No. 14-3265

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee

v.

WALTER E. ACKERMAN,
Defendant-Appellant.

On Appeal from the United States District Court
for the District of Kansas (Wichita)
No. 6:13-cr-10176-EFM (Hon. Eric F. Melgren)

BRIEF OF DROPBOX, INC., FACEBOOK, INC., GOOGLE INC., MICROSOFT CORPORATION, PINTEREST, INC., SNAPCHAT, INC., and TWITTER, INC. AS AMICI CURIAE SUPPORTING APPELLEE

Eric D. Miller
Ryan T. Mrazik
Nicola Menaldo
Erin K. Earl
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Telephone: (206) 359-8000

CORPORATE DISCLOSURE STATEMENT

Dropbox, Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Facebook, Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Google Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Microsoft Corporation has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Pinterest, Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Snapchat, Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Twitter, Inc. has no parent corporation and no publicly held corporation owns 10% or more of its stock.

Respectfully submitted,

By:/s/ Eric D. Miller
Eric D. Miller
Attorney for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATEMENT OF INTEREST[1]

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

Dropbox enables the easy storage and synchronization of photos, documents, and videos across multiple electronic devices. It empowers users to seamlessly share and collaborate with colleagues, family, and friends.

Facebook's mission is to make the world more open and connected. 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 offers a variety of web-based products and services—including Search, Gmail, Google+, Maps, YouTube, and Blogger—used by people everywhere.

Microsoft empowers people and organizations to achieve more through a wide range of cloud- and desktop computer-based software, services, and hardware products, including its Windows operating system, the Microsoft Office suite of productivity applications, the Surface tablet, and the Xbox entertainment system.

[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.

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

Snapchat is a mobile storytelling platform. People everywhere use Snapchat every day to share video and photo Snaps with friends, view Live Stories from major cultural events and cities around the world, and explore curated news and entertainment through Snapchat's Discover feature.

Twitter provides a web- and mobile-based global platform for public self-expression and conversation in real time. Its mission is to give everyone the power to create and share their ideas and information instantly, without barriers.

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 small fraction of users abuse amici's services, in violation of amici's terms of service, to offer, store, and transmit child pornography.[2] Amici

[2] Amici and courts sometimes use other terms to refer to such material, including "child exploitation material" or "child sexual abuse images." *See, e.g.*, *Paroline v. United States* 134 S. Ct. 1710, 1741 (2014) (Sotomayor, J., dissenting). In this brief, amici use the term "child pornography" for clarity and to be consistent 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.

devote substantial human and technological resources to keeping this material, which exploits the most vulnerable members of our society, off of their services.

One such technological resource is the process of hash matching, an automated computer process used to detect duplicates of previously identified images of child pornography. Although service providers may use different types of hash matching processes—such as the MD5 process used by AOL in this case or the PhotoDNA process developed in part by Microsoft—hash matching enables service providers such as amici to protect their networks, services, and users by reliably and efficiently detecting duplicates of files that they have previously identified as child pornography and to remove those files from their services. Amici also report such images to fulfill their statutorily imposed duty to report any "apparent violation of" the federal child pornography statutes to the National Center for Missing and Exploited Children ("NCMEC"). 18 U.S.C. § 2258A.

Because of their interests, as both corporate citizens and businesses, in safeguarding the integrity of their services and keeping child pornography off of their products and services, amici have a strong interest in the outcome of this case.

SUMMARY OF ARGUMENT

The district court correctly held that NCMEC did not violate the Fourth Amendment when a NCMEC analyst reviewed an image that AOL had identified as child pornography through the technological process known as hash matching.

Hash matching is an automated process that permits providers like AOL and amici to determine whether one electronic file is the same as another. By using hash matching to identify files that are duplicates of an image of child pornography that a person has previously viewed with his or her own eyes, service providers can protect their networks, services, and users by efficiently finding and removing copies of that file from their services without further human review. Then, having identified an "apparent violation of" the federal child pornography statutes, service providers report the image to NCMEC in accordance with 18 U.S.C. § 2258A.

The district court correctly held that, under the analysis of *United States v. Jacobsen*, 466 U.S. 109 (1984), the NCMEC analyst's review of an image of child pornography was within the scope of a private search conducted by AOL via hash matching and therefore did not violate the Fourth Amendment. Given the reliability of hash matching technology, when the NCMEC analyst reviewed the image reported by AOL, she was virtually certain to find only child pornography and stood to gain little, if any, additional information from reviewing that image.

Ackerman nevertheless argues that the NCMEC analyst exceeded the scope of AOL's initial private search because the analyst "actually viewed the images." Ackerman Br. 51. He relies on *Walter v. United States*, 447 U.S. 649 (1980), in which the Supreme Court held that the FBI violated the Fourth Amendment by conducting a warrantless viewing of films after a private search had examined only the labels on the films' canister. But as the district court recognized, a hash value for a file is different from a label on a film canister because the hash value is derived mathematically from a particular file using industry-standard algorithms and is unique to that file. A hash match, therefore, is file-specific, accurate, and reliable, and AOL had already identified the images at issue as duplicates of child pornography before the NCMEC analyst reviewed them. That AOL identified these duplicate images using an automated computer process instead of a person makes no difference to the Fourth Amendment analysis.

ARGUMENT

Hash matching is a reliable, accurate, and efficient process for service providers to find duplicates of files that they previously identified as child pornography. Here, AOL used hash matching to identify an image of child pornography, and it reported that finding and a copy of the image to NCMEC. Dist. Ct. Op. 3; *see* 18 U.S.C. § 2258A. Ackerman argues that NCMEC's subsequent review of the image violated the Fourth Amendment. Ackerman Br. 41-47. The district court rejected that argument on the ground that NCMEC is not a state actor subject to the Fourth Amendment. Memorandum and Order dated 4/28/15, docket number 37 ("Dist. Ct. Op."), at 11-16. Amici take no position on that issue, but even if NCMEC is a state actor, the district court's judgment should be affirmed on the basis of its alternative holding that NCMEC's review of the image did not exceed the scope of the initial private search that AOL had already conducted.[3]

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

Service providers use hash matching technology to identify duplicates of images that a person previously identified as child pornography. In this context, hash matching involves calculating an alphanumeric value (a "hash value") from a specific file that a person identifies as child pornography and then identifying duplicates of that file by comparing its hash value with the hash values of unknown files. Dist. Ct. Op. 3. Hash matching enables service providers to find and remove duplicates of child pornography files accurately and efficiently, without a need for further human review of the image.

Calculating a hash value involves applying a mathematical algorithm to a piece of information. Although there are various methods and algorithms for calculating hash values, the process, known as "hashing," has been widely used 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

[3] As an alternative basis for affirmance, the government argues that Ackerman lacked a reasonable expectation of privacy in his email. *See* Gov't Br. 16-25. This Court need not consider that argument, which raises a difficult constitutional question, because the judgment may be affirmed on the basis of the district court's correct determination that the NCMEC analyst did not exceed the scope of AOL's private search.

of data are exact matches. *See Microsoft Computer Dictionary* 214 (4th ed. 1999); Niels Ferguson, Bruce Schneier & Tadayoshi Kohno, *Cryptography Engineering: Design Principles & Practical Applications* 77 (2010); *see also* Richard P. Salgado, *Fourth Amendment Search and The Power of The Hash*, 119 Harv. L. Rev. F. 38, 39 (2005) ("Hashing is the process of taking an input data string (the bits on a hard drive, for example), and using a mathematical function to generate a (usually smaller) output string.").

A hash value is "unique to a specific file" and often referred to as a "digital fingerprint," Dist. Ct. Op. 3, or a "digital signature." Ronald Rivest, *The MD5 Message-Digest Algorithm* (1992), *available at* 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 or might not accurately describe the file's content. Rather, a hash value for a file is specific to that file and is inextricably linked to the file, bit-for-bit. *See* Salgado, 119 Harv. L. Rev. F. at 39 ("[O]ne could take a digital wedding photo from a hard drive and calculate the hash value of the photo [and] [n]o other file will have the same hash value as the wedding photo, except a file that is identical, bit-for-bit.").

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 on their services only against calculated hash values for images that have already been identified by a person as child pornography. Here, for example, "AOL's graphic review team would . . . determine if an image met the definition of child pornography" and, if so, would calculate the file's hash value and store that value in a database. Dist. Ct. Op. 3.

Then, because the calculated hash value is specific to each image whose hash value was included in the data set, a service provider can use the hash value to identify duplicates of that file. *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."). According to the district court, AOL, for example, systematically scans emails "sent, saved, or forwarded from an AOL account to scan for malware, viruses, and illegal images such as child pornography." *See* Dist. Ct. Op. 3. When scanning to identify duplicates of images of child pornography, AOL calculates the hash values for such emails and compares them to its stored hash values for child pornography files. *Id*. When it finds a match—indicating that an unknown file is child pornography—"the email is captured, and AOL terminates the user's account." *Id.*

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). The hashing algorithm used in this case is called MD5, and it generates a hash value represented as a 32-digit hexadecimal sequence. *See* Dist. Ct. Op. 3; Rivest, *supra*. Like other industry-standard hash algorithms, MD5 reliably generates identifiers that are sufficiently unique to ensure that files with matching hash values are indeed the same. The algorithm can generate more than 340 undecillion (340 x 10^{36}) possible hash values, so while a false positive hash match—that is, two different files that yield matching hash values—is theoretically possible, the chances of it occurring are "infinitesimally small." Salgado, 119 Harv. L. Rev. F. at 39 n.6.

Hash matching identifies duplicates of 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. With billions of users sending tens of billions of communications through amici's services, a reliable and accurate automated process for identifying duplicates of child pornography is the best and most realistic means for service providers to protect their services and users from child pornography. *See Paroline*, 134 S. Ct. at 1717

(“Because child pornography is now traded with ease on the Internet, ‘the number of still images and videos memorializing the sexual assault and other sexual exploitation of children, many very young in age, has grown exponentially.’” (quoting P. Saris et al., U.S. Sentencing Comm’n, *Federal Child Pornography Offenses* 3 (2012)).

B. A NCMEC analyst does not violate the Fourth Amendment by reviewing an image of child pornography that has been identified by a service provider through hash matching.

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

The Fourth Amendment applies “when government officers violate a person’s reasonable expectation of privacy” or physically trespass upon the areas enumerated in the Amendment. *United States v. Jones*, 132 S. Ct. 945, 950 (2012) (internal quotation marks and citation omitted). The Fourth Amendment “proscrib[es] only governmental action,” and therefore “it is wholly inapplicable ‘to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government.’” *Jacobsen*, 466 U.S. at 113 (quoting *Walter*, 447 U.S. at 662 (Blackmun, J., dissenting)); *see United States v. Benoit*, 713 F.3d 1, 9 (10th Cir. 2013).

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 conduct unreasonable." *Id.* at 114-15. When a government agent reviews or conducts another search based on the information provided to it 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. Walsh*, 791 F.2d 811, 814 (10th Cir. 1986). 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 NCMEC's review of an image of child pornography was within the scope of AOL's initial private search.

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. Applying that decision, the district court correctly determined that the Fourth Amendment did not prohibit a NCMEC analyst from reviewing an image of child pornography that AOL had identified by hash matching and then reported to NCMEC. Dist. Ct. Op. 16-20.

In *Jacobsen*, FedEx employees opened both a package and a tube inside the package to discover plastic bags, the innermost of which contained white powder that the FedEx employees identified as cocaine. *See* 446 U.S. at 111. They turned the package over to the DEA, which again removed the cocaine from the tube. *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 further concluded that a field test conducted by the agent to confirm the presence of cocaine did exceed the scope of the private search but that the field test did not require a warrant because it could not disclose any facts in which defendants had a legitimate privacy interest. *Id.* at 122-26.) In sum, the Court held 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 controlled by *Jacobsen*. Dist. Ct. Op. 18-19. Because NCMEC did not exceed the scope of AOL's search but merely "view[ed] … what a private party had freely made available for [its] inspection," it did not implicate the Fourth Amendment. *Jacobsen*, 446 U.S. at 119.

Ackerman contends instead that this case is controlled by *Walter*, but his reliance on that case is misplaced. In *Walter*, a private carrier misdelivered a set of packages, and the recipients opened the packages and saw that they 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 that "[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." *United States v. Lichtenberger*, 786 F.3d 478, 485-86 (6th Cir. 2015). In this case, those factors make clear that the district court was correct to conclude that NCMEC did not exceed the scope of AOL's search.

First, when NCMEC viewed the image file reported by AOL, there was a virtual certainty that the file would contain nothing other than child pornography. *See Jacobsen*, 466 U.S. at 119-120. AOL's hash matching process can identify only duplicates of files previously identified as child pornography, so the chance that the image AOL reported to NCMEC would be something other than child pornography was essentially zero. Indeed, the reliability of hash matching is even better than the reliability of a human report of the results of a private search, as in *Jacobsen*. Hash matching processes can identify duplicates of a file, bit-by-bit, and their recollection and ability to match unknown files to those that a person previously identified as child pornography are more reliable and accurate than a human trying to look at two photographs to determine whether they are the same.

That extremely high level of certainty distinguishes this case 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, AOL knew the contents of the file: it was a duplicate of a file that a person previously identified as child pornography. The hash match indicating as much was not a mere label on a canister, which can be subjective or inaccurate. Instead, the MD5 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, or the possibility of human error or misdescription. The district court correctly understood that distinction:

> A label does not tell you anything about the file—except for what the file may contain. In contrast, a hash value is much

> more specific. As noted above, a hash value is derived from a specific digital file and is an alphanumeric sequence that is unique to that digital file. Any identical copy of that file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. AOL only retains a database of hash values already associated with child pornography. AOL's discovery of an email containing a hash value that matched its database of hash values, therefore, would convey that the file contains child pornography.

Dist. Ct. Op. 18-19.

Second, because NCMEC could be virtually certain that the image reported by AOL was child pornography, it stood to gain little or no additional information through its review. Because NCMEC analysts are humans, they must view hash-matched child pornography files received from providers to confirm their content. But when NCMEC analysts receive a hash-matched image file, they know what they will find: an image that the service provider identified as child pornography. 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.

Ackerman attempts to analogize a NCMEC analyst's review of an image of hash-matched child pornography to the FBI's viewing of the films in *Walter*. Ackerman Br. 51. Unlike in *Walter*, however, when the NCMEC analyst reviewed the images here, AOL had already identified them as child pornography. How a service provider such as amici identifies a file as child pornography—whether by human review or by a reliable and accurate computer program finding duplicates of such files—is irrelevant. In either case, a NCMEC analyst's review of an image identified by a service provider as child pornography does not expand the scope of the private search conducted by the service provider.

3. The district court's conclusion is supported by decisions of other courts of appeals.

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 when he enlarged images previously identified as child pornography by a private computer technician who had viewed the images only as thumbnails. (Thumbnails are "reduced, lower-resolution versions of full-sized images." *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1155 (9th Cir. 2007).) The court explained that the police "did not exceed the scope of [the private] search because" both the police and the private 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." *Tosti*, 733 F.3d at 822; *see United States v. Walser*, 275 F.3d 981, 987 (10th Cir. 2001) (law enforcement officer did not exceed scope of search warrant when, while searching a computer for evidence of drug dealing, he happened upon a thumbnail of a file appearing to be child pornography and enlarged the images to confirm).

Here, as in *Tosti*, it is irrelevant that NCMEC viewed the image in a different form (as a complete image rather than as identified by its hash value) than did AOL. NCMEC viewed the precise image that AOL identified as child pornography, and it therefore was unlikely to learn anything new through its viewing. Dist. Ct. Op. 19 ("NCMEC, in viewing the hashed file, did not learn anything additional that had not been previously learned by AOL."). The subsequent viewing was within the scope of the initial private search.

Amici are not aware of any decisions of a federal court of appeals holding that the government violated the Fourth Amendment by reviewing the results of an initial, reliable private search of an item that revealed contraband. Rather, other circuits have identified Fourth Amendment violations where government searches involved *more* or *different* items than the private search. *See, e.g.*, *Lichtenberger*, 786 F.3d at 488 (government's search of a laptop included accessing and viewing images that had not been accessed or viewed by the private party); *United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001) (government searched computer disks turned over by suspect's ex-wife that the ex-wife had not previously examined).

In contrast, courts have held that subsequent review of an initial, private search does not violate the Fourth Amendment where a private party examined the same evidence and identified it as contraband. *See, e.g.*, *Rann v. Atchison*, 689 F.3d 832, 837-38 (7th Cir. 2012) (upholding police review of child pornography where the victim "turned exactly one memory card over to the police, and her mother gave the police exactly one zip drive" and the victim and her mother "knew exactly what the memory card and the zip drive contained"); *United States v. Bowers*, 594 F.3d 522, 524 (6th Cir. 2010) (upholding government agents' search of a photo album because the roommate had described the contents of the album as child pornography); *cf. United States v. Brooks*, 427 F.3d 1246, 1250 (10th Cir. 2005) (holding that there was "no discernable difference" between an automatic disk search for child pornography that defendant consented to and the manual search that took place because the defendant "understood his computer was to be searched for pornographic images and voluntarily consented to such a search"). The reasoning of those cases is fully applicable here.

CONCLUSION

The judgment of the district court should be affirmed.

Respectfully submitted.

s/ Eric D. Miller

Eric D. Miller
Ryan T. Mrazik
Nicola Menaldo
Erin K. Earl
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000

Attorneys for Amici Curiae

August 2015

CERTIFICATE 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 4,434 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). 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 2010 in 14-point Times New Roman font.

Dated: August 7, 2015

s/ Eric D. Miller
Eric D. Miller

CERTIFICATE OF SERVICE

I certify that on August 7, 2015, I electronically filed the foregoing brief with the Clerk of Court for the United States Court of Appeals for the Tenth 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.

I certify that all required privacy redactions have been made.

I certify that, within two business days, I will cause to be delivered to the Clerk of the Court seven exact copies in paper form of this electronically filed brief.

I certify that, prior to filing, I have scanned this file using System Center Endpoint Protection updated on August 7, 2015, which indicates that it is free of viruses.

s/ Eric D. Miller
Eric D. Miller