EXHIBIT A

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

In re Search Warrant No. 16-960-M-1 to Google	:	Magistrate No. 16-960-M-1
	:	
In re Search Warrant No. 16-1061-M-1 to Google	:	Magistrate No. 16-1061-M-1
	:	

BRIEF OF *AMICUS CURIAE* YAHOO INC.

Magistrate Judge Rueter's order compelling Google to produce private customer communications stored outside of the United States in response to a warrant conflicts with the plain text of the Stored Communications Act and Federal Rule of Criminal Procedure 41 and it creates a conflict with the Second Circuit's decision in *Microsoft*.[1] By creating this conflict, the Magistrate Judge's order has made it difficult for providers to understand when they must produce private customer data residing on a server outside of the United States to law enforcement in response to a warrant.

The Magistrate Judge's analysis of whether the SCA applies extraterritorially is incorrect. Rule 41 and the particular warrants issued under it, not the SCA, govern whether law enforcement has the power to conscript a provider to execute a search warrant and gather data located abroad. Rather than relying on established law and rules regarding warrants issued under Rule 41 or state warrant procedures, the Magistrate Judge improperly rewrote the SCA to create a hybrid warrant—setting off a chain of events that creates confusion, ignores international law and interests, and makes it more difficult for providers[2] like Yahoo with subsidiaries that manage

[1] *Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft, Corp.*, 829 F.3d 197 (2d Cir. 2016).
[2] "Providers" are any entity offering electronic communications services or remote computing services to the public. 18 U.S.C. § 2703(a) & (b).

and control data outside the United States to honor their obligations to their customers, the United States, and the foreign countries in which they operate.

The SCA's plain text is clear. It should not be read to create a never-before-seen type of legal process by implication. Section 2703(a) merely codifies an exception to the SCA's general prohibition on disclosure of customer information when law enforcement obtains and serves a warrant under the Federal Rules of Criminal Procedure or state law. Given the nature of the information sought and the unique role of providers in the context of data the SCA protects, Congress also expanded courts' authority to issue Rule 41 warrants and excused an officer from being present during the execution of a warrant. But it did not invent a new kind of legal process or otherwise imbue a Rule 41 warrant with extraterritorial power. In concluding otherwise, the Magistrate Judge erred.

The Magistrate Judge compounded his error by holding that the "search" of customers' data occurs solely in the United States because that is where the provider discloses data to law enforcement. This is wrong. Section 2703(a) has no force of its own. It does not even command any types of disclosure. Rule 41, not the SCA, must do the work, and it is the proper touchstone when analyzing where a search is conducted. Cases decided under Rule 41 repeatedly hold that the search occurs where the information is accessed—not where it is received or reviewed. The instant search will occur outside the United States, and Rule 41 does not authorize it.

Regardless of whether this Court adopts the Magistrate Judge's approach or Yahoo's, the search, if compelled, will impact data stored abroad, and issues of comity should be part of the Court's analysis. If other courts follow the Magistrate Judge's ruling and avoid comity and conflicts of laws analysis, the result will harm providers like Yahoo that can identify the particular foreign country in which they store data.

Addressing international comity is important because the pressure to respond properly to warrants from U.S. law enforcement that require the production of data stored outside the United States does not come solely from the United States. It comes from business partners around the world that require contractual terms that conflict with providers' obligations in responding to U.S. legal process. And additional pressure comes from customers who expect providers to live up to their privacy promises and disclosure truthfully how their data will be handled. Increasingly, these customers value these privacy protections and transparency. If U.S. companies cannot provide clear answers on which laws govern their data, they will be unable to offer competitive services globally.

The Magistrate Judge made what is essentially a policy choice to apply the SCA to data stored abroad and compel production. Rather than doing so, the Magistrate Judge should have acknowledged the current limitations of the SCA and Rule 41 and left any perceived defect or shortcoming for Congress to resolve. If Congress intended for the Government to have the power it seeks here—to compel the production of electronically stored data abroad—it could have addressed that goal in any number of previous amendments to the SCA and Rule 41. Any change should now come from Congress, not the Courts.

I. Interest of the Amicus Curiae

Yahoo offers electronic communications and remote computing services to customers around the world. Yahoo uses a global network of servers to provide fast, efficient, reliable services to users. Because some of those servers are located outside the United States and are operated by foreign subsidiaries, Yahoo and its foreign subsidiaries are subject to various foreign laws regarding data access and transfer. To comply with these laws and serve its customers, Yahoo is committed to transparency and enabling users to understand how it handles their personal information.

Yahoo faces these conflicts frequently when U.S. law enforcement requests data stored on servers abroad. The Magistrate Judge's failure to apply the SCA and Rule 41 as written, to consider the ramifications of applying Rule 41 extraterritorially, and to analyze issues of international comity, makes it difficult for Yahoo to comply with U.S. process and international law. Yahoo should be granted leave to participate as *amicus* in these proceedings and asks that this Court reject the Magistrate Judge's report and recommendation.

II. Argument

The Magistrate Judge's analysis of whether the SCA applies extraterritorially is incorrect. Rule 41 and the warrants issued under it, not the SCA, govern whether law enforcement has the power to conscript a provider to execute a search warrant and gather data located abroad. The SCA's plain text is clear and does not create a new form of legal process with virtually unlimited power. The SCA's warrant provisions only provide an exception to its general prohibition on disclosure of customer information when law enforcement obtains and serves a warrant under the Federal Rules of Criminal Procedure or state law. Resolution of this case depends on what the particular warrant served on Google can compel by its own force. Under Rule 41 and the cases that have considered it, the warrant is insufficient to compel Google to produce data stored abroad.

Even if the Court adopts the SCA extraterritorial analysis the Magistrate Judge employed, a compelled search here will impact data stored abroad, and issues of comity should be considered in this Court's analysis.

A. The Stored Communications Act Does Not Create a New Type of Search Warrant Authorizing or Compelling Extraterritorial Searches

The SCA does not create a new type of legal process dubbed a warrant, but that functions like a court order or subpoena. The warrant at issue is a Rule 41 search warrant, generally

subject to the restrictions of that rule with one exception. A Rule 41 warrant to search or seize electronic data would not authorize FBI officials to enter a foreign data center themselves and seize emails of a customer. The SCA does not grant this additional power. The Magistrate Judge erred in reading the SCA to permit warrants that conscript technology companies into doing on the Government's behalf what warrants do not and cannot empower law enforcement agents to do themselves.

The Magistrate Judge failed to consider the structure of the SCA properly. In § 2702(a), the SCA prohibits providers from knowingly divulging the contents of a communication carried or maintained on their service to any person or entity. An exception to this rule allows production to a governmental entity only as "authorized in section 2517, 2511(2)(a), or 2703 of this title . . . ." 18 U.S.C. § 2702(b)(2). And § 2703(a) imports Rule 41 by authorizing a governmental entity to "require the disclosure by a provider of an electronic communication service" of contents of communication "*only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure* (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a) (emphasis added). It also provides immunity to providers that respond to such a "warrant" and a good faith defense for reliance on "warrant or order." 18 U.S.C. § 2707(e).

This simple statutory scheme does not create any new form of warrant. Rather, it explicitly relies on *existing* authorities for federal and state warrants and merely included a warrant as an exception to its general prohibition on disclosure. When Congress used the word "warrant" in this exception, it meant a Rule 41 warrant or one issued under state warrant procedures. *See F.A.A. v. Cooper*, 566 U.S. 284, 292 (2012) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed

word in the body of learning from which it was taken.'") (quoting *Morissette v. United States*, 342 U.S. 246, 263 (1952)); *see also United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) *cert denied* 538 U.S. 993 (2003) ("While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants, and we find that Congress intended them to be treated as warrants."). Subpoenas or court orders are not the same. *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 854 (9th Cir. 1991) ("subpoenas are not search warrants."); *In re Grand Jury Proceedings*, 115 F.3d 1240, 1244 (5th Cir. 1997) ("the instruments are different in nature.") By contrast, when Congress intended to create a new type of process in the SCA it did so expressly, as is the case in § 2703(d), which applies to requests for certain types of non-content information from providers. The SCA has no similar provisions for hybrid warrants.

Rather than simply read "warrant" to have its common, everyday meaning, the Magistrate Judge mistakenly relied on 18 U.S.C. § 2703(a) and (g) to form the creation of a hybrid warrant. The text of 18 U.S.C. § 2703(a) creates no new form of legal process and by itself cannot compel production. It merely states that "[a] governmental entity may require" the disclosure of content from a provider "only pursuant to a warrant …." The only document with force to compel disclosure here is the warrant. Likewise, § 2703(g) does not refer to new court orders or special processes (as is the case in § 2703(d)). Instead, subsection (g) was Congress's response to *United States v. Bach*. In *Bach*, the Eighth Circuit found that law enforcement had violated 18 U.S.C. § 3105, which requires an officer's presence when executing a warrant, because Yahoo performed a search of the defendant's stored emails outside the presence of law enforcement. Congress responded with a narrow amendment removing *only* the restriction in § 3105 regarding the presence of an officer when executing a warrant. *See* 21st Century Dep't of Justice

Appropriations Auth. Act § 11010, Pub. L. 107-273 (2002) (amending the SCA to add § 2703(g)). Neither *Bach* nor the amendment had anything to do with the extraterritorial application of the SCA. *See* 21st Century Dep't of Justice Appropriations Auth. Act, H.R. 107-685 at 196 (2002) (commenting on amendment without references to extraterritorial application). The Court should not read such intent into it now.

Furthermore, subsection (g) would not have been required if the SCA had not otherwise incorporated Rule 41's procedures because nothing in the SCA itself requires an officer's presence. This subsection proves that Congress relied on existing Rule 41 authorities in drafting the SCA. Notably, the SCA does not exempt law enforcement from *any other* requirement applicable to warrants in chapter 205 of Title 18 or the Federal Rules of Criminal Procedure. *See Leatherman v. Tarrant Cty. Narcotics Intelligence & Coordination Unit*, 507 U.S. 163, 168 (1993) ("*Expressio unius est exclusio alterius*.") If the Magistrate Judge's decision is correct, Congress was remarkably unclear in both creating hybrid warrants and identifying what procedures and restrictions apply to them. The Magistrate Judge's decision would leave providers (and law enforcement) to wonder which other provisions of Rule 41 apply.

Congress has amended § 2703 in other ways but has not jettisoned Rule 41 or created new forms of legal process in the face of prior jurisdictional challenges. *See* USA PATRIOT ACT, Pub. L. 107–56, § 220; 115 Stat. 272, 291–92 (2001) (codified at 18 U.S.C. § 2703(a), (b)) (giving federal courts in a district where offense under investigation occurred authority to issue a search warrant for electronic records); Foreign Evidence Request Efficiency Act of 2009, Pub. L. 111–79, § 2, 123 Stat. 2086, 2086 (2009) (codified at 18 U.S.C. § 2711(3)(A)) (modifying definition of district court of competent jurisdiction to include courts with jurisdiction over offense being investigated, where service provider is located or electronic records are stored, or

acting on requests for foreign assistance under 18 U.S.C. § 3512). Congress has thus had numerous opportunities to revisit the SCA to create or clarify the scope of the alleged warrants the Magistrate Judge appears to have read into the statute. But it did not. This court should not do so now.

B. Rule 41 Does Not Permit Searches Outside the United States Where the Search at Issue Occurred

Rule 41 warrants "would be a dead letter outside the United States." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990). Rule 41 provides no authority for an extraterritorial search in this case. Fed. R. Crim. P. 41(b)(1). The search in this case, which required Google to locate, gather, and transmit data to the United States to provide to law enforcement, will occur outside the United States. As such, the warrant exceeds the power granted to law enforcement under Rule 41.

1. Rule 41 Does Not Provide For Extraterritorial Searches of Data

Rule 41 generally limits searches to a Court's district, and provides only limited exceptions to the general rule against searches outside a court's judicial district, none of which include searches in a foreign country. The *only* exceptions that specifically allow for searches outside the United States limit those searches to United States property in three places: (1) territories, possessions, or commonwealths, (2) the premises of a U.S. diplomatic or consular mission in a foreign state, or (3) the residence and any land owned or leased by the United States and used by U.S. personnel assigned to a diplomatic or consular mission in a foreign state. Rule 41(b)(5).[3] Rule 41(b)(6) confirms the geographic limits of Rule 41. That subsection addresses the search warrants for data in an unknown location. That section allows a magistrate to issue a search warrant for information located outside the district if "*the district where the media or*

[3] Other subsections address searches that occur outside the Court's judicial district, but no exception expressly or impliedly extends those searches to foreign countries.

information is located has been concealed through technological means." This rule assumes that the information must be in a judicial district, which does not include locations outside the United States. It also demonstrates that Congress has expressly addressed how a magistrate can issue a search warrant for data whose location is unknown. *See also In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (examining extraterritorial applications of Rule 41).

While Rule 41 provides for searches abroad only in extremely limited circumstances, given that the SCA does not provide any independent power, the question here is whether the warrant served on Google authorizes such a search. The Magistrate Judge's opinion did not even consider this and should, therefore, be rejected.

2. The Search Occurs Abroad, Not In the United States

By compelling Google to access servers in a foreign country, collect data, transmit it to the United States, and deliver it to law enforcement—the district court compelled a search that occurs outside the United States. If, rather than using its internal network, Google had commanded an employee located in its data center outside the United States to make a copy of the email account data and then mail it to Google's headquarters in Mountain View, a reasonable person would conclude that the search had occurred outside the United States, even though the disclosure eventually occurred in California. The fact that Google uses a technical means—an interconnected network—to send the data should not change the result. The data is not in the United States. It is collected in a foreign country. It is transmitted to California and then disclosed to law enforcement. The search occurs outside the United States, not in California.

Cases have repeatedly adopted this view, finding that a search occurs where the data is obtained, not where it is viewed. The Magistrate Judge cited to *Kyllo v. United States*, 533 U.S.

27, 33 (2001), for the proposition that a "search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (Dkt. 13 at 23). But *Kyllo* compels a different result here. In *Kyllo*, law enforcement used a thermal imaging device outside of the defendant's home on public property to detect heat inside the home consistent with growing marijuana plants indoors. The Supreme Court held that a search had occurred and was unlawful without a warrant. Even though law enforcement received the information (heat signatures) outside the home in a public street—the information was collected from *inside* the home. If the Supreme Court had applied Magistrate Judge's reasoning, the "disclosure" would have occurred in the public street—and the search would have occurred outside the home. But the Supreme Court came to the opposite conclusion. Here, even though law enforcement will receive information in the United States about a user, the information will be pulled from another location—and the search occurs in the location where the data resided.

The fact that Google's user can still access his or her data from a foreign server when Google copied it and transmitted it to the United States does not change the analysis. Cases have consistently held that intangible property or information can be seized even absent interference with any right of access to the property. *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). And for electronically-stored data, like the emails in question here, copying electronic data effects a seizure of that data from the place where it was stored. *See Microsoft*, 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, 288 (6th Cir. 2010); *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); *Bach*, 310 F.3d at 1065 (search and seizure occurred when Yahoo technicians copied contents of email accounts from Yahoo servers to turn data over to law enforcement authorities), *cert. denied*, 538 U.S. 993 (2003).

Likewise, Rule 41(e)(2)(B) reinforces this view. That subsection states that a search warrant for electronically stored information ("ESI"), of which data subject to the SCA is a subset, is executed and the search occurs when the electronically stored data is seized *or copied*—not when it is later reviewed or disclosed to law enforcement. Given that the SCA itself refers to warrants for ESI, it would be inconsistent to read the SCA as altering this rule to have searches occur when data is reviewed by law enforcement, not when it is obtained or "copied."

By compelling Google to obtain data stored abroad, transmit it to the United States, and produce it in response to a warrant, the Magistrate Judge co-opted Google into exercising a power to search data that law enforcement itself lacks. Providers can indeed assist the government (as provided for by § 2703(g)) when executing warrants. But it is wrong to suggest that such assistance is a trivial thing entirely disconnected from the process of a government search of seizure. Compelling an email provider to locate, seize, and copy its customers' the private emails effects a 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 a governmental action where that individual is acting as an agent of the government); *see also Warshak*, 631 F.3d at 286 (concluding that a Fourth Amendment search is conducted when "government agents compel an ISP to surrender the contents of a subscriber's emails") and *Bach*, 310 F.3d at 286-87 (analyzing whether Yahoo violated defendant's Fourth Amendment during its "search and seizure" of emails in response to a warrant). As here, when the customer's information is stored

outside the United States, executing the warrant requires the technology company to conduct, at the Government's behest, a search and seizure in foreign territory. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 755 (rejecting the 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). Rule 41 would not authorize law enforcement to conduct the foreign search requested here. The court should not enforce a warrant to conscript a technology company into doing on the Government's behalf what warrants cannot empower law enforcement agents to do themselves. As such, the Magistrate Judge's order should be rejected.

C. The Magistrate Judge's Analysis Improperly Failed to Consider the Conflict Between Foreign and United States' Law

Regardless of whether this Court accepts the Magistrate Judge's reliance on the SCA or Yahoo's focus on Rule 41, it should consider comity interests when data is collected from a foreign country. If other courts follow the Magistrate Judge's determination that there was no extraterritorial application of law, even when the data was likely stored and collected from a foreign country, they too will bypass comity concerns—even when a provider, like Yahoo, *can identify* the foreign country in which it stores data. This interpretation will cause courts to ignore conflicts between U.S. and foreign law. This Court should, at a minimum, recognize the importance of a comity analysis in situations where a foreign jurisdiction can be identified.

In choosing to consider only where law enforcement would receive the data from Google and finding that there was no extraterritorial application of United States law, the Magistrate Judge acted contrary to the Supreme Court's admonition in *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa,* 482 U.S. 522, 546 (1987) that, "in supervising pretrial proceedings . . . American courts should . . . take care to demonstrate due

respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state." *See also* Fed. R. Civ. P. 44.1 (specifically allowing parties to raise foreign law issues in civil proceedings). "'Comity,' in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protection of its laws." *Hilton v. Guyot*, 159 U.S. 113, 163-64 (1895); *see also* Restatement (Third) of Foreign Relations Law § 101 (1987). Where a foreign user's data is stored abroad, comity should be an essential part of any analysis because the Magistrate Judge's decision will impact the protections provided by another sovereign.

Even if Google has limited information about where, precisely, it stored this user's data, comity should be part of the calculus. Rather than focus solely on where the search occurred, the Magistrate Judge should have considered: (a) the nature of the relationship between the user and the provider—is it a foreign user contracting with a foreign entity? (b) the identity of the data controller—is it a foreign entity or a United States-based one? (c) the location of the underlying alleged criminal conduct—was it inside the United States or outside the United States? The answers to these questions would inform whether it is appropriate to permit a search that occurs outside the United States and whether it is proper to compel a provider to import data into the United States for the sole purpose of responding to a law enforcement demand.

Companies like Yahoo with foreign subsidiaries that control confidential data are subject to numerous foreign laws protecting user data. Interpreting the SCA to avoid analyzing foreign law issues in *all cases*, as the Magistrate Judge did here, not only exacerbates conflicts issues,

but violates Justice Marshall's admonition "that 'an Act of Congress ought never to be construed to violate the law of nations if any other possible construction remains . . . .'" *Lauritzen v. Larsen*, 345 U.S. 571, 578 (1953) (citing *Murray v. The Schooner Charming Betsy*, 6 U.S. 64 (1804)). When these conflicts exist, providers and their employees are at increased risk of criminal sanctions for producing data, particularly where courts demanding production do not consider foreign law. Employing a comity analysis allows courts to ensure that the right balance is struck between the United States law enforcement interests and its treaty obligations especially when ignoring those obligations places U.S. providers in unresolvable conflict of laws situations. The Magistrate Judge should have instead considered the full international ramifications of upholding the warrant, including its impact on providers and their foreign subsidiaries.

III. Conclusion

When faced with questions about a providers' role in executing a Rule 41 warrant obtained under the SCA, Congress acted to excuse the presence of an officer during execution rather than clarify that instrument being enforced was a hybrid, not a Rule 41, warrant. However imperfect it might be, the SCA merely opens the door to allow the government to compel the production of data insofar as a Rule 41 warrant can reach it by its own force. Rather than rewriting § 2703(a) of the SCA, this Court should allow Congress to address, in the first instance, when law enforcement should be able to conscript providers to conduct searches for electronically stored evidence abroad. Rule 41 has repeatedly been modified to address any identified deficiencies, including as recently as last year. And Congress has crafted legislative responses to circumstances like the one law enforcement faces here. Congress, not the courts, should be the one to do so again. If Congress decides to extend law enforcement's power to search and seize data stored overseas, it should do so expressly in an amendment to Rule 41 or the SCA. Accordingly, Yahoo urges the court to reject the Magistrate Judge's ruling.

Respectfully submitted,

Dated: March 10, 2017

GREENBERG TRAURIG, LLP

s/ Brian T. Feeney
Brian T. Feeney (Pa. I.D. No. 78574)
Bradly A. Nankerville (Pa. I.D. No. 313660)
2700 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
Tel: 215.988.7800
feeneyb@gtlaw.com
nankervilleb@gtlaw.com

Jacob A. Sommer (*pro hac vice* pending)
Marc J. Zwillinger (*pro hac vice* pending)
ZWILLGEN PLLC
1900 M St. NW
Washington, D.C. 20036
Tel: 202.296.3585
jake@zwillgen.com
marc@zwillgen.com

Attorneys for Yahoo Inc.