Misc. Nos. 16-960-M-1, 16-1061-M

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH WARRANT NO. 16-960-M-1
TO GOOGLE

IN RE SEARCH WARRANT NO. 16-1061-M
TO GOOGLE

BRIEF FOR AMICI CURIAE MICROSOFT CORPORATION, AMAZON.COM, CISCO SYSTEMS, INC., AND APPLE INC. IN SUPPORT OF GOOGLE INC.

Kevin M. Kelly (PA Bar No. 311876)
James M. Garland*
Alexander A. Berengaut*
Katharine Goodloe*
COVINGTON & BURLING LLP
One CityCenter
850 10th Street, NW
Washington, DC 20001

Counsel for Amici Curiae Microsoft Corporation and Amazon.com

David Harvey (PA Bar No. 89122)
ORRICK, HERRINGTON & SUTCLIFFE LLP
2121 Main Street
Wheeling, WV 26003

Robert M. Loeb*
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street NW
Washington, DC 20005

E. Joshua Rosenkranz*
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Brian P. Goldman*
Evan Rose*
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105

Counsel for Amici Curiae Microsoft Corporation, Apple Inc., and Cisco Systems, Inc.

*Admissions for *pro hac vice* pending

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTERESTS OF *AMICI CURIAE*

Amici Microsoft Corporation, Amazon.com, Apple Inc., and Cisco Systems, Inc. are leading technology companies that provide communications and cloud-based computing services and software to more than one billion customers in over 90 countries around the world. Customers entrust Amici to securely store their private emails and contents of other communications in data centers. Certain Amici store some of those communications in data centers in foreign countries. Microsoft, for example, stores European customers' communications in a European data center in order to reduce network delays and allow customers faster access to their private correspondence. The U.S. Government frequently serves some Amici with warrants issued under the Stored Communications Act (SCA). When the data sought is stored in a U.S. data center, Amici regularly comply with such warrants. The Government, however, also has attempted to use such warrants to force some Amici, without consent of the customer or the foreign country, to seize private emails stored in a foreign country and to turn them over to the Government. But the SCA does not authorize warrants that reach into other countries, and forcing those Amici to execute such searches on the Government's behalf would place those Amici in the position of being compelled to risk violating foreign data privacy laws.

When faced with such a warrant seeking private emails stored in Ireland, Microsoft recently challenged the lawfulness of the warrant—a challenge supported by 28 technology and media companies, 23 trade associations and advocacy groups, 35 of the nation's leading computer scientists, and the Republic of Ireland. The Second Circuit agreed with Microsoft that the SCA does not authorize warrants seeking data stored on servers in foreign countries. That court recognized, as do Amici, that the SCA—a statute enacted when the internet was still in its

infancy—needs to be updated to both strengthen its protections on individual privacy in light of advances in technology and ensure that those advances do not prevent law enforcement from being able to do their jobs. But the court also understood that any such modernization must come from Congress, not the judiciary. Amici submit that this Court should embrace the Second Circuit's ruling and reject the magistrate judge's contrary approach.[1]

INTRODUCTION

This case addresses the reach of the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., which Congress enacted as part of the Electronic Communications Privacy Act of 1986. Technology has changed dramatically since the SCA became law. The Congress that drafted the SCA could barely have imagined the notion of storing emails halfway across the globe. That is why companies, commentators, and privacy advocates alike have long called for the SCA to be updated in light of the realities of 21st century technology.

The question here, however, is the scope of the SCA as it now stands, not as Congress might eventually revise it. As written today, the SCA does *not* contain a "clear indication of an extraterritorial application," and so, under the established presumption against extraterritoriality, "it has none." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 248 (2010).[2] That presumption ensures that courts do not apply statutes in ways that potentially risk "unintended clashes between our laws and those of other nations," *EEOC v. Arabian Am. Oil. Co.*, 499 U.S. 244, 248 (1991) (*Aramco*). Yet, notwithstanding its agreement that the SCA does not extend outside the United States, the Government here seeks to use SCA warrants to do just that: reach into other

[1] Amici are filing this brief with the consent of both parties. More information about individual Amici is included in the motion for leave to file this brief.

[2] The parties here agree "that Congress did not intend the SCA's warrant provisions to apply extraterritorially." Op. 16.

countries to seize private email content stored there. The magistrate judge, believing that granting the Government such power is sound policy, embraced the Government's flawed argument that a warrant requiring a provider to seize and copy communications stored overseas at the behest of the Government is a domestic act so long as the communications are disclosed to and reviewed by law enforcement agents in the United States. But the Supreme Court has expressly directed that such policy considerations are the sole province of Congress.

The magistrate judge therefore erred both in looking to policy considerations and in his ultimate conclusion that there is no invasion of privacy when a service provider is compelled by the Government to execute an SCA warrant by seizing and copying private communications in another country—and that the only privacy breach occurs upon the later domestic disclosure of the data to the Government. The fiction that such a foreign search and seizure is a domestic act was properly rejected by the Second Circuit in *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* (*Microsoft I*), 829 F.3d 197 (2d Cir. 2016). There, the Second Circuit correctly held that the Government cannot use a warrant issued under the SCA to compel a provider to retrieve email content stored in Ireland. The court recognized that the SCA's focus is "protecting the privacy of … stored electronic communications," and that an "invasion of [that] privacy takes place under the SCA where the customer's protected content is accessed." *Id.* at 217, 220. When a warrant seeks email content from a foreign data center, that invasion of privacy occurs outside the United States—in the place where the customers' private communications are stored, and where they are accessed, and copied for the benefit of law enforcement, without the customer's consent.

Because execution of a warrant seeking data stored abroad constitutes an improper extraterritorial application of the SCA, the magistrate judge's ruling should be set aside. The

magistrate judge's approach allows for an intrusion upon foreign sovereignty that Congress has not authorized. Equally troubling, it invites foreign nations to reciprocate by likewise demanding that local offices of U.S. technology companies turn over U.S. citizens' private communications stored on U.S. soil. It also places technology companies that store customer data abroad in the untenable position of being compelled to risk violating foreign data privacy laws to comply with warrants issued by U.S. courts. Only Congress can update the SCA to reflect the new technological landscape while at the same time appropriately balancing relevant interests. Congress should promptly do so; but until it does, courts may not extend the SCA to reach data stored in another sovereign country.

ARGUMENT

I. The Stored Communications Act Does Not Authorize Warrants For Seizure Of Private Emails Stored In A Foreign Country.

It is a "basic premise of our legal system," *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016), that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none." *Morrison,* 561 U.S. at 248. The Government agrees that the SCA gives no such indication, and so does not extend extraterritorially. Simply put, nothing in the SCA purports to regulate or protect in any way private communications stored overseas. The question here, then, is whether forcing a provider to execute a warrant in another country constitutes an extraterritorial *application* of the SCA. As the Second Circuit explained in regard to a warrant seeking email content stored in Ireland, "[b]ecause the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States." *Microsoft I,* 829 F.3d at 220.

This conclusion is confirmed by the international outrage the Government's actions have provoked in similar cases. Our sister nations clearly view U.S. warrants directing service providers to access, copy, and transmit to the United States data stored on servers located within their territory as an extraterritorial act on the part of the U.S. Government. *See*, *e.g*, Brief of *Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *Microsoft I*, No. 14-2985, Dkt. 148 (2d Cir. Dec. 19, 2014). Indeed, they view this as an affront to their sovereignty in much the same way that physically conducting law enforcement activity on foreign soil would violate their sovereignty and territorial integrity. *See* Restatement of Foreign Relations § 432 cmt. b; *see also* Morrison, 561 U.S. at 269 ("The probability of incompatibility with the applicable laws of other countries" is a strong signal that Congress did not intend such a foreign application.). Warrants issued under the SCA therefore "may reach only data stored within United States boundaries," and authorizing such a warrant to seize emails from a data center in a foreign country, as the magistrate judge has done here, constitutes "an unlawful extraterritorial application of the Act." *Microsoft I*, 829 F.3d at 221.

A. The conduct relevant to the SCA's focus is intrusion on the privacy of stored communications.

Where, as here, a statute has no extraterritorial force, the Supreme Court instructs courts to examine whether the "conduct relevant to the statute's focus" or "the objects of the statute's solicitude," would occur abroad. *RJR Nabisco*, 136 S. Ct. at 2101; *Morrison*, 561 U.S. at 267. The magistrate judge here correctly recognized that the SCA's focus is on safeguarding the privacy of electronically stored communications. Op. 16. The magistrate judge was also correct that, for purposes of extraterritoriality analysis, the conduct relevant to that focus is the interference with or intrusion on privacy. *Id.* The magistrate judge therefore asked the right question: Where does the interference with the customer's privacy occur? Op. 18. But the

magistrate judge went astray by equating the relevant conduct—the conduct that intruded on a customer's privacy—with the ultimate disclosure of the customer's information to law enforcement officials in the United States. Op. 23. The magistrate judge's focus on the place of *disclosure*, as opposed to the location of the "electronic storage" from which a provider would be ordered to *access and retrieve* private communications, is, given the current structure of the law, wrong for several reasons.

First, the SCA makes clear that its focus is protecting against the accessing and removal of private "communications … in electronic storage." 18 U.S.C. §§ 2702(a), 2703(a). Notably, the SCA is violated as soon as someone "accesses without authorization" a service provider's servers and "thereby obtains" an "electronic communication while it is in electronic storage," irrespective of whether that person discloses the communications. *Id.* § 2701(a). And, as the Third Circuit has recognized, "the Stored Communications Act was born from congressional recognition" of the need to protect "against potential intrusions on individual privacy arising from illicit *access* to … large data banks that stored e-mails." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) (emphasis added and internal quotation marks omitted), *cert. denied*, 137 S. Ct. 36 (2016). Accordingly, "[t]he better approach, which … is more in keeping with the *Morrison* analysis and the SCA's emphasis on data storage, is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* (*Microsoft II*), No. 14-2985, 2017 WL 362765, at *5 (2d Cir. Jan. 24, 2017) (Carney, J., concurring in the denial of rehearing en banc). That access occurs at the location of the servers on which the data is stored, just as when an agent points a thermal imaging sensor at a house "from the passenger seat of [his] vehicle across the street," the search

is in the house, not in the car and not on the exterior wall. *Kyllo v. United States*, 533 U.S. 27, 30, 35 & n.2 (2001).

Second, if the relevant conduct were disclosure, as the magistrate judge suggests, the SCA provision that prohibits providers from voluntarily disclosing customers' communications, § 2702, would offer no protection against a U.S. service provider who copied a U.S. customer's U.S.-stored emails and willfully disclosed them to a foreign tabloid newspaper. Under the magistrate judge's view of the SCA, so long as the disclosure occurred overseas, the customer would have no recourse under §§ 2702 and 2707. That cannot be right. The one thing Congress certainly sought to protect when it enacted the SCA in 1986 was the privacy of U.S. customers' electronic communications stored within the United States.

Third, the magistrate judge was wrong to suggest that a customer's privacy interest in his or her stored emails is not infringed where a provider retrieves the email content from storage and copies it at the Government's behest and without the customer's permission. Such access violates the customer's reasonable expectation of privacy in a way that the provider moving the customer's data from one location to another in order to ensure fast, uninterrupted service does not. It also is in tension with foreign data protection and privacy laws, which protect the customer's privacy interests in email stored abroad. Thus, as the Second Circuit held, the infringement is not limited to the disclosure, but rather occurs when the service provider is required "to 'collect' [private email content] from servers located overseas and 'import' [it] into the United States." *Microsoft I*, 829 F.3d at 221.

B. Executing a warrant seeking email content from a data center in a foreign country would effect a law enforcement search and seizure on foreign soil.

In deciding where the relevant privacy infringement occurs, the magistrate judge looked to Fourth Amendment search and seizure standards. That analysis, however, does not support the magistrate judge's ruling.

As an initial matter, law enforcement agencies may not execute search warrants for property in foreign countries *at all*: Any warrant issued by a judicial officer in this country "would be a dead letter outside the United States." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990).[3] Thus, a warrant issued under the SCA plainly would not authorize FBI officials to enter a foreign data center themselves and seize emails of a customer. The SCA should not be read to permit warrants that conscript technology companies into doing on the Government's behalf that which SCA warrants do not—and cannot—empower law enforcement agents to do themselves.

The SCA describes the company's role in complying with the Government's demand as "execut[ing the] search warrant." § 2703(g). In so doing, the email provider—compelled to locate, seize, and copy the private emails of its customers—effects a law enforcement search and seizure. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (search or seizure conducted by a private individual is treated as governmental action where that individual is acting as an agent of the government). And when the customer's information is stored outside the United States, executing the warrant requires the technology company to conduct, at the Government's

[3] For that reason, the U.S. Department of Justice has recognized that a U.S. search warrant cannot even authorize law enforcement agents to remotely access electronic storage media located in another country because to do so would be an extraterritorial application of U.S. law. *See* Letter from Mythili Raman, Acting Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 1, 4-5 (Sept. 18, 2013), https://perma.cc/MC3X-RPYH.

behest, a search and seizure in foreign territory. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (rejecting argument that computer software that compiles data from a target computer and transmits the data to FBI agents in a particular district would effect a search only in that district).

In concluding that no extraterritorial application of the SCA occurs when the Government invokes the statute to require a service provider to execute a warrant for email content stored in a foreign country, the magistrate judge mistakenly focused on only one aspect of customers' interest in their stored data—the customer's ability to retrieve her own email content. The magistrate judge reasoned that no extraterritorial seizure would occur because copying content stored on a foreign server and importing it into the United States does not meaningfully interfere with a customer's ability to access her correspondence. Op. 18-22. But even if that is correct, privacy rights are not so narrow. The warrants *do* interfere with important property rights—namely, the right to exclude and limit access. *See Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419 (1982). Thus, the Supreme Court has recognized that intangible property can be seized even absent interference with any right of access to that property. *See Katz v. United States*, 389 U.S. 347, 354 (1967) (listening to and recording telephone-booth conversations constituted both a search and a seizure); *Berger v. New York*, 388 U.S. 41, 59 (1967) (electronic audio recording device seized "communications, conversations, or discussions" when they were recorded). Email conversations are no different.[4]

[4] The cases the magistrate judge cited holding that physical property is not seized when photographs are taken or photocopies are made of it, *see* Op. 19-21, are therefore inapposite. *Katz* and *Berger* show that it makes no sense to mechanically apply standards relating to the seizure of tangible property when assessing whether a seizure of *intangible* property, such as digital communications, has occurred.

Significantly, at least four Courts of Appeals have held that copying electronic data effects a seizure of that data, and none has held otherwise. *See Microsoft I*, 829 F.3d at 220 (executing SCA warrant would mean seizing stored communications from foreign datacenter); *see also, e.g.*, *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (emails were seized when provider acceded to the Government's request that the provider make copies); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1169 (9th Cir. 2010) (en banc) (data was seized when copied from a defendant's computer); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (search and seizure occurred when Yahoo! technicians copied contents of email accounts from Yahoo! servers without reviewing the contents of individual emails in order to turn data over to law enforcement authorities), *cert. denied*, 538 U.S. 993 (2003). These cases reaffirm that, even under Fourth Amendment seizure standards, an invasion of a customer's privacy interest in the content of his emails occurs at the time the provider is compelled to locate, seize, and copy the email content without the customer's consent.

The magistrate judge's related conclusion that no search would occur until the communications are disclosed to and reviewed by law enforcement authorities, Op. 22-23, is similarly mistaken. The Government intrudes upon customers' reasonable expectation of privacy in the contents of their emails as soon as the provider, acting under orders from the Government, gathers up and copies their communications from electronic storage. *See Warshak*, 631 F.3d at 288. It is no answer to say, as the magistrate judge did, that a provider might regularly move communications as part of the everyday process of providing and improving email service; customers do reasonably expect that their stored data will be moved for these ordinary (and authorized) business purposes, but *only* those purposes. By contrast, customers *do not* expect that the Government will conscript the provider to access, copy, and transmit their

emails to the United States for purposes of handing them over to law enforcement. Such an extraordinary, government-mandated act is an invasion of privacy, plain and simple. *See id.*

The magistrate judge's position that a search would occur only when and where law enforcement *review* the emails is also at odds with the Supreme Court's Fourth Amendment jurisprudence. *See Kyllo*, 533 U.S. at 30, 35; *Katz*, 389 U.S. at 358 (by recording and listening to conversations, police searched telephone booth). In fact, the Government has acknowledged that, where law enforcement agents execute a warrant for private electronic information themselves, a search occurs even *before* they review the data.[5] The result is no different when the Government forces a service provider to access its overseas servers, seize and copy private customer email content, and import it into the United States to be turned over to a law enforcement agency—whether or not the service provider can accomplish this task from a terminal based in the United States. "[C]alling such an application 'domestic'" because the data is turned over within the United States "runs roughshod over the concerns that undergird the Supreme Court's strong presumption against extraterritoriality." *Microsoft II*, 2017 WL 362765 at *4 (Carney, J. concurring); *see Morrison*, 561 U.S. at 266 (the mere presence of "*some* domestic activity" does not render a particular application of the statute domestic).

II. Only Congress Can Decide Whether And How To Update The SCA.

The magistrate judge's rejection of the Second Circuit's *Microsoft I* decision was largely animated by his view of practical considerations about law enforcement needs. Op. 24-29. But the Supreme Court established the presumption against extraterritoriality precisely because

[5] U.S. Dep't of Justice, Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 113 (2009), https://perma.cc/CK8H-R2RY ("Where the service provider lacks the ability or will to comply with [SCA warrant] … agents must search the provider's computers themselves.").

courts, unlike Congress, are inherently "limited … by the information provided by litigants in a particular case," *Microsoft I*, 829 F.3d at 232 (Lynch, J., concurring), and are therefore ill-equipped to address concerns of foreign sovereignty and international comity. The presumption against extraterritoriality therefore "cautions courts to assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws. It thereby helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164-65 (2004). How those foreign relations concerns should be balanced against the needs of law enforcement to obtain data stored in other countries is a policy question Congress must address, not one for courts to resolve.

The magistrate judge noted, for example, that, given Google's network architecture, it might not be possible to obtain the data stored abroad using the established Mutual Legal Assistance Treaty (MLAT) process.[6] *See* Op. 27-28. The magistrate judge also opined that, because Google's customer data is separated into "shards" and is therefore useless unless the Government receives every shard, the Government should be able to order a provider to seize all shards wherever they may be located. *See* Op. 24 n.17, 25-29. Those concerns had no application in the Second Circuit, which addressed Microsoft's storage of private electronic communications in Ireland, without any sharding. But the question whether the SCA can be used to reach into other countries is a question of statutory interpretation that does not turn on the network architecture of a particular provider.[7] The magistrate judge's concern about the

[6] Amici have no knowledge of the specifics of Google's network architecture, and therefore take no position as to the location of the data sought by the government in the warrants at issue here.

[7] The magistrate judge speculated that Google's storage methods reduce the risk of interference with foreign laws. Op. 24-26. But the specifics of one company's network architecture has no bearing on the SCA's extraterritorial reach. Under the magistrate judge's construction of the

practical effects of data sharding—which highlights one of the many ways the SCA is outdated—is ultimately for Congress to address.

By permitting U.S. law enforcement agencies to force service providers to retrieve and turn over data stored in foreign countries, without the consent of the foreign country or the customer, the magistrate judge's decision raises the very concerns identified in *Morrison* and *Kiobel*. So bold a projection of U.S. law enforcement power into foreign countries would show disdain for their sovereignty and threaten to disrupt the harmony existing between the United States and other nations. It also disregards the carefully calibrated, comity-protective framework established through MLATs and other bilateral agreements. And it might put service providers in the untenable position of being forced to violate foreign privacy law in order to comply with warrants issued by U.S. courts.

Authorizing such wide-ranging international warrants would also invite foreign nations to reciprocate, demanding access to communications stored in the United States without regard for U.S. law. The United States would have little ground to object if Russia or China or Saudi Arabia instructed a service provider operating within its territory to turn over private electronic communications stored within the United States, without the permission of the United States or the U.S.-based customer and without any federal court warrant. After all, under the magistrate judge's reasoning, that would be a purely domestic act by that foreign nation.

---

statute, courts could issue SCA warrants for *any* foreign-stored data, irrespective of a provider's network architecture. More fundamentally, the only proper question under *Morrison* is whether Congress has expressly indicated that an extraterritorial application of the statute is proper, not whether any *particular* warrant will cause international friction. *Morrison* thus overruled decades of Court of Appeals cases that engaged in the sort of case-by-case comity balancing the magistrate judge employed here, holding instead that the presumption against extraterritoriality "applies regardless of whether there is a risk of conflict between the American statute and a foreign law." 561 U.S. at 255.

These potentially disruptive outcomes underscore why only Congress has constitutional authority to balance law enforcement needs against the United States' relations with foreign nations, the privacy of its citizens, and the competitiveness of its technology industry. Amici fully agree with Judge Lynch, concurring in *Microsoft I*, that "the statute should be revised, with a view to maintaining and strengthening [its] privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement … against the interests of other sovereign nations." 829 F.3d at 233.

Congress has any number of possible revisions it might want to consider. It might seek to authorize the extraterritorial application of the SCA only for investigations of certain crimes and national security matters. It could extend the SCA to reach emails overseas, but only those belonging to U.S. citizens and permanent residents. Congress might even grant the Government the full power it now claims. But it was improper for the magistrate judge to substitute what he viewed as a "commonsense" result for Congress's silence on the question. Op. 24-25. It is not for a court to try to "'discern' whether Congress *would have wanted* the statute to apply" abroad had it foreseen that global electronic communications would present these challenges. *Morrison*, 561 U.S. at 255 (emphasis added).

By "design[ing the statute] afresh," Congress could "address today's data realities" while remaining "cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers." *Microsoft II*, 2017 WL 362765 at *5 (Carney, J., concurring). Until Congress does so, however, compelling service providers to execute SCA warrants to search and seize communications

stored on servers located in foreign countries remains an impermissible extraterritorial application of U.S. law.

CONCLUSION

For the foregoing reasons, the magistrate judge's order should be vacated.

Respectfully submitted,

/s/David Harvey

David Harvey (PA Bar No. 89122)
ORRICK, HERRINGTON & SUTCLIFFE LLP
2121 Main Street
Wheeling, WV 26003
dharvey@orrick.com

Robert M. Loeb*
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street NW
Washington, DC 20005
RLoeb@orrick.com

E. Joshua Rosenkranz*
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Brian P. Goldman*
Evan Rose*
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105

Counsel for Amici Curiae Microsoft Corporation, Apple Inc., and Cisco Systems, Inc.

Kevin M. Kelly (PA Bar No. 311876)
James M. Garland*
Alexander A. Berengaut*
Katharine Goodloe*
COVINGTON & BURLING LLP
One CityCenter
850 10th Street, NW
Washington, DC 20001

Counsel for Amici Curiae Microsoft Corporation and Amazon.com

*Admissions for *pro hac vice* pending

March 10, 2016

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing Amicus Curiae Brief with the Clerk of the Court for the United States District Court for the Eastern District of Pennsylvania by using the appellate CM/ECF system on March 10, 2017.

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.

COVINGTON & BURLING LLP

/s/ Kevin M. Kelly
Kevin M. Kelly (PA Bar No. 311876)
Counsel for Amici Curiae Microsoft Corporation and Amazon.com

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ David Harvey
David Harvey (PA Bar No. 89122)
Counsel for Amici Curiae Microsoft Corporation, Apple Inc., and Cisco Systems, Inc.