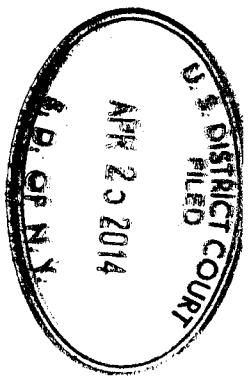
DOC # 97

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation	M9-150 13 Mag. 2814



GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO MICROSOFT'S MOTION TO VACATE EMAIL ACCOUNT WARRANT

PREET BHARARA
United States Attorney for the Southern District of New York
Attorney for the United States of America

LORIN L. REISNER
THOMAS G. A. BROWN
JUSTIN ANDERSON
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Statutes, Rules and Other Authorities:

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation	13 Mag. 2814

Preliminary Statement

The Government respectfully submits this memorandum in opposition to the motion of Microsoft Corporation ("Microsoft") to vacate a sealed warrant directing it to produce stored records under its custody and control, as required by the Stored Communications Act, codified at Title 18, United States Code, Sections 2701-12 (the "SCA"). Microsoft's motion is premised on the misimpression that, because it allegedly has chosen to store certain records overseas, it need not comply with a warrant issued by this Court under the authority of the SCA and in full compliance with the procedures set forth in Rule 41 of the Federal Rules of Criminal Procedure.

In pressing this argument, Microsoft errs on multiple levels. First, nothing in the text or structure of the SCA permits U.S. service providers to avoid compliance with compulsory disclosures mandated by statute simply by storing the data abroad. Second, longstanding precedent requires the production of all records controlled by a party who receives compulsory process in a federal criminal investigation, regardless of where the records are stored physically. Third, Microsoft's attempts to impose limitations on an SCA warrant by analogizing to warrants providing for the search and seizure of physical evidence is misguided, as warrants directing service providers to produce records pursuant to the SCA are fundamentally different from search warrants authorizing law enforcement to enter physical premises and seize evidence. Fourth, Microsoft is wrong to describe a warrant compelling disclosure of records by a U.S. service provider under the SCA as "extraterritorial," as the subject of the warrant is the service

provider, not a physical location abroad. Fifth, policy considerations weigh heavily against Microsoft's position, which serves as a dangerous impediment to the ability of law enforcement to gather evidence of criminal activity. Accordingly, the motion should be denied, and Microsoft should be directed to comply with the warrant.

Statement of Facts

A. The Warrant

On December 4, 2013, this Court issued Warrant No. 13 Mag. 2814 (the "Warrant") pursuant to the SCA. The Warrant directed Microsoft to disclose to the Government certain information within the "possession, custody or control" of Microsoft, including the contents of emails stored in an account (the "Account") and other relevant records that Microsoft controls and maintains.[1] After reviewing its records, Microsoft allegedly determined that the email content for the Account is stored in a so-called "datacenter" in Dublin, Ireland. (Br. 4).[2] According to Microsoft, it stores email content in a foreign datacenter when a subscriber claims to be physically present in an overseas location, but it takes no steps to confirm whether the subscriber is, in fact, logging in from a foreign location.[3] (Br. 3). Even when email data is stored abroad, employees of Microsoft located within the United States can access that data by using a computer program designed exactly for that purpose, which makes the data readily available within the United States. (Br. 4).

---

[1] A copy of the Warrant is attached to this memorandum as Exhibit A.

[2] "Br." refers to Microsoft's memorandum in support of its motion to vacate the Warrant.

[3] Microsoft represents that it began this policy of selectively storing email content outside the United States in September 2010. (Br. 2).

B. Microsoft's United States Contacts

Microsoft is a multi-billion dollar, United States-based company that is incorporated in the State of Washington and has a principal place of business in Redmond, Washington. *See generally*, https://www.microsoft.com/en-us/news/inside_ms.aspx; http://www.microsoft.com/investor/InvestorServices/FAQ/default.aspx. Founded in this country in 1975, it has conducted business here continuously since that time and is publicly traded on the NASDAQ stock exchange in New York City. Microsoft has grown over the years to become one of the world's largest companies, with more than $77 billion in revenue and over 100,000 employees, including 43,000 in Washington State alone. *Id.* Microsoft operates a number of software, hardware, and online business lines, and offers a free email service to the public. (Br. 2). According to the United States Trademark and Patent Office, Microsoft has taken extensive advantage of United States patent protection for its intellectual property, and was the sixth most prolific recipient of U.S. patents in 2012, receiving 2,610 patents in that year alone. *See* http://www.uspto.gov/web/offices/ac/ido/oeip/taf/topo_12.htm.

ARGUMENT

The Warrant Properly Requires Microsoft to Produce All of the Requested Information Within Its Possession, Custody, or Control Regardless of Where It Is Stored

A. Applicable Law

1. The Stored Communications Act

Section 2703 of the SCA, entitled "Required disclosure of customer communications or records," compels service providers to produce certain records to the Government upon receipt of an appropriate demand. That section empowers the Government to use three mechanisms—subpoena, court order, and warrant—to "require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication," such as

electronically stored emails. 18 U.S.C. § 2703. The types of records a service provider must produce under this provision will depend on which instrument law enforcement agents utilize.

If the Government proceeds by subpoena, a service provider must produce only the following categories of information:

> (1) basic subscriber and transactional information related to a subscriber or customer of the provider, such as the subscriber's or customer's name, address, Internet Protocol connection records,[4] and means of payment for the account, 18 U.S.C. § 2703(c)(1)(A) and (2);
>
> (2) retrieved communications and other files stored with the provider (*e.g.*, opened emails, regardless of how old they are), 18 U.S.C. §§ 2703(b)(1)(B)(i) and (b)(2); and
>
> (3) unretrieved communications stored with the provider (*e.g.*, unopened emails) that are *more than* 180 days old, 18 U.S.C. § 2703(a).

These materials must be produced to the Government upon receipt of an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. §§ 2703(b)(1)(B)(i) and (c)(2). Such subpoenas may be issued pursuant to the otherwise applicable standards for compulsory production, and the SCA does not impose any further showing of probable cause or reasonable suspicion for their issuance.

Where the Government obtains a court order pursuant to Section 2703(d) (a "2703(d) Order"), a service provider must disclose the following:

> (1) all records subject to production under a subpoena; and
>
> (2) an additional category of information, defined as "record[s] or other information pertaining to a subscriber to or customer of [the provider] (not including the contents of communications)," such as historical logs showing the email addresses with which a subscriber has corresponded, 18 U.S.C. § 2703(c)(1).

---

[4] Internet Protocol ("IP") addresses are unique numeric addresses assigned to computers that use the Internet. Online providers like Microsoft routinely capture and log the IP addresses of the computers that access email accounts that they maintain and produce these logs to the Government pursuant to court process like SCA warrants.

A 2703(d) Order may be issued only when the Government provides a court with "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication [*e.g.*, emails], or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Finally, if the Government seeks a warrant (an "SCA Warrant"), it may compel a service provider to produce the following records:

> (1) all records subject to production under a 2703(d) order (and therefore a subpoena); and
>
> (2) an additional category of information: unretrieved communications (*e.g.*, unopened emails) stored with a provider for *fewer than* 180 days, 18 U.S.C. § 2703(a).

To obtain an SCA Warrant, the Government must make a showing of probable cause to a court of competent jurisdiction, "using the *procedures* described in the Federal Rules of Criminal Procedure or, in the case of a State court, . . . State warrant *procedures*." 18 U.S.C. 2703(a) and (b) (parenthesis omitted) (emphasis added); *see* Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants).

Under the SCA, a court is empowered to grant an application for a 2703(d) Order or an SCA Warrant if it "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

2. The Fourth Amendment's Warrant Clause

The Fourth Amendment to the United States Constitution protects individuals against "unreasonable searches and seizures." U.S. Const. amend. IV. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia School Dist. 47J* v. *Acton*, 515 U.S. 646, 652 (1995). The Supreme Court has held that, to be reasonable, the Fourth Amendment "normally" requires that "searches

of private property be performed pursuant to a search warrant issued in compliance with the Warrant Clause." *Arkansas* v. *Sanders*, 442 U.S. 753,758 (1979). There are numerous exceptions to the warrant requirement, including its inapplicability to overseas searches, even when a United States citizen has a reasonable expectation of privacy in the area searched. Where the Government seeks to search such a location, no warrant is required, as "foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness." *United States* v. *Odeh*, 552 F.3d 157, 171 (2d Cir. 2008).

B. Discussion

1. Neither the Text nor the Structure of the SCA Limits the Scope of Compelled Disclosure by a U.S. Service Provider to Records Maintained Within the United States

Microsoft argues that it is not required to produce the records demanded by the Warrant solely because it has chosen to store those records abroad.[5] (Br. 1). This argument finds no support in the text or structure of the SCA, pursuant to which the Government may "require the disclosure" of electronic records by a service provider. 18 U.S.C. § 2703. The SCA does not contain a "safe harbor" for records stored overseas, much less a provision limiting a court's authority to issue an SCA Warrant to records maintained in a particular physical location. To the contrary, the SCA confers broad authority on courts to issue 2703(d) Orders and SCA Warrants where a court has "jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The location of the records is simply irrelevant under the SCA, which empowers courts to compel *service providers* in the United States to produce records—upon subpoena, order, or

[5] Microsoft does not allege that (i) it is not subject to the Court's jurisdiction, (ii) the Warrant is defective under the SCA, (iii) the Warrant was not issued in full conformity with the procedures of Rule 41 of the Federal Rules of Criminal Procedure, or (iv) the Warrant suffers from any other infirmity. Nor does Microsoft cite any case, statute, or rule permitting it to move to vacate a search warrant. The SCA certainly does not include such a provision.

warrant—when the Government has made the requisite showing. As the service provider itself—not the storage location of the records—is the subject of a 2703(d) Order and SCA Warrant, Microsoft's concern with the physical location of its records is wholly misplaced.

Microsoft concedes as much, recognizing that if it had received a subpoena seeking information required to be disclosed under the SCA but stored abroad, it would have had no choice but to "produc[e] . . . evidence located outside the United States." (Br. 8-9). Under Microsoft's reading of the SCA, it can properly be compelled to produce records stored abroad upon receipt of an administrative or grand jury subpoena—which is not issued by a neutral, impartial magistrate and requires no showing of reasonable suspicion or probable cause—but need not produce the same records if the demand arrives in the form of a court-authorized order or warrant issued upon the requisite showing. That result runs directly counter to common sense, established precedent (*see infra* at 9-12), and the structure of the SCA, which does not differentiate between the geographic reach of the various methods of disclosure.

Indeed, Section 2703 expressly contemplates the use of a grand jury or trial subpoena to compel the production of certain stored email content (*i.e.*, opened emails and any unopened emails stored more than 180 days) and other electronic records. 18 U.S.C. § 2703(a), (b). Had Microsoft received such a subpoena, it would have had to produce records for the Account regardless of whether they were stored here or abroad. It cannot be that Congress intended that a subpoena can properly require a service provider to produce emails regardless of where they are stored, but a 2703(d) Order or SCA Warrant—issued pursuant to higher standards and court approval—imposes more limited obligations on a U.S. service provider. Microsoft presents no argument rooted in the text or structure of the SCA that supports such a muddled reading of the statute. Indeed, there is no good reason to believe that the compelled disclosure of email content

and other electronic records by a U.S. service provider pursuant to an order or warrant, issued by a court upon a finding of reasonable suspicion or probable cause, results in a narrower reach than a subpoena directed to the same type of information. But that is the position Microsoft urges this Court to adopt.[6]

Microsoft's arguments also conflict with the SCA's general principle that information available through less rigorous legal process is also available through more demanding process. That is, a 2703(d) Order can be used to obtain every category of information available by a subpoena (plus more), and an SCA Warrant can be used to obtain everything available with a 2703(d) Order and subpoena (plus more). *See* J. Carr & P. Bellia, Law of Electronic Surveillance § 4:80 ("One feature of [the SCA] is that through use of greater legal process officials can gain access to any information that they could obtain with lesser process."); Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to amending It, 72 Geo. Wash. L. Rev. 1208, 1222 (2004) ("The rules for compelled disclosure operate like an upside-down pyramid. Because the SCA's rules allow greater process to include the lesser, different levels of process can compel different groups of information. The higher up the pyramid you go, the more information the government can obtain."). Microsoft's interpretation of the SCA as providing a broader reach for subpoenas than SCA Warrants is entirely inconsistent with the structure of the SCA.

---

[6] The absurdity of Microsoft's position is compounded when considered in the context of trial subpoenas issued by courts. *See, e.g., In re Grand Jury Subpoena Duces Tecum*, 767 F.2d 26, 28 (2d Cir. 1985) (recognizing court's power to issue trial subpoenas). Microsoft must concede that a court has the authority to issue trial subpoenas under the SCA, and such subpoenas extend to all materials within the recipient's possession, custody, or control. Under Microsoft's theory, it must comply with a court-issued subpoena for records that are stored overseas, but it need not comply with a court-issued warrant seeking the exact same materials, even though the warrant is issued on a higher showing of cause. Such an arbitrary restriction on the power of courts to compel the production of records finds no basis in law or logic.

2. A Court May Order the Production of Records Within an Entity's Custody or Control Regardless of Where the Records Are Stored

Microsoft's efforts to impose a geographical limitation on what it can be ordered to produce under the SCA is inconsistent with longstanding principles applicable to the production of records by U.S. persons in response to a subpoena or other compulsory demand for information in connection with a federal criminal investigation. Addressing this very point, the Second Circuit has held that when an investigative demand compels the production of records, a witness may not "resist the production of documents on the ground that the documents are located abroad." *In re Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983). Under that precedent, "[t]he test for the production of documents is control, not location." *Id.* Where the recipient of compulsory process is within the court's personal jurisdiction, electronic records and other requested material within a recipient's possession, custody, or control, must be produced, regardless of where they are kept.[7] *See, e.g., In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (requiring Canadian bank with branches in the United States to produce documents in Bahamas pursuant to grand jury subpoena); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544 (S.D.N.Y. 2002) (Chin, J.) (grand jury subpoena for records stored in foreign country enforceable); *United States* v. *Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080 (S.D.N.Y. 1984) (IRS summons properly used to compel American bank to disclose documents held by a branch in Hong Kong).

This requirement is enforced strictly, as recipients of compulsory process can be required to produce foreign-stored material even if doing so might violate the laws of the country where

---

[7] Here, Microsoft does not contest that it is subject to the jurisdiction of this Court, nor could it in light of its substantial contacts to the United States generally and the Southern District of New York in particular.

the information resides. *See, e.g.*, *In re Marc Rich & Co., A.G.*, 707 F.2d at 665 (production ordered despite claim that it would violate Swiss law); *Bank of Nova Scotia*, 740 F.2d at 831 (production ordered despite Bahamian bank secrecy laws); *United States* v. *Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981) (possible criminal penalties under Swiss law did not preclude enforcement of order to produce documents); *Grand Jury Subpoena*, 218 F. Supp. 2d at 564 (subpoena enforced even if production prohibited by foreign laws); *Chase Manhattan Bank, N.A.*, 584 F. Supp. at 1086-87 (Hong Kong bank secrecy orders did not prevent production); *cf. Linde* v. *Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (observing that "the operation of foreign law does not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that law." (internal quotation marks and brackets omitted)).

The compelled disclosure provisions set forth in Section 2703 of the SCA do not alter the settled rule that a party located in the United States properly served with a compulsory demand for information as part of a federal criminal investigation is required to produce all responsive records within that party's possession, custody or control, regardless of where those records are located. Under the plain terms of the statute, the Government "may require the disclosure" by a U.S. service provider of emails and other records upon service of a subpoena, 2703(d) Order, or SCA Warrant. 18 U.S.C. § 2703. And, under longstanding Circuit precedent, the scope of record production is determined by "control, not location." *In re Marc Rich & Co., A.G.*, 707 F.2d at 667. Microsoft offers no reason, much less a good one, to believe that the drafters of the SCA intended to abrogate longstanding precedent by exempting U.S. service providers from producing otherwise responsive records when they are stored abroad. Even more anomalous—and therefore even less defensible—is Microsoft's view that the drafters exempted orders and

warrants, but not subpoenas, from the unambiguous rule that compulsory process requires record production based on control, not location. Microsoft has presented this Court with no valid reason to discard Second Circuit precedent on the scope of compulsory process, which is fatal to its construction of the statute.

That an SCA Warrant is named "warrant" rather than "subpoena" or "order" does not alter this analysis, as the instrument's effect is to compel the recipient to produce records to the Government. *See United States* v. *Jones*, 415 F.3d 256, 262 (2d Cir. 2005) (instructing courts in another context to look to "substance" rather than "label[s]"). In fact, the service of an SCA Warrant is indistinguishable from the service of other compulsory process: the warrant, order, or subpoena is served on a party who then must gather the responsive material. *See* Ex. A. Also like subpoenas, SCA Warrants instruct service providers to produce certain records, leaving the gathering of responsive documents entirely within the hands of that service provider. *See id.* Underscoring that similarity, service providers are permitted to disclose electronic information to the Government in the same manner as records ordinarily are produced in response to a grand jury or trial subpoena. *See id.*; 18 U.S.C. § 2703(g) ("[T]he presence of an officer . . . for service or execution" of an SCA Warrant is not required.). The mere fact the instrument is named "warrant" does not alter its substance. Indeed, it is clear that the SCA's use of the term warrant and the importation of the "procedures" of the Federal Rules of Criminal Procedure were intended to adopt the "probable cause" standard and the involvement of a court, not to narrow the geographic scope of the disclosures required under Section 2703. *See also infra* at 14.

In addition, the operative portions of the SCA addressing the use of an SCA Warrant (as well as the other available mechanisms) to compel providers to produce stored content and records expressly use the language of compulsory disclosure by a responding person or entity to

describe the activity authorized by that provision. Section 2703(a), for example, repeatedly uses the phrase "[a] governmental entity may require the disclosure by a provider . . . of the contents of [stored communications]," while Sections 2703(b) and (c) both use the phrase "[a] governmental entity may require a provider . . . to disclose [the contents of stored communications or records]." 18 U.S.C. §§ 2703(a), (b) and (c). As a result, an SCA Warrant served by the Government operates functionally like a grand jury, trial, or administrative subpoena, which requires a recipient to search the information under its custody or control and to then produce responsive material.

3. An SCA Warrant Ordering the Production of Stored Records Is Not Subject to the Same Limitations as a Search Warrant Authorizing Entry into Physical Premises in Order to Conduct a Search and Seize Evidence

Having found nothing hospitable in the SCA's text or structure or in precedent construing the scope of compulsory process,[8] Microsoft defends its crabbed view of SCA Warrants by relying on court decisions that do not discuss the scope of the SCA at all, let alone warrants issued under its authority. (Br. 5-6). Instead, these decisions address challenges to overseas searches of physical premises and conclude either that the Fourth Amendment *does not* impose any limitation on the searches, that the searches were reasonable, or both. *See United States* v. *Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (holding that "the Fourth Amendment has no application" to the search of a residence in Mexico that belonged to "a citizen and resident of Mexico with no voluntary attachment to the United States"); *United States* v. *Odeh*, 552 F.3d 157, 171 (2d Cir. 2008) (holding that "the Fourth Amendment's Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness" and that the

---

[8] Not surprisingly, Microsoft largely avoids these matters in its brief.

challenged searches were reasonable);[9] *United States* v. *Williams*, 617 F.2d 1063, 1075, 1087-88 (5th Cir. 1980) (holding that Warrant Clause does not apply to searches in international waters); *United States* v. *Vilar*, No. 05 Cr. 621 (KMK), 2007 WL 1075041, at *51 (S.D.N.Y. Apr. 4, 2007) (rejecting challenge to overseas search after noting that "seven of the nine [Supreme Court] Justices [in *Verdugo-Urquidez*] expressly stated or implicitly agreed that the Warrant Clause did not apply to extraterritorial searches"); *United States* v. *Bin Laden*, 126 F. Supp. 2d 264, 285 (S.D.N.Y. 2000) (rejecting U.S. citizen's challenge to warrantless overseas search because "the search was executed in a reasonable manner").

If anything ties these decisions together, it is their common holding that the Warrant Clause does not limit the Government's ability to gather evidence overseas. Microsoft therefore has it exactly backward when it argues that the Warrant Clause—or any of the decisions it relies on that construe its scope—impose a limitation on SCA Warrants.

Microsoft is equally mistaken to suggest that the substantive limitations on conventional search warrants directed to physical premises, as set forth in Rule 41 of the Federal Rules of Criminal Procedure, have any impact on SCA Warrants. Microsoft observes that under Rule 41(b), conventional search warrants can be issued, except in limited circumstances, only by a court in the district in which the *physical property or person* to be searched is located. (Br. 5-6 (citing *Weinberg* v. *United States*, 126 F.2d 1004 (2d Cir. 1942)). But that restriction does not apply to SCA Warrants, which may be issued without regard to whether the electronic information or material sought is inside or outside the district in which the warrant is obtained. By statute, any court that "has jurisdiction over the offense being investigated" is authorized to

---

[9] The Seventh Circuit has reached the same conclusion. *See United States* v. *Stokes*, 726 F.3d 880, 893 (7th Cir. 2013) ("[T]he Fourth Amendment's warrant requirement, and by extension the strictures of the Warrant Clause, do not apply to extraterritorial searches by U.S. agents.").

issue an SCA Warrant. 18 U.S.C. § 2711(3)(A)(i). Indeed, Congress specifically amended the SCA in 2001 to eliminate reliance on the location of data as the necessary basis for obtaining an SCA warrant. *See* Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56 § 220; *United States* v. *Bansal*, 663 F.3d 634, 662 (3d Cir. 2011); *United States* v. *Berkos*, 543 F.3d 392, 397 n.4 (7th Cir. 2008). As explained in the legislative history accompanying the amendment, this change, which modified the "requirement that the 'warrant' be obtained 'within the district' where the property is located," was intended to "to address the investigative delays caused by the cross-jurisdictional nature of the Internet." H.R. Rep. No. 107-236, pt. 1, at 57 (2001).

While the SCA does incorporate the *procedures* of Rule 41 for obtaining a warrant, which are set forth in subsection (d) of the rule, *see* 18 U.S.C. § 2703(a), nothing in the SCA suggests that the substantive limitations described elsewhere in Rule 41 apply to SCA Warrants. Judge Kaplan recognized that important distinction in *Hubbard* v. *MySpace, Inc.*, noting that "the limitation on federal magistrate judges' territorial authority is substantive and therefore does not apply to § 2703(a), which, the courts reasoned, requires compliance only with *procedural* warrant safeguards." 788 F. Supp. 2d 319, 325 n.18 (S.D.N.Y. 2011) (emphasis added). That the SCA incorporated only Rule 41's procedural requirements for obtaining a warrant is further demonstrated by the manner in which SCA Warrants are served and executed. In contrast to a conventional search warrant directed at physical property, a law enforcement officer need not be present for the service or execution of an SCA Warrant. *Compare* Fed. R. Crim. P. 41(f) and 18 U.S.C. § 3105 *with* 18 U.S.C. § 2703(g).

It is equally unavailing for Microsoft to rely on an unsuccessful 1990 amendment to Rule 41 relating to the issuance of "warrants authorizing searches for property outside of the United

States" in support of its efforts to limit the disclosure obligations of a U.S. service provider under the SCA. (Br. 6). An examination of the Advisory Committee Notes on the proposed amendment undercuts Microsoft's argument, as that amendment did not involve any expansion of the Government's ability to conduct physical searches abroad.[10] Rather, it was proposed in order to provide "clarification as to how a warrant may be obtained when law enforcement officials are required, or find it desirable, to do so." *See* Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules – 1990 Amendments. A clarification along these lines would have been useful in a pre-*Odeh,* pre-*Verdugo-Urquidez* environment where the application of the Warrant Clause to overseas searches of U.S. citizens had not yet been decided and obtaining such a warrant, even if unnecessary, would protect the Government from a Fourth Amendment challenge to an overseas search.

Even less persuasive is Microsoft's argument premised on a letter from a Department of Justice official. (Br. 6 (quoting Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) (the "Raman Letter"))). Microsoft misconstrues this letter, which concerns a proposed amendment to Rule 41 that would authorize nationwide jurisdiction for magistrate judges to issue warrants permitting the Government to remotely search electronically stored information. (Raman Letter at 3). In passing, the letter observes that the amendment does not purport to authorize overseas searches because the "Fourth Amendment does not apply to searches of the property of non-United States persons outside the United States, and the Fourth Amendment's warrant requirement does not apply to searches of United States

---

[10] In fact, the drafters of the amendment recognized that a warrant is not required to conduct a search overseas. *See* Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules – 1990 Amendments.

persons outside the United States." (*Id.* at 4 (internal citations omitted)). It is hard to understand how a fair reading of the Raman Letter supports Microsoft's interpretation of the SCA, particularly since the Raman Letter refers to physical searches executed by law enforcement agents, not SCA Warrants directed to U.S. service providers, and recognized that the Warrant Clause does not require warrants for overseas searches. It has no bearing on whether a U.S. service provider is exempt from disclosing records under the SCA that are within its control but stored abroad.

4. The Warrant Does Not Authorize an "Extraterritorial" Search

The crux of Microsoft's argument is that the SCA Warrant here is tantamount to authorizing law enforcement agents to conduct a search in Ireland. That is simply not so. SCA Warrants, like the Warrant challenged here, are not directed at a physical location and are not physically executed by law enforcement officers. Instead, they are the functional equivalent of a subpoena or other investigative demand served on a service provider, which compels the provider to review its stored records and produce the relevant material, without regard to where it is stored. *See In re Application of the United States*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009) ("in the case of electronic information ... no property is actually taken or seized as that term is used in the Fourth Amendment context"). The SCA expressly acknowledges that warrants under section 2703 do not require "the presence of an officer" for "the service or execution of a search warrant issued in accordance with this chapter." 18 U.S.C. § 2703(g). As Microsoft concedes, in order to comply with the Warrant, its own employee in the United States will use proprietary software to access the Dublin datacenter and retrieve responsive documents to the United States, all without the participation, supervision, or even knowledge of law enforcement agents. (Br. 6-7).

Microsoft contends nevertheless that this amounts to an extraterritorial search because of its own efforts to locate and retrieve records stored abroad. In support of this dubious proposition, Microsoft points to *United States* v. *Gorshkov*, which held that law enforcement's warrantless access of data stored in Russia was not subject to the Fourth Amendment and was reasonable in any event. No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001). (Br. 7). Microsoft also relies on *In re Warrant to Search a Target Computer at Premises Unknown*, in which a judge denied an application to install "data extraction software" on an unidentified computer at an unknown location. No. H-13-234M, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013). (Br. 7). Neither decision has anything to do with Microsoft's application, as there was no request in either case that a service provider take any action—whether domestic or foreign—in response to a warrant seeking the production of records. Accordingly, neither decision supports Microsoft's view that its own actions to comply with a duly-issued instrument compelling the disclosure of records by a U.S. service provider can constitute an overseas "search" by the Government.

To the extent Microsoft addresses SCA Warrants and subpoenas at all, it attempts to distinguish between the two by relying on *United States* v. *Bach*, 310 F.3d 1063 (8th Cir. 2002). (Br. 8). In *Bach*, the Eighth Circuit considered whether it was a violation of the Fourth Amendment's reasonableness requirement to serve by fax a warrant seeking the contents of an email account and then have the warrant executed by the service provider outside the presence of any law enforcement official. *Id.* at 1066-67. The Eighth Circuit rejected that attempt to impose the statutory requirements governing conventional search warrants for physical locations on warrants compelling the production of email records under the SCA. *Id.* at 1068. Microsoft does not discuss the holding of *Bach*, but instead selectively quotes from a footnote of the opinion, in

which the Eighth Circuit observed that it was evaluating the challenged warrant "under the search warrant standard, not under the subpoena standard" because "Congress called them warrants and . . . intended them to be treated as warrants." *Id.* at 1066 n.1. While the Court did not elaborate on its reasoning or the implications of its observation, nothing in that footnote prevented the Eighth Circuit from rejecting the defendant's attempt to impose the substantive requirements associated with conventional search warrants on the equivalent of SCA Warrants, which are expressly exempted from those limitations.[11]

Microsoft's reliance on *Zheng* v. *Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 21, 2009), is similarly misplaced. (Br. 10). In that lawsuit, the plaintiffs claimed to have been persecuted by the Chinese government based on information that a China-based service provider turned over to that government in violation of the privacy protections of the SCA. *Id.* at *2. The district judge rejected the plaintiffs' argument, holding that the privacy protections of the SCA did not govern the exchange of data entirely within Chinese borders. *Id.* at *4. Those facts could not be more dissimilar to the issue presented by Microsoft's motion, which involves (i) compulsory process under the SCA, not the SCA's privacy safeguards; and (ii) the service of compulsory process here in the United States for records that must be produced in the United States, not the transmission of data which occurred entirely within China. Most importantly, the *Zheng* decision says nothing about the power of Congress to compel service

---

[11] This was an academic point to the *Bach* Court, in any event, because the challenged search "passe[d] muster under warrant requirements," which were "more stringent than the subpoena standard." 310 F.3d 1066 n.1. Had the "warrant requirements" not been met in that case, then the Court would have had to the reach the question, which would have been informed by its observations on the compulsory process-like features of such warrants, "including the fact that no warrant was physically 'served,' no persons or premises were searched in the traditional sense, and there was no confrontation between [the service provider's] technicians and [the defendant]." *Id.* at 1067. Accordingly, the *dicta* in *Bach* does little to advance Microsoft's cause, while the holding weighs directly against it.

providers to produce records upon the issuance of a warrant, a court's power to issue such an instrument, or a domestic service provider's ability to avoid compliance with lawful process by storing data abroad. It therefore does little to clarify the relevant issues.

Finally, Microsoft is wrong to rely on *Morrison* v. *Nat'l Austl. Bank Ltd.*, 130 S. Ct. 2869 (2010), for the proposition that the Warrant authorized an extraterritorial search. (Br. 9). Microsoft appears to believe that the mere fact that records are stored abroad renders them beyond the scope of compulsory process. In addition to running again against longstanding precedent holding exactly the opposite, *see In re Marc Rich & Co., A.G.*, 707 F.2d at 667, the argument is not even a faithful application of *Morrison*. Applying *Morrison* to a securities fraud prosecution in *United States* v. *Vilar*, 729 F.3d 62 (2d Cir. 2013), the Second Circuit rejected precisely the type of argument that Microsoft presses here. In *Vilar*, the defendants argued that the fraudulent "purchases and sales of [the relevant securities] were deliberately and carefully structured to occur outside the United States." *Id.* at 78 n.12. That the deals were structured "to evade U.S. law" was of no moment to the Second Circuit, as relevant activity in the United States—including the signing of contracts—was sufficient to bring the transactions within the reach of the securities laws. *Id.* ("The parties' intention to engage in foreign transactions is entirely irrelevant."). That teaching applies with equal force here. While Microsoft might have structured its affairs in order to place records beyond what it understood to be the reach of U.S. law enforcement, its misunderstanding of the reach of compulsory process does not transform a lawful demand upon a U.S. service provider to produce records into an extraterritorial search.

5. Policy Considerations Weigh Decisively Against Microsoft's Position

Microsoft's position is equally unsound as a matter of policy. Imposing the limitations urged by Microsoft would lead to absurd results and severely undercut criminal investigations

conducted by U.S. law enforcement authorities. Under Microsoft's proposed regime, whether email content is produced would depend entirely on where a service provider chooses to store data. Electronically stored information, like the data sought by the Warrant, can be maintained in any location and moved around the world easily, at any time and for any reason. Under the proposed regime, whether records are produced would depend solely on the service provider's arbitrary decision to store records within the United States or in a foreign country at the time a warrant is served. Providers would need to check the location of stored data each time they receive legal process in a criminal investigation, and it is entirely conceivable that, based on where a service provider decided to store information on a given day due to its own technical requirements, or even its views about whether the Government should have access to the data, it could reject an SCA warrant one day but accept it the next. Moreover, as records are transferred from one datacenter to another, becoming subject to production and then immune, their production would turn on nothing more than the timing of service of a warrant. Congress did not intend the production of records in criminal investigations to turn on mere chance.

Microsoft's position creates a further absurdity because it stores email content overseas based on where its subscribers claim to live. According to Microsoft's own description of its policies, users can determine whether their data will be stored domestically or abroad based on unverified representations the user makes about his country of residence. (Br. 3). A person planning or committing crimes in or affecting the U.S. could easily reduce the risk of detection by providing false information about his place of residence, causing Microsoft to store responsive records outside the United States and beyond law enforcement's ability to obtain the records in a timely manner, if at all.

Such a restriction would have a devastating impact on the Government's ability to conduct criminal investigations. The speed, perceived anonymity and ease of use makes email communications over the Internet a foundational support for a wide variety of criminal behavior, from traditional fraudsters to sophisticated computer hackers and others. Accordingly, just as emails play a significant role in crime, so too are the content and records stored by service providers important information for law enforcement investigations. Under Microsoft's view of the statute, criminals using a U.S. service provider could avoid lawful process to obtain stored content in their accounts simply by representing falsely that they live outside the country. And in addition to the lack of any basis to conclude that Congress intended that they be used to compel disclosure by U.S. service providers, Mutual Legal Assistance Treaties and letters rogatory are slow and cumbersome processes. Reliance on them would greatly diminish, if not entirely preclude, the Government's ability to obtain evidence in a timely manner.

This arbitrariness and delay runs counter to the intent of the SCA, which was designed and amended in 2001 to provide law enforcement with effective tools to conduct investigations through the use of well-established investigative methods and the application of a "probable cause" standard where appropriate. Borrowing that standard was not intended to otherwise limit the territorial reach of the compelled disclosure of electronic records.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny Microsoft's motion and direct it to comply with the Warrant.

Dated: New York, New York
February 14, 2014

Respectfully submitted,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /S/
Lorin L. Reisner
Thomas G. A. Brown
Justin Anderson
Assistant United States Attorneys
Tel.: 212-637-2299/2194/1035

CERTIFICATION OF SERVICE

I hereby certify that a copy of the Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant filed in this matter was served on:

Nancy Kestenbaum, Esq.
Claire Catalano, Esq.
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018
Tel: 212-841-1000
nkestenbaum@cov.com
ccatalano@cov.com

Guy Petrillo, Esq.
Nelson A. Boxer, Esq.
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, New York 10017
Tel: 212-370-0330
gpetrillo@pkbllp.com
nboxer@pkbllp.com

James M. Garland, Esq.
Alexander A. Berengaut
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004
Tel: 202-662-6000
jgarland@cov.com
aberengaut@cov.com

by electronic mail on the 14th day of February 2014

/S/
Thomas G. A. Brown
Assistant U.S. Attorney

EXHIBIT A

UNITED STATES DISTRICT COURT

for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.
✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JCF
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013 4:30 pm

James C. Francis IV
Judge's signature

City and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY
Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT C

Particular Things To Be Seized

I. Information To Be Disclosed By MSN [redacted]:

To the extent that the information described in Attachment A for MSN, [redacted], is within the possession, custody, or control of MSN [redacted], then MSN [redacted] is required to disclose the following information to the Government for each account or identifier listed in Attachment A [redacted] (the "TARGET ACCOUNT") for the period of inception of the account to the present:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files,

and means and sources of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized By The Government

A variety of techniques may be employed to search the seized e-mails for evidence of the specified crimes, including but not limited to keyword searches for various names and terms including the TARGET SUBJECTS, and other search names and terms; and email-by-email review.

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 959, 960, and 963, Title 46, United States Code, Section 70503, and Title 18, United States Code, Section 1956, including, for each account or identifier listed on Attachment A [redacted], information pertaining to the following matters:

a. Any communications:

1. Pertaining to narcotics, narcotics trafficking, importation of narcotics into the United States, money laundering, or the movement or distribution of narcotics proceeds;

2. [redacted];

3. Pertaining to the use of ports or other places of entry to receive or ship narcotics or narcotics proceeds;

4. Related to the physical location of the TARGET SUBJECTS and their co-conspirators;

5. Constituting evidence of who uses the TARGET ACCOUNT, and where they live and work, and where they are using the TARGET ACCOUNT; and

6. Constituting information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.