law enforcement" in its effort "to stop the spread of child sexual abuse material and stand up to child traffickers").

For private business reasons and to pursue their goals as corporate citizens, service providers like amici may at times collaborate with NCMEC or other organizations on initiatives for combating the spread of child pornography online. *See, e.g.*, Hayley Tsukayama, *How Google and Other Tech Firms Fight Child Exploitation*, Wash. Post. (May 6, 2015) (cited in Miller Br. 20 n.3), http://www.washingtonpost.com/news/the-switch/wp/2015/05/06/how-google-and-other-tech-firms-fight-child-exploitation/. But any such collaboration on broadly shared goals at the policy level does not suggest any intent to assist the police in any particular investigation or any particular search. *See Hardin*, 539 F.3d at 419.

2. Miller's "nexus" text is inapplicable, but Google would not qualify as a "state actor" under it in any event.

Miller argues for a separate, "nexus" test, under which "a private entity can be held to constitutional standards when its actions so approximate state action that they may be fairly attributed to the state." *Lansing v. City of Memphis*, 202 F.3d 821, 828 (6th Cir. 2000); Miller Br. 17-21. The cases on which he relies involve 42 U.S.C. § 1983, but the state-action test applicable in that context differs from the test governing a motion to suppress evidence obtained through a search performed by a private person. *See, e.g.*, *United States v. Barry*, 673 F.2d 912, 915 (6th Cir.

1982) (where challenged search of a package occurred under FedEx policy regarding package damage, rejecting argument that a memorandum prepared by FedEx and the Drug Enforcement Agency asking employees to cooperate in detecting illegal drug shipments showed "nexus" between company and law enforcement). Miller's proposed "nexus" standard is therefore inapplicable here.

Even if the "nexus" test applied, however, the relationship between NCMEC and providers, including Google and the other amici, would not qualify. The existence of a sufficiently "close nexus" turns "on whether the State 'has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State.'" *Am. Mfrs. Mut. Ins. Co. v. Sullivan*, 526 U.S. 40, 52 (1999). Yet Congress has expressly declined to require any provider to take efforts to identify apparent child pornography on its platform. *See* 18 U.S.C. § 2258A(f). Instead, each provider (amici included) makes its own decision as to whether and how to look for apparent child pornography—and there is substantial variation in practices between amici. Further, it is well established that providers' statutory obligations to report and preserve apparent child pornography when they learn of it does not transform them into state actors. *See, e.g.*, *United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010).

Miller contends that cooperating with NCMEC or the government on technological solutions to fighting sexual exploitation of children is in itself sufficient to transform providers into state actors. Miller Br. 20-21. Not so.

Sharing the general societal consensus that images of child pornography are harmful, and voluntarily taking action to reduce their spread, do not suggest that service providers are acting in response to any coercive power or encouragement from the State. *See, e.g.*, Dist. Ct. Op. Page ID #267; *Stevenson*, 727 F.3d at 831 (a provider's "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent"); *see also Barry*, 673 F.2d at 915. If adopted, Miller's position would mean that companies that collaborate with law enforcement to develop security cameras to protect businesses against theft, for example, would similarly find themselves transformed into state actors subject to constitutional restrictions. This reasoning also would suggest that anyone who reports criminal activity to the government does so as a government actor. That is not the law.

In sum, complying with a statutory reporting obligation and acting collaboratively toward a shared goal of reducing the spread of online child pornography do not transform service providers' voluntary private action into action coerced or encouraged by the Government.

B. Hash matching is a reliable, accurate, and efficient technological process for service providers to identify duplicates of child pornography files.

One way that service providers advance their private interests in reducing the spread of child pornography online is to use hash-matching technology to identify copies of files they have already viewed and reported to NCMEC.

Automated technological solutions help counter the spread of child pornography online as the volume grows dramatically. In 2017 alone, for example, NCMEC received more than 10.2 million reports of suspected child sexual exploitation (including apparent child pornography) through the CyberTipline, and reports have "been growing exponentially each year." Nat'l Ctr. for Missing & Exploited Children, *The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports*, http://www.missingkids.com/content/dam/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf.

Some providers therefore use hash matching to identify duplicates of images that a person previously identified as apparent child pornography. In this context, hash matching means calculating an alphanumeric value (a "hash value") from a specific image that a person identifies as apparent child pornography, then identifying duplicates of that image by comparing its hash value with the hash values of unknown images. Dist. Ct. Op. Page ID #260. Calculating a hash value involves applying a mathematical algorithm to a piece of information. Although

there are various methods and algorithms for doing so,[5] the process, known generally as "hashing," has been used widely in the technology industry for many years, including to store information in data structures that allow for more efficient searches and to ensure that two files or sets of data are exact matches. *See, e.g.*, *Microsoft Computer Dictionary* 214 (4th ed. 1999); Niels Ferguson, Bruce Schneier & Tadayoshi Kohno, *Cryptography Engineering: Design Principles & Practical Applications* 77 (2010).

A hash value is unique to a specific file and often referred to as a "digital fingerprint," Dist. Ct. Op. Page ID #260, or a "digital signature." Ronald Rivest, *The MD5 Message-Digest Algorithm* (1992), http://tools.ietf.org/html/rfc1321; *see also* Ryan D. Balise & Gretchen Lundgren, *The Fourth Amendment's Governmental Action Requirement: The Weapon of Choice in the War Against Child Exploitation*, 41 New Eng. J. on Crim. & Civ. Confinement 303, 308-09 (2015). Importantly, a hash value is not a mere label or title for a file that might not accurately describe the file's content. Rather, a hash value is specific to that file and inextricably linked to the file, bit-for-bit. *See* Richard P. Salgado, *Fourth*

[5] For example, some hashing algorithms, such as PhotoDNA, use image-specific functions to identify, with a high degree of accuracy, duplicate and near-duplicate images—i.e., images that have been altered, potentially with the goal of escaping detection by file-based hashing algorithms. *See Reddick*, 900 F.3d at 637-38. Amici therefore disagree with EPIC's assertion that so-called "image hashing" is "fundamentally different" from file hashing—*both* "are good at achieving a near-zero percentage of false positive matches." EPIC Br. 10-11.

Amendment Search and The Power of the Hash, 119 Harv. L. Rev. F. 38, 39 (2005).

Because a hash value can be calculated only for a specific file and not for features in a general category of images (such as images showing sexual activity), providers seeking to identify and remove child pornography from their services can match files only against calculated hash values for images that have already been identified by a person as apparent child pornography. Here, for example, "[a]fter an image of child sexual abuse is viewed by at least one Google employee, the image is given a digital fingerprint (hash) and is added to [Google's] repository of hashes of apparent child pornography." Dist. Ct. Op. Page ID #260 (quoting McGoff Decl. Page ID #161 ¶ 4) (internal quotation marks omitted) (second alteration in original).

Then, because the calculated hash value is specific to each image whose hash value was included in the data set, a provider can use the hash value to identify duplicates of that image. *See* Salgado, 119 Harv. L. Rev. F. at 40 ("[I]f [the] unknown file has a hash value identical to that of [the] known file, then you know that the first file is the same as the second."). For example, the district court found that Google's product abuse detection system recognized two images attached to an email as apparent child pornography by calculating the hash value

for each image and comparing them to its repository of hash values for apparent child pornography files. Dist. Ct. Op. Page ID #259-60.

Hash matching identifies duplicates of apparent child pornography files more reliably and efficiently than humans, who cannot search for or review content at the rate of an automated computer program and cannot detect duplicates of files as accurately as can a computer program. *See* Salgado, 119 Harv. L. Rev. F. at 41. Using hash matching also relieves providers' review teams of the need to review the same imagery countless times.

And hash matching provides these benefits without incurring any decrease in accuracy. In its amicus brief supporting Miller, the Electronic Privacy Information Center claims that hash matching has three sources of potential inaccuracy: (1) human error in the original identification; (2) error in hash matches received from another entity; and (3) false positives. None is persuasive.

First, any potential for human error has nothing to do with hash matching but would be presented equally by *any* form of provider reporting—humans are as likely to make mistakes in identifying an image they review personally as they are in identifying an image that is added to a hash database used to automatically identify duplicate images. As such, any potential for human error is immaterial to the legal issue here, as it has no impact on the scope of the private or governmental search. Further, any risk is low because Google personnel are "trained by counsel

on the federal statutory definition of child pornography and how to recognize it on [Google's] products and services." McGoff Decl., Page ID #161 ¶ 6.

Second, any potential for erroneous matches to hash values received from another entity is nonexistent here, where the record shows Google relied on its own repository of hashes generated from images its own team had previously reviewed. *See* McGoff Decl. Page ID #161-62¶¶ 7, 9.

Finally, the risk of false positives is negligible for any industry-standard hashing algorithm. Accuracy in hash matching relies on the uniqueness of the hash value, which depends upon the specific hashing algorithm used. *See* Ferguson, Schneier & Kohno, *supra*, at 78-79; Larry J. Hughes, Jr., *Actually Useful Internet Security Techniques* 54-55 (1995).[6] For any industry-standard algorithms, there is at most a vanishingly small risk of a false positive being reported. *See, e.g.*, Salgado, 119 Harv. L. Rev. F. at 39 n.6; *Technical Supplement - Forensic Use of Hash Values and Associated Hash Algorithms*, Neth. Forensic Inst. Ministry of Just. & Sec., at 4 (Jan. 2018) (each of three hashing functions had "almost zero" risk of false positives), http://www.forensicinstitute.nl/binaries/forensicinstitute/

[6] EPIC complains that "neither Google nor the federal agency has revealed the specific nature of the underlying algorithm" or "established the accuracy, reliability, and validity of this technique." EPIC Br. 2. But providers should not be compelled to provide detailed information about the operation of any proprietary technology they may use to identify and remove duplicates of apparent child pornography from their platforms, at the risk of enabling evasive maneuvers by those who spread such material and its further proliferation, nor should providers be restricted to using hashing algorithms that have been publicly disclosed.

documents/publications/2018/02/13/forensic-use-of-hash-values-and-associated-hash-algorithms/Supplement-hashes-v2018_01a_English.pdf.

In sum, with billions of users sending tens of billions of communications through amici's services, hash matching is a reliable and accurate automated process for identifying duplicates of previously-reviewed apparent child pornography images and is the best and most realistic means for providers to be able to protect their services and users from child pornography.

C. Government review of an image of child pornography that has been identified through hash matching does not violate the Fourth Amendment.

1. When a private entity conducts a search and informs the government of what it finds, the government may repeat the search without violating the Fourth Amendment.

When a private entity conducts a search, it may inform the government of what it has found, and "the Fourth Amendment does not prohibit governmental use of that information." *Jacobsen*, 466 U.S. at 117. In other words, the actions of the private entity in making "an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable." *Id.* at 114-15. When a government agent reviews or conducts another search based on information provided by the private entity, any "additional invasions of . . . privacy by the government agent must be tested by the degree to which they exceed[] the scope of the private search." *Id.* at 115; *see United States*

v. Lichtenberger, 786 F.3d 478, 482 (6th Cir. 2015). When a government agent merely repeats the initial private search, no "additional invasion" of privacy occurs, and the government agent does not violate the Fourth Amendment.

2. The district court correctly held that the detective's review of two images of child pornography was within the scope of Google's initial private review.

The Supreme Court's decision in *Jacobsen* establishes the standard for determining when a government agent's subsequent search is within the scope of an initial private search. In *Jacobsen*, FedEx employees opened a package and a tube inside the package to discover plastic bags, the innermost of which contained white powder that the employees identified as cocaine. *See* 466 U.S. at 111. They turned the package over to the DEA. *Id.* The Court held that the DEA agent's subsequent warrantless search of the package did not violate the Fourth Amendment because the agent did not exceed the scope of FedEx's private search. *Id.* at 125-26. Instead, the agent merely confirmed what the FedEx employees had told him, and there was a "virtual certainty" that he would find contraband and little else within the package. *Id.* at 118-120. The Court reasoned that the agent had not violated the Fourth Amendment by "viewing . . . what a private party had freely made available for his inspection." *Id.* at 119.

As the district court explained, this case is similar to *Jacobsen*. Dist. Ct. Op. Page ID #272. Applying *Jacobsen*, the district court correctly determined that the

Fourth Amendment did not prohibit the detective from reviewing the two images that Google reported to NCMEC after it had identified them, using hash matching, as duplicates of child pornography images Google had previously viewed. Dist. Ct. Op. Page ID #267-75. Hash matching does not "reveal anything about an image that Google does not already know from the regular eyes of its employees." *Id.* Page ID #275. Instead, it is "a sophisticated way of confirming that Google already conducted a private search." *Id.* Because "the evidence reveals that Detective Schihl and Google saw the same images—no more and no less," Detective Schihl did not expand the scope of Google's private review and, under *Jacobsen*, the Fourth Amendment was not implicated. *Id.* Page ID #275.

Miller contends that this case is controlled by *Walter v. United States*, 447 U.S. 649 (1980), but his reliance on that case is misplaced. Miller Br. 12-14. In *Walter*, a private carrier misdelivered a set of packages, which the recipients opened and saw contained film boxes. 447 U.S. at 651-52. The recipients did not view the films, but after seeing "suggestive drawings" and "explicit descriptions of the contents" on the outside of the boxes, they contacted the FBI. *Id.* at 652. The FBI then viewed the films without obtaining a warrant. *Id.* The Supreme Court held that the FBI had violated the Fourth Amendment by exceeding the scope of the initial private search. The controlling opinion emphasized that "the private party had not actually viewed the films" and "[p]rior to the Government screening

one could only draw inferences about what was on the films." *Id.* at 657 (opinion of Stevens, J.). Therefore, "[t]he projection of the films was a significant expansion of the search that had been conducted previously by a private party." *Id.*

Reading *Walter* and *Jacobsen* together, two "critical measures" determine "whether a governmental search exceeds the scope of the private search that preceded it"—"how certain [the government] is regarding what it will find . . . when it re-examines the evidence" and "how much information the government stands to gain." *Lichtenberger*, 786 F.3d at 485-86. In this case, those factors make clear that the district court was correct to conclude that Detective Schihl did not exceed the scope of Google's review.

First, when Detective Schihl viewed the image files reported by Google, there was a virtual certainty that the files would contain nothing other than apparent child pornography. *See Jacobsen*, 466 U.S. at 119-120. Google's hash matching process only identifies duplicates of previously-viewed apparent child pornography files, so the chance that the images Google reported to NCMEC would be anything else was essentially zero.

That extremely high level of certainty distinguishes this case—and providers' use of hash matching in general—from *Walter*. The private employee in *Walter* viewed only the outside of the film boxes, not the films themselves, and the

labels and imagery on the film boxes allowed a person only to "draw inferences about what was on the films." 447 U.S. at 657 (opinion of Stevens, J.).

Here, by contrast, after hash matching the files' *contents*, Google knew what the files were: both were duplicates of images that a person had previously reviewed and identified as apparent child pornography. A hash match identifying a duplicate is not a mere label on a canister, which can be subjective or inaccurate. Instead, a hash value is a unique, objective, reliable, and accurate identifier for an image file that identifies duplicates, without any need for human inference or interpretation, and without the possibility of human error or misdescription. The district court correctly understood that distinction:

> A hash value, unlike a label, has no inherent meaning–it gains meaning only when it matches with a hash value in the child pornography repository and therefore reminds Google that it has seen this image before. Indeed, a closer analog to the *Walter* case would be if Google had flagged the images in Defendant's email as apparent child pornography *merely because of their file names*, without having ever looked at the images to verify their content. If that were the situation, Detective Schihl's subsequent examination of the files would present a different, and much more difficult, question of scope.

Dist. Ct. Op. Page ID #270.

Second, because Detective Schihl could be virtually certain that the reported images were apparent child pornography, he stood to gain little or no additional information through his review. As a human, Detective Schihl had to view the files

to confirm their content. But he already knew what he would find: images that Google identified as duplicates of apparent child pornography it had previously viewed. In *Jacobsen*, the DEA agent's search of the box and tube inside was not an additional search under the Fourth Amendment because "a manual inspection of the tube and its contents would not tell him anything more than he already had been told" by FedEx. 466 U.S. at 119. Just so here.

As the district court found, "Google's practice is to register hash values for images that Google has already physically viewed," such that "Google itself had already viewed the images and identified them as apparent child pornography to Detective Schihl before he ever conducted his search." District Ct. Op. Page ID #269, 271. That Google's identification occurred through hash matching does not mean that the detective expanded the scope of Google's private review. In *United States v. Bowers*, for example, this Court held that the FBI's review of a photo album containing child pornography did not exceed the scope of the defendant's roommate's private review of that same album. 594 F.3d 522, 524 (6th Cir. 2010). The only distinction between *Bowers* and this case is, as the district court explained, "that the images here are made of pixels, not photo paper, and that Google identified the images as ones it had previously viewed by using hash values instead of human memory." District Ct. Op. Page ID #273.

Miller's attempt to analogize this case to *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), is similarly unavailing. In *Ackerman*, AOL used hash matching to "identif[y] one of four images attached to Mr. Ackerman's email as child pornography." *Id.* at 1294. After AOL reported the email and all attachments to NCMEC (without further review), an analyst "opened the email, viewed each of the attached images, and confirmed that all four (not just the one AOL's automated filter identified) appeared to be child pornography." *Id.* The court held that NCMEC, which it concluded was a government entity, exceeded the scope of AOL's private review not by opening the original attachment identified by hash matching, but by opening the *email* and the *other three* attachments—"the content of which AOL and NCMEC knew nothing about before NCMEC opened them." *Id.* at 1306. Here, in contrast, Detective Schihl opened *only* the two attached images that Google's hash-matching technology had already identified as apparent child pornography. *See* Dist. Ct. Op. Page ID #262. The holding in *Ackerman* does not apply. *See id.* Page ID #271-72.

In sum, *Jacobsen*'s "virtual certainty" standard is met here. "Virtual certainty" need not be absolute certainty—in *Jacobsen*, the field test could have revealed that the white powder was baking powder and not cocaine. But where, as here, the chances of the images being anything other than apparent child pornography were vanishingly small, and because Detective Schihl did not open

the email itself or any other images, the government did not exceed the scope of Google's private review.

3. The district court's conclusion is consistent with decisions of other courts of appeals.

The district court's conclusion that *Jacobsen* and not *Walter* controls here accords with the weight of authority to address law enforcement's review of images identified through private hash matching.[7] In *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), for example, the Fifth Circuit considered whether a detective expanded the scope of Microsoft's private search when Microsoft identified and reported images that PhotoDNA matched as duplicates of previously-identified child pornography. *Id.* at 637-38. Applying *Jacobsen*, the court concluded that "opening the file merely confirmed that the flagged file was indeed child pornography, as suspected," and thus "there was no 'significant expansion of the search that had been conducted previously by a private party'

[7] The only case to reach a contrary conclusion, *United States v. Keith*, 980 F. Supp. 2d 33, 43 (D. Mass. 2013), is inapplicable. Miller Br. 12-14. As the district court noted, the hash value in *Keith* confirmed "the suspect file is identical to a file that someone, sometime, identified as containing child pornography, *but the provenance of that designation is unknown*." Dist. Ct. Op. Page ID #270 (quoting *Keith*, 980 F. Supp. 2d at 43) (internal quotation marks omitted). Accordingly, who performed the initial review was unclear. *Id.* Because here "the evidence indicates that Google itself had already viewed the images and identified them as apparent child pornography to Detective Schihl before he ever conducted his search," *id.* at Page ID #271, *Keith* does not support Miller's argument.

sufficient to constitute 'a separate search.'" *Id.* at 639 (quoting *Walter*, 447 U.S. at 657). So too here.

Similarly, in *United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013), the Ninth Circuit held that a government agent did not violate the Fourth Amendment by enlarging images that a private computer technician had identified as child pornography after viewing them only in a small "thumbnail" format. *Id.* at 822. The court explained that the police "did not exceed the scope of [the private] search because" both the police and the technician "testified that they could tell from viewing the thumbnails that the images contained child pornography. That is, the police learned nothing new through their actions." *Id.*; *see United States v. Lucas*, 640 F.3d 168, 179-80 (6th Cir. 2011) (officer did not exceed scope of search warrant when, while searching a computer for evidence of drug dealing, he happened upon thumbnails of files appearing to be child pornography and enlarged a few images to confirm).

Here, as in *Reddick* and *Totsi*, it is irrelevant that Detective Schihl viewed these particular files in a different form (as a rendered image rather than as identified by its hash value) than did Google. Detective Schihl in fact viewed the same images that Google hash matched as images that it had *previously viewed*. Although Google personnel did not open and lay human eyes on these two particular files, they had previously done so for duplicates of the same images, and

Detective Schihl was unlikely to learn anything new. Dist. Ct. Op. Page ID #274. The subsequent viewing was within the scope of the initial private review.

CONCLUSION

The judgment of the district court should be affirmed.

December 26, 2018

Respectfully submitted.

/s/ *Ryan T. Mrazik*

Ryan T. Mrazik
Erin K. Earl
Rachel A. S. Haney
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000

Attorneys for Amici Curiae

CERTIFICATION OF COMPLIANCE

I certify that this brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 6,480 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). I further certify that the 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 it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

Dated: December 26, 2018

/s/ Ryan T. Mrazik
Ryan T. Mrazik

CERTIFICATE OF SERVICE

I certify that on December 26, 2018, I electronically filed the foregoing brief with the Clerk of Court for the United States Court of Appeals for the Sixth Circuit by using the CM/ECF system. I further certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: December 26, 2018

/s/ Ryan T. Mrazik
Ryan T. Mrazik