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<br>M9-150 |

**GOVERNMENT'S BRIEF IN SUPPORT OF THE MAGISTRATE JUDGE'S DECISION TO UPHOLD A WARRANT ORDERING MICROSOFT TO DISCLOSE RECORDS WITHIN ITS CUSTODY AND CONTROL**

PREET BHARARA
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

SERRIN TURNER
JUSTIN ANDERSON
Assistant United States Attorneys
*Of Counsel*

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

***Cases:***

***Statutes, Rules & Other Authorities:***

## PRELIMINARY STATEMENT

Microsoft Corporation, a U.S.-based provider of electronic communications services, resists compliance with a warrant—issued by a U.S. Magistrate Judge upon a showing of probable cause—that ordered it to disclose the contents of a specific email account. Microsoft does not contend that the warrant seeks records beyond its custody or control, that its business activities place it outside the personal jurisdiction of the issuing court, that the warrant failed to comply with the authorizing statute or any applicable procedural rule, or that the magistrate judge who issued the warrant erred in his determination that the records are likely to contain evidence of a crime. Microsoft presents none of those claims, which would at least have a theoretical basis in precedent. Instead, Microsoft contends, without supporting authority, that because it has chosen to store certain business records overseas, it need not comply with a valid court order requiring disclosure of those records.

Microsoft's position was rejected in its entirety when first presented to the Honorable James C. Francis IV. In a well-reasoned decision, following full briefing and oral argument, Judge Francis held that nothing in the text, structure, or legislative history of the Stored Communications Act (the "SCA") indicated that "Congress intended to limit the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas." *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, __ F. Supp. 2d. __, No. 13 Mag. 2814, 2014 WL 1661004, at *11 (S.D.N.Y. Apr. 25, 2014). Quite to the contrary, Judge Francis concluded that warrants issued under the SCA invoke "the basic principle that an entity lawfully obligated to produce information must do so regardless of the location of that information." *Id.* at *5.

Resisting that "basic principle," Microsoft mischaracterizes the nature of warrants authorized by the SCA and draws inapt analogies to search warrants for physical premises. Those

efforts do not withstand scrutiny. Indeed, they are entirely incompatible with the express text of the statute, which orders service providers to disclose records upon receipt of a warrant or other appropriate legal instrument. Nothing in the text or structure of the statute carves out an exception for records stored abroad, and none exists in precedent construing the scope of compulsory process. Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production. The disclosure of records under such circumstances has never been considered tantamount to a physical search under Fourth Amendment principles, and Microsoft is mistaken to argue that the SCA provides for an overseas search here. As there is no overseas search or seizure, Microsoft's reliance on principles of extraterritoriality and comity falls wide of the mark. So does Microsoft's claim that the warrant is insufficiently particular even though it pertains to a specific, clearly identified email account. Even less persuasive are Microsoft's policy-based arguments against this mechanism for obtaining evidence—a mechanism that has been authorized by Congress and is subject to prior judicial review each and every time it is used. Upholding this well-regulated method of obtaining evidence, as Judge Francis did, strikes the right balance between protecting valid privacy interests and promoting effective law enforcement.

## BACKGROUND

Microsoft is a multi-billion-dollar, U.S.-based company, incorporated and headquartered in the State of Washington. *See generally* http://www.microsoft.com/en-us/news/inside_ms.aspx. Founded in this country in 1975, Microsoft 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 annual revenue and over 100,000 employees, including 43,000 in Washington State alone. *Id.* Microsoft operates a number of software, hardware, and web-based business lines, including an

email service that is free to the public. (Br. 5).[1] According to the United States Trademark and Patent Office, Microsoft has taken extensive advantage of U.S. patent protection for its intellectual property, and was the fifth most prolific recipient of U.S. patents in 2013, receiving 2,659 patents that year alone. *See* http://www.uspto.gov/web/offices/ac/ido/oeip/taf/topo_13.htm.

On December 4, 2013, Judge Francis issued a warrant under the SCA (the "Warrant"), directing Microsoft "to disclose" records within its "possession, custody or control" pertaining to a particular email account.[2] After reviewing its records for that account, Microsoft represented that it had chosen for its own business purposes to migrate the account's contents to a Microsoft "datacenter" in Dublin, Ireland. *In re Warrant*, 2014 WL 1661004, at *1. According to Microsoft, it seeks to store a subscriber's emails at the datacenter nearest the subscriber's location, which Microsoft assumes to be the county of residence selected by the subscriber upon registration. *Id.* Microsoft takes no steps, however, to confirm that the subscriber resides in, or is logging in from, the specified country. (Decl. of A.B. dated Dec. 17, 2013 ¶ 5). In any event, all Microsoft account data, whether stored in the United States, the Dublin datacenter, or in any of Microsoft's many other locations located throughout the world, are under the control of and readily available to Microsoft's employees in the United States, who can access the data using a program designed for that very purpose. (Decl. of C.D. dated Dec. 17, 2013 ¶¶ 4-6).

On December 18, 2013, Microsoft moved to vacate the Warrant, and Judge Francis denied that motion on April 25, 2014. Microsoft now challenges Judge Francis's decision.

[1] "Br." refers to Microsoft's brief objecting to Judge Francis's Order; "[Name] Br." refers to the brief filed by the named amicus curiae.

[2] A redacted copy of the Warrant is attached to this brief as Exhibit A.

# ARGUMENT

## POINT I

## The Warrant Properly Requires Microsoft to Disclose Data Under Its Control Regardless of Where Microsoft Has Chosen to Store the Data

### A. Applicable Law

Congress enacted the SCA in 1986, as part of the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99–508, 100 Stat. 1848 (1986). The statute was intended to extend privacy protections to then-nascent forms of telecommunications and computer technology, with the greatest protection—specifically, the requirement that a warrant based on probable cause be issued by a neutral magistrate—reserved for unopened emails held by the provider for fewer than 180 days. *See* H.R. Rep. 99-647 (1986), at 68 (explaining that Congress viewed emails older than 180 days as "back-up copies" that are "closer to a regular business record" entitled to less protection); *see generally* 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, 1209-13 (2004).

Section 2703 of the SCA, entitled "Required disclosure of customer communications or records," empowers the Government to "require the disclosure" of records by electronic communications service providers such as Microsoft. 18 U.S.C. § 2703(a). Depending on the type of records to be disclosed, the Government may proceed by subpoena, order, or warrant.

Using a subpoena, the Government can "require the disclosure" by a service provider of the following categories of information:

(1) basic subscriber and transactional information concerning a user, 18 U.S.C. § 2703(c)(1)(A) and (2);

(2) "received," *i.e.*, opened, emails, regardless of how old they are, 18 U.S.C. §§ 2703(b)(1)(B)(i) and (b)(2); and

(3) unopened emails *more than* 180 days old, 18 U.S.C. § 2703(a).

These materials may be obtained through any "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) & (c)(2). The SCA does not require any prior judicial review, based on either probable cause or reasonable suspicion, for the issuance of such subpoenas.

Where the Government obtains a court order pursuant to 18 U.S.C. § 2703(d) (a "2703(d) order"), the Government may compel a service provider to disclose the following:

(1) all records subject to production under a subpoena; and

(2) any other "record or other information" concerning a user other than "the contents of communications"—such as historical logs of the email addresses in contact with the user, 18 U.S.C. § 2703(c)(1).

A 2703(d) order may be issued where the Government provides a court with "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Finally, if the Government obtains a warrant under the SCA (an "SCA warrant"), it may "require the disclosure" by a service provider of the following records:

(1) all records subject to production under a 2703(d) order (and therefore a subpoena); and

(2) unopened emails stored with a provider for *fewer than* 180 days, 18 U.S.C. § 2703(a).

Thus, with an SCA warrant, the Government can obtain *all* email data in an account. An SCA warrant is "issued using the procedures described in the Federal Rules of Criminal Procedure" and thus requires a sworn affidavit establishing probable cause. 18 U.S.C. 2703(a) & (b) (parenthesis omitted); *see* Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants). Unlike a warrant issued under Rule 41, which must comply with the jurisdictional provisions of Rule 41(b), the SCA has a separate, express jurisdictional provision that empowers any "court of competent jurisdiction" to issue an SCA warrant. 18 U.S.C. § 2703(b)(1)(A). This grant of jurisdiction is broader than the

one in Rule 41, as it authorizes courts with "jurisdiction over the offense being investigated," as well as those with jurisdiction over the physical location of the records and service providers, to issue SCA warrants. 18 U.S.C. § 2711(3).

In short, under the statute, every category of information that the provider must disclose pursuant to a subpoena must be disclosed pursuant to a 2703(d) order (plus more); and every category of information that the provider must disclose pursuant to a 2703(d) order must, in turn, be disclosed pursuant to a warrant (plus more). "The rules for compelled disclosure operate like an upside-down pyramid. . . . The higher up the pyramid you go, the more information the government can obtain." Kerr, *A User's Guide*, at 1222. Notably, the language in the statute requiring disclosure by the provider remains the same regardless of the instrument.

**B. Discussion**

**1. Microsoft's Position Is Contrary to the Text and Structure of the SCA, Which Requires the Disclosure of Records Upon Service of a Warrant**

Microsoft argues that it is not required to produce the records demanded by the Warrant because it has chosen to store those records abroad. (Br. 1). That argument finds no support in the text or structure of the SCA, including its jurisdictional and substantive provisions, which authorize the Government to "require the disclosure" of electronic records by a service provider in the United States upon service of appropriate legal process. 18 U.S.C. § 2703.

Microsoft's argument is inconsistent with the jurisdictional provisions of the SCA. Under the statute, any "court of competent jurisdiction" is authorized to issue an SCA warrant, and such courts include those that have jurisdiction over (i) the offense under investigation, (ii) the physical location of the service provider, or (iii) the storage site of the relevant records. 18 U.S.C. § 2711(3)(A). As applied here, the SCA authorized Judge Francis to compel disclosure of the relevant records because the offense under investigation is subject to the jurisdiction of the Court and Microsoft is located in the United States. Microsoft's arguments, which are based entirely on the

physical location of records, are incompatible with the far broader scope of jurisdiction set forth in the SCA. Contrary to Microsoft's arguments, the SCA does not contain a "safe harbor" exclusion for data that a U.S. company chooses to store overseas, much less a provision limiting a court's authority to order the disclosure of records to those maintained in a particular physical location. Rather, the physical location where records are stored is only one basis under the SCA for a court's jurisdiction.

Equally divorced from the SCA's text and structure is Microsoft's characterization of the SCA warrant at issue here as requiring a physical search. Far from authorizing law enforcement agents "to break down the doors of Microsoft's Dublin facility" (Br. 1), the Warrant simply triggers the statutory obligation of a U.S.-based company to disclose records within its possession and control to law enforcement in the United States. In keeping with the statutory mandate, the Warrant does two things: (1) it "require[s]" Microsoft "to disclose the contents of any wire or electronic communication" under Section 2703, and (2) it authorizes a review of that data by law enforcement agents in the United States after the data has been disclosed. The simple language of the statute, which speaks of "requir[ing] . . . to disclose"—not "break[ing] down doors"—makes plain that its focus is on the production of records, not the entry of law enforcement officers into private physical spaces.

Judge Francis recognized exactly that when he held that the Warrant was "not a conventional warrant" but instead "a hybrid: part search warrant and part subpoena." *In re Warrant*, 2014 WL 1661004, at *5. As Judge Francis correctly observed, an SCA warrant "is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause" but then "is executed like a subpoena in that it is served on the [internet service provider ("ISP")] in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question." *Id.*

While Microsoft might dispute Judge Francis's use of the term "hybrid," it offers no explanation of how statutory text "requir[ing]" an entity "to disclose records" is the equivalent of forced entry into private spaces for the gathering of evidence. (Br. 11-13). That failure demonstrates how far afield Microsoft's position is from the statutory text.

The plain language of the SCA clarifies that Congress intended for SCA warrants to operate as a form of compulsory process, functionally similar to subpoenas. Thus, the SCA specifically uses the language of compulsory process in describing how electronic communications may be obtained by warrant, providing that the Government may use a warrant to "require the disclosure" of communications "by a provider." 18 U.S.C. § 2703(a); see also *In re Warrant*, 2014 WL 1661004, at *2 ("The *obligation* of . . . Microsoft *to disclose* to the Government customer information or records is governed by the [SCA]." (emphasis added)). The SCA uses precisely the same language in describing how electronic communications may be obtained by way of subpoena or 2703(d) order. The statute provides that the Government may "require the disclosure" of electronic communications *either* pursuant to a warrant *or*, for emails older than 180 days, pursuant to a subpoena or 2703(d) order. 18 U.S.C. § 2703(a). The fact that Congress used the same language with respect to these various forms of process reflects that Congress understood that each could be executed in the same way: through a disclosure requirement directed at a service provider, rather than a forced entry onto physical property.[3] *See Drescher* v. *Shatkin*, 280 F.3d 201, 205-06 (2d Cir. 2002) ("[I]t would be needlessly untidy and confusing, absent good reason, to have one term mean two different things in a single statutory scheme.").

[3] All three provisions creating a requirement use nearly identical language. 18 U.S.C. § 2703(a) ("may require the disclosure by a provider"), (b)(1) ("may require a provider . . . to disclose"), (c)(1)(may require a provider . . . to disclose"), (c)(2) (A provider . . . shall disclose").

Other provisions of the statute corroborate that Congress did not intend for an SCA to warrant operate like a physical search warrant issued under Rule 41 of the Federal Rules of Criminal Procedure. Whereas a law enforcement officer must be present during execution of a physical search warrant and inventory the seized property, the SCA specifically provides that a law enforcement officer need not be present at all for service or execution of an SCA warrant. *Compare* Fed. R. Crim. P. 41(f)(1)(B) *and* 18 U.S.C. § 3105 *with* 18 U.S.C. § 2703(g) ("the presence of an officer shall not be required for service or execution of [an SCA] warrant"). In fact, SCA warrants are most often served in the same manner as subpoenas—by faxing or otherwise transmitting them to the provider, who then must gather the material required to be disclosed. And, again, whereas a physical search warrant can be obtained only in the district where the property to be searched is located, *see* Fed. R. Crim. P. 41(b)(1), an SCA warrant can be obtained from any court that "has jurisdiction over the offense," 18 U.S.C. § 2711(3), just as a federal criminal subpoena may be issued out of the investigating district and served anywhere the recipient is subject to service, *see* Fed. R. Crim. P. 17(e).

Furthermore, nothing in the legislative history of the SCA indicates that Congress intended to artificially impose "territorial" limits on warrants issued under the statute. Misreading the legislative history, Microsoft points to a 2001 amendment allowing SCA warrants to be served "nationwide," which it argues "confirms that [SCA] warrants . . . are limited to the territory of the United States." (Br. 18 (citing Pub. L. 107-56 § 220, 115 Stat. 272 (2001))). The amendment, however, merely provides that SCA warrants may be *served* nationwide; it says nothing about the locations where a provider must subsequently collect responsive records. And even as to service, the 2001 amendment was not intended to limit the reach of SCA warrants, but rather was intended to expand it, by permitting an SCA warrant to be served anywhere in the nation as opposed to only in the district where the warrant was issued. *See* H.R. Rep. No. 107-236, pt. 1, at 57 (2001)

(explaining that the amendment eliminated the "requirement that the 'warrant' be obtained 'within the district' where the property is located," in order to "address the investigative delays caused by the cross-jurisdictional nature of the Internet"). If anything, the amendment shows that Congress sought to allow the Government to obtain SCA warrants free from jurisdictional obstacles that affect physical search warrants.[4]

The label of the method of compelled disclosure—"warrant," "order," or "subpoena"—should not impact the scope of the obligation to disclose records under the SCA. That is why Judge Francis was right to dismiss Microsoft's over-reliance on the term "warrant" as excessively "simple, perhaps deceptively so." *In re Warrant*, 2014 WL 1661004, at *3. The issue is the nature of the governmental power being exercised, not the way it is labeled. *See Bay Ridge, Inc.* v. *Fed'l Mine Safety & Health Review Comm'n*, 715 F.3d 631, 646 (7th Cir. 2013) ("For purposes of our Fourth Amendment analysis, we look to the substance of [the Government's] power rather than how the Act nominally refers to those powers."). When the Government serves a provider with an SCA warrant, the power being exercised is not a temporary dominion over the provider's private property, as entailed in a physical search warrant. Instead, the Government is exercising a power to compel the provider to produce records in its possession, subject to judicial sanction, as entailed in a subpoena. That is the essence of compulsory process. *See id.* at 645 (holding that, where regulatory agency was not seeking to enter companies' "private offices and search through [their] file cabinets

[4] Another inaccurate citation to legislative history is found in one of the *amicus* briefs, which cites a comment in a legislative report accompanying the SCA for the proposition that the SCA was "intended to apply only to access within the territorial United States." (AT&T Br. 5 (quoting H.R. Rep. 99-647, at 32-33 (1986))). Context makes clear that the quoted comment refers only to the territorial scope of a criminal prohibition contained in 18 U.S.C. § 2701, which makes it a crime to "intentionally access[] without authorization a facility through which an electronic communication service is provided." *See* H.R. Rep. 99-647, at 32 (discussing the "legislation of penalties" in the SCA). The comment has nothing to do with the scope of compelled disclosure authorized under Section 2703.

and computer files" but instead was seeking "only to require the [companies] to provide certain documents," that agency's demands were more properly considered "subpoenas rather than physical searches carried out by government agents").

This logical construction of the statute, which takes into account the text and structure of the SCA, gives full meaning to Congress's use of the term "warrant." The distinction Congress drew in the statute between warrants, orders, and subpoenas does not concern how these different forms of process are executed. Rather, the distinction concerns the requirements that must be met before they are issued. For records subject to disclosure under the statute that Congress deemed most sensitive—unopened emails less than 180 days' old—the SCA requires the Government to obtain a warrant "*issued using the procedures* described in the Federal Rules of Criminal Procedure." 18 U.S.C. § 2703(a) (emphasis added). Unlike a subpoena or 2703(d) order, a warrant may issue only upon a finding of probable cause by a magistrate judge, based on a sworn affidavit of a law enforcement agent. *See* Fed. R. Crim. P. 41(d)(1). Congress thus sought to incorporate the *same form of prior judicial review* required for a physical search warrant, based on the heightened privacy interests it believed were implicated by emails in electronic storage for less than 180 days.

The purpose of this requirement, therefore, was to extend the safeguards of the probable cause standard and prior approval by a neutral judge to unopened emails less than 180 days' old, which Congress deemed worthy of special protections. But Congress did not mean to transplant every other feature of physical search warrants—in particular, their mode of execution—into the novel context of electronic communications stored by a provider. *See United States* v. *Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) ("Section 2703(a) refers only to the specific provisions of the Rules of Criminal Procedure, namely, Rule 41, that detail the *procedures* for obtaining and issuing warrants."); *cf. United States* v. *Abu-Jihaad*, 630 F.3d 102, 121-22 (2d Cir. 2010) ("[T]he Constitution's warrant requirement is 'flexible,' so that 'different standards may be compatible with

the Fourth Amendment in light of the different purposes and practical considerations' at issue."). As Judge Francis held, the SCA's protections did not "alter the basic principle that an entity lawfully obligated to produce information must do so regardless of the location of that information." *In re Warrant*, 2014 WL 1661004, at *5. The imposition of a warrant requirement here has nothing to do with the physical location of the relevant records, and Microsoft has identified no authority whatsoever suggesting that it does.

**2. Under Longstanding Precedent, Courts May Order the Domestic Disclosure of Records Regardless of Where They Are Stored**

As a form of compulsory process that requires Microsoft to disclose records, the scope of the Warrant is not limited by the physical location of those records. Under binding Second Circuit precedent, the production of records compelled by legal process, in connection with a federal criminal investigation, may not be "resist[ed] . . . on the ground that the documents are located abroad." *In re Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983). Rather, "[t]he test for the production of documents is control, not location." *Id.*; *see also, e.g., In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (requiring Canadian bank with U.S. branches to produce documents stored in Bahamas); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544 (S.D.N.Y. 2002) (Chin, J.) (enforcing grand jury subpoena for records stored in foreign country); *United States* v. *Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080 (S.D.N.Y. 1984) (IRS summons properly used to compel U.S. bank to disclose documents held by branch in Hong Kong).

Under the line of cases establishing what has come to be known as the *Bank of Nova Scotia* ("*BNS*") doctrine, recipients of compulsory process may even be ordered to produce foreign-stored

material where doing so would violate the laws of the country where the information resides.[5] Courts in such situations may at times apply a balancing test weighing the competing national interests at stake, but they generally find the interest in enforcing U.S. criminal law paramount. *See, e.g.*, *Bank of Nova Scotia*, 740 F.2d at 831 (production ordered despite Bahamian bank secrecy laws); *In re Marc Rich & Co., A.G.*, 707 F.2d at 665 (production ordered despite claim that it would violate Swiss law); *United States* v. *Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981) (production ordered despite possible criminal penalties under Swiss law); *Grand Jury Subpoena*, 218 F. Supp. 2d at 564 (production ordered even though prohibited by foreign laws); *Chase Manhattan Bank, N.A.*, 584 F. Supp. at 1086-87 (production ordered despite Hong Kong bank secrecy orders); *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" (quotation marks and internal citation omitted)).

Microsoft contests this principle by taking the Warrant's requirement that records be disclosed and mischaracterizing it as a "search" of the Dublin datacenter. From that flawed premise,

[5] Without citation to any authority or presentation of any analysis, Microsoft asserts in a footnote that it is an "open question whether the *BNS* doctrine remains good law" following the Supreme Court's decision in *Morrison* v. *Nat'l Austl. Bank Ltd.*, 561 U.S. 247 (2010). (Br. 25 n.15). The Government is unaware of any decision so holding, and even if there were an "open question" about the validity of Second Circuit precedent, that question should be resolved by that Court in the first instance. *See Agostini* v. *Felton*, 521 U.S. 203, 237 (1997) ("[I]f a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions."). In any event, there is no such question here—open or otherwise—as *Morrison* does not purport to overrule the *BNS* doctrine, nor does it conflict with the SCA. In *Morrison*, the Court limited the statutory reach of securities fraud suits to those involving domestic transactions. That holding has nothing to do with the SCA, which enables U.S. law enforcement to obtain records from domestic service providers in connection with violations of U.S. laws.

Microsoft argues that because the Government could not "undertake . . . a foreign search and seizure *directly*," it should not be allowed to conduct the search and seizure "*indirectly* by conscripting Microsoft to act in its stead." (Br. 21 (emphasis in original)). But the Government does not seek to enter the Dublin datacenter and has neither sought nor obtained authorization from a magistrate judge to do so. Instead, the Government has obtained a court-ordered instrument directing Microsoft to disclose records under the authority of a statute that expressly allows the Government to "require the disclosure" of data by service providers. While Microsoft submits that compelled disclosure of records is prohibited when forcible seizure is unavailable, that argument is foreclosed by the *BNS* doctrine, which expressly authorizes the Government to obtain through compulsory process records stored abroad, even though no U.S. court could authorize entry into the location where the records are stored so that they could be seized directly. Under that established precedent, the Government's inability to obtain a warrant to enter overseas premises has no bearing on the Government's ability to use other means to compel disclosure of records stored overseas.[6]

Far from being "conscripted" to execute a physical search as the Government's agent (Br. 25-26), Microsoft is simply required to collect and produce its own records, similar to any subpoena recipient. "Whether a private party should be deemed an agent or instrument of the Government for

[6] This is not to argue that SCA warrants "involve no constitutional 'search' at all." (Br. 15). An SCA warrant authorizes the Government to review the contents of electronic communications produced by a provider in response to the warrant. An SCA warrant—issued by a neutral magistrate based upon a showing of probable cause—satisfies any Fourth Amendment prerequisites for disclosure and review. As to the required disclosure of records, that compelled disclosure is no more in conflict with the Fourth Amendment than it would be if the communications were sought by subpoena or court order, as the conduct is neither carried out nor controlled by law enforcement. *See Oklahoma Press Pub. Co.* v. *Walling*, 327 U.S. 186, 195 (1946) (holding that subpoenas *duces tecum* presented "no question of actual search and seizure" where "[n]o officer or other person has sought to enter petitioners' premises against their will, to search them, or to seize or examine their books, records or papers"). An SCA warrant simply requires the provider to disclose records to law enforcement, while imposing no obligation on the provider to review the materials for criminal evidence.

Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *Skinner* v. *Ry. Lab. Execs. Ass'n*, 489 U.S. 602, 614 (1989) (internal quotation marks omitted). A corporation's gathering and production of records in response to compulsory process has never been considered the equivalent of a physical search by government agents as contemplated by the Fourth Amendment,[7] and there is no basis to conclude differently here. No law enforcement officer would even be present during Microsoft's collection of the records to be produced. As Microsoft concedes, in complying with the Warrant, its own employee in the United States will use proprietary software to access a Microsoft datacenter and retrieve the requested records electronically, all without the participation, supervision, or even contemporaneous knowledge of law enforcement agents. (Br. 6-7).[8]

[7] The Fourth Amendment imposes only a reasonableness requirement on compulsory process: the requirement to disclose information cannot be too indefinite, too broad, or too burdensome. *See Oklahoma Press Pub. Co.*, 327 U.S. at 208.

[8] Relying on authority addressing computer searches conducted directly by law enforcement personnel, Microsoft contends that "in the context of electronic data, the 'place to be searched' is the physical location where the data is stored." (Br. 16 (citing *United States* v. *Gorshkov*, No. 00 Cr. 550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001); *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013))). As Judge Francis recognized, those decisions do not support Microsoft's position because the Government is not seeking authority to itself log into or otherwise maintain a presence on the overseas computers where the data resides. *In re Warrant*, 2014 WL 1661004, at *10. Microsoft likewise errs in arguing that "[w]arrants for remotely stored electronic data also involve the *seizure* of that data at the place where it is stored." (Br. 16 n.10). The mere gathering of data by a provider in anticipation of disclosing it to law enforcement is not a "seizure." *See In re Application of the United States*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009) ("[I]n the case of electronic information . . . no property is actually taken or seized as that term is used in the Fourth Amendment context."). Until the data is actually produced to law enforcement agents, it has not even entered the Government's possession, let alone been "seized" within the meaning of the Fourth Amendment. *United States* v. *Jacobsen*, 466 U.S. 109, 113 (1984) (holding that a "'seizure' of property only occurs when there is some meaningful interference with an individual's possessory interests in that property").

There is no reason to believe that the drafters of the SCA intended to abrogate longstanding precedent holding that that a recipient of compulsory process in a federal criminal investigation may validly be compelled to produce any documents under its control regardless of location. Not only is Congress presumed to know the state of federal law against which it legislates, *see Cannon* v. *Univ. of Chicago*, 441 U.S. 677, 696-97 (1979), but the SCA expressly contemplates the use of a subpoena to compel the disclosure of opened emails, any unopened emails older than 180 days, and other electronic records. Under established law, Microsoft could not properly refuse to comply with such a subpoena based simply on the foreign location of the responsive records. Yet, on its reading of the statute, if the same records are sought through an SCA warrant—issued pursuant to higher standards and court approval—the records are off limits to the Government. Not only does this muddled reading of the statute run counter to common sense, it also conflicts with the SCA's general principle that any information available under the statute through less rigorous legal process is also available through more demanding process. *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.").

Microsoft objects that applying the *BNS* doctrine to SCA warrants would "vitiate an integral part of the *BNS* doctrine: the opportunity for *ex ante* review on comity grounds." (Br. 24-25). Microsoft's argument is ironic given the very existence of this litigation, as Microsoft itself is now seeking "*ex ante* review" of the Warrant by challenging it pre-compliance.[9] Moreover, to challenge compulsory process on comity grounds, Microsoft must first establish that the production of records

[9] Microsoft fails to cite any case, statute, or rule permitting it to move to vacate an SCA warrant. The SCA certainly does not include such a provision. A service provider directed to assist with a warrant may challenge the assistance order under the Due Process Clause, including where providing the assistance would impose an undue burden on the provider. *Cf. United States* v. *New York Tel. Co.*, 434 U.S. 159, 171-72 (1977); *In re Application*, 610 F.2d 1148, 1156-57 (3d Cir. 1979). However, Microsoft has made no Due Process argument here.

"would violate the law of the state in which the documents are located" and then persuade a court that the records should not be produced in light of the competing interests at stake. *See, e.g.*, *United States* v. *Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985). Insofar as there might be any non-speculative comity concerns raised by the Warrant (although none are apparent), Microsoft has been free to raise them during the course of this litigation. To date, Microsoft has not claimed that Irish law bars Microsoft from complying with the Warrant.[10] With no conflict of law argued or identified, Microsoft's concern for comity is more rhetorical than real.

Microsoft further errs by arguing that "*ex ante* review is possible for subpoenas issued under [the SCA], because . . . subpoenas are generally accompanied by notice to the subscriber," but "[i]f the Government seizes data using a *warrant*, . . . the Government is not required to notify the user, and the user, in turn, is unable to challenge the seizure *ex ante* on comity grounds." (Br. 25 (emphasis in original)). But the user would not be the appropriate party to raise a comity challenge to an SCA warrant ordering the compelled disclosure of records. Any such objection would belong to the service provider, not the user, because the basis for the objection would be the competing legal obligations imposed on the party being compelled to act—that is, the service provider. Even if the user were notified of the warrant, the user would not be in any position to know whether the SCA warrant implicated competing legal obligations on the provider, and would not have standing to raise this objection in any event, since the provider, not the user, would be the one facing

[10] While Microsoft has submitted an affidavit from an Irish attorney, the affidavit is more illuminating with regard to what it does not say than for what it does. The declaration does not opine that Irish law would subject Microsoft to either criminal or civil penalties were it to comply with the Warrant. Instead, the declaration notes that disclosures may be made under "certain particular exceptions" without opining that none of the exceptions are applicable in the case at hand.

potential legal ramifications in the foreign country. *See Davis*, 767 F.2d at 1033 (rejecting bank customer's attempt to object on comity grounds to trial subpoena issued to bank).[11]

### 3. The Warrant Does Not Authorize an Extraterritorial Search, Much Less Present a Violation of the Law of Nations

Finding no support for its position in the text, structure, or legislative history of the SCA, or in precedent construing the scope of compulsory process, Microsoft strays from the statute itself and attempts to ground its position in two principles of statutory construction concerned with avoiding harm to international relations—the presumption against extraterritoriality and the *Charming Betsy* canon. Neither has anything to do with this case.

The presumption against extraterritoriality assumes that Congress "ordinarily legislates with respect to domestic, not foreign matters," and therefore that "legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Morrison* v. *Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010). The presumption does not apply here because the SCA warrant at issue does not involve any "extraterritorial application" of U.S. law. Instead, as Judge Francis held, the law is being applied exclusively within the United States—to a domestic provider served within U.S. territory and subject to the personal jurisdiction of the issuing court. *See In re Warrant*, 2014 WL 1661004, at *9. An SCA warrant does not criminalize or regulate any conduct in a foreign country; it merely compels the provider receiving the warrant to disclose responsive records within its control to law enforcement agents located in the United States.

[11] Microsoft's argument also ignores that, under the SCA, a subpoena need not be accompanied by notice to the user, as the statute allows the Government to delay any governmental notice required and to preclude any notice by the provider, based on a showing that notice would adversely affect or seriously jeopardize the Government's investigation, *see* 18 U.S.C. § 2705(a), (b), as will often be the case with a criminal inquiry.

The fact that a provider may need to retrieve records from abroad in order to do so, due to the provider's own record-keeping practices, does not render the SCA "extraterritorial." By comparison, the fact that a corporation may need to move funds from a foreign bank account into the United States in order to pay its taxes, due to the corporation's own banking practices, does not render the tax laws "extraterritorial." The principle against extraterritoriality presumes that Congress does not intend for a law to *apply* extraterritorially. It does not presume Congress's intention to be that the law has no incidental effects outside the country whatsoever. *See Envtl. Def. Fund.* v. *Massey*, 986 F.2d 528, 531-32 (D.C. Cir. 1993) ("Even where the significant effects of the regulated conduct are felt outside U.S. borders, the statute itself does not present a problem of extraterritoriality, so long as the conduct which Congress seeks to regulate occurs largely within the United States.").[12]

In an effort to support its position, Microsoft relies on authority addressing challenges to overseas searches of physical premises. (Br. 17). But these decisions have nothing to do with the required disclosure of records. Instead, they stand for the far different proposition that the Fourth Amendment's Warrant Clause does not apply at all to extraterritorial searches of physical property, and therefore that a warrant is *not required* for such searches. *See 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"); *United States* v. *Vilar*,

[12] Microsoft cites *Zheng* v. *Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009), as a case "applying the presumption against territoriality" to the SCA (Br. 19), but *Zheng* has nothing to do with Section 2703. The case instead concerns a private lawsuit brought by a set of plaintiffs over disclosures of their communications made by a provider in China to the Chinese Government, which the plaintiffs alleged were in violation of Section 2702, a provision of the SCA prohibiting a provider from making unauthorized disclosures of user data. Thus, the lawsuit involved extending a regulatory prohibition to conduct occurring wholly outside the United States—a fact pattern far removed from the one at issue here.

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 Warrant Clause does not apply to extraterritorial searches); *United States* v. *Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000) (holding that the warrant requirement does not apply to foreign-intelligence activities conducted abroad). Microsoft thus has it exactly backward in suggesting that the Warrant Clause—or any of the cases it relies on that construe its scope—imposes a limitation on the Government's ability to conduct an extraterritorial search, much less compel the disclosure of records stored abroad by a U.S. service provider.

To the extent the cases cited by Microsoft note that courts lack statutory authority to issue warrants for physical searches abroad, this has nothing to do with any "territorial limits of the warrant power." The reason courts lack such authority is that "foreign searches have neither been historically subject to the warrant procedure, nor could they be as a practical matter." *Odeh*, 552 F.3d at 170 (quoting *United States* v. *Barona*, 56 F.3d 1087, 1093 n. 1 (9th Cir. 1995)). There is simply no mechanism for enforcing a search warrant directed at physical property located in a foreign country. *See United States* v. *Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (noting that a warrant issued by a magistrate judge in this country authorizing a search in foreign territory "would be a dead letter outside the United States").

Because the Warrant does not involve an attempt to exercise control over foreign territory, the practical and jurisdictional limitations Microsoft raises are completely inapposite here. SCA warrants do not generally contemplate federal law enforcement agents entering the physical premises of a provider at all, whether those premises are located in the United States or abroad. An SCA warrant instead compels the disclosure of documents. To the degree that such compulsion involves the exercise of sovereign power, that power is exercised exclusively within the United States. The warrant is served upon the provider *here*; the provider must produce its records to a law

enforcement agent *here*; and if the provider fails to do so, the provider is subject to court sanction imposed *here*. There is no extraterritorial application of domestic law under these circumstances.

Equally inapplicable here is the *Charming Betsy* doctrine, which counsels that statutes should be construed to be consistent with international law. Microsoft fails to identify any principle of international law violated by the use of an SCA warrant to obtain records stored abroad. Relying on Section 432(2) of the Restatement (Third) of Foreign Relations, Microsoft argues that "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state." (Br. 20). But requiring the disclosure of records by a U.S. company does not involve any enforcement activity by government personnel on foreign territory, which is the concern of that section. *See* Restatement (Third) of Foreign Relations § 432 n.1 (explaining that the rule arose from situations in which one country's "territory was violated" by foreign officers conducting arrests or interrogations without the country's knowledge). The Restatement section truly on point is Section 442(1)(a), which recognizes that "[a] court or agency in the United States, when authorized by statute or rule of court," is empowered to "order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States." *Id.* § 442(1)(a). That, of course, precisely describes what the Warrant orders Microsoft to do.

Microsoft further errs by arguing that compelling a U.S. company to disclose records stored abroad "would infringe the U.S.'s obligation to perform its treaty commitments in good faith," by "allowing the Government to end run the MLATs that the United States has signed with Ireland and the [European Union]." (Br. 20-21). There is nothing in international law that requires the Government to use a Mutual Legal Assistance Treaty ("MLAT") to obtain evidence (particularly from a U.S. provider) located in a foreign country when other lawful means of obtaining the

evidence are available. Nor do the specific MLATs the United States has signed with Ireland and the European Union contain any such requirement. *See United States* v. *Alvarez-Machain*, 504 U.S. 655, 664-67 (1992) (holding that a treaty does not prohibit actions "outside of its terms" where it "does not purport to specify the only way" in which the United States may accomplish a task); *see also In re Grand Jury Subpoena*, 646 F.3d 159, 165 (4th Cir. 2011) (finding that MLAT was "not the exclusive means for the government to obtain documents from a party located in [a foreign] country"); *United States* v. *Rommy*, 506 F.3d 108, 129 (2d Cir. 2007) (finding that MLAT had "no application to evidence obtained outside the MLAT process"); *cf. Societe Nationale Industrielle Aerospatiale* v. *U.S. Dist. Court for Southern Dist. of Iowa*, 482 U.S. 522, 536 (1987) (holding that Hague Convention is "a permissive supplement, not a pre-emptive replacement, for other means of obtaining evidence located abroad").[13] An MLAT simply provides one mechanism for the United States to request the assistance of a foreign country where such assistance is needed to obtain evidence located within that country.

Microsoft's arguments based on the presumption against extraterritoriality and the *Charming Betsy* canon are further dispelled by the *BNS* doctrine. Where the SCA requires disclosure of records that a provider has chosen to store abroad, the extraterritorial and international-law implications are no different from those of a subpoena seeking the same. The statutes and rules authorizing subpoenas do not typically contain any express provisions stating that subpoenas may be used to compel the disclosure of records stored abroad, as Microsoft's view of the presumption against extraterritoriality would seem to require. Yet, Microsoft concedes that,

[13] Indeed, no MLAT to which the United States is a party requires "exclusive use" of the MLAT to obtain records from the other party. At most, a few MLATs require the parties to make "first use" of the MLAT before resorting to other means, but preserve the ability to use measures such as a *BNS* subpoena in the event that the MLAT process generates problems or delays. Notably, the U.S.-Ireland MLAT does not contain any such "first use" provision. A copy of the MLAT between the United Sates and Ireland is attached to this brief as Exhibit B.

under the *BNS* line of cases, a provider cannot resist compliance with a subpoena based on the foreign location of the responsive records. (Br. 24). Likewise, Microsoft does not suggest that the *Charming Betsy* canon is violated by construing the statutes and rules authorizing subpoenas to permit the compelled disclosure of records located abroad. Yet, Microsoft fails to explain why such a construction is suddenly transformed into a violation of international law when the form of process that triggers the obligation to disclose records is labeled "warrant" rather than "subpoena."

**4. Policy Considerations Weigh Decisively Against Microsoft's Position**

The policy consequences of Microsoft's position further demonstrate that it cannot reflect the intent of Congress.[14] In today's digital environment, email and other electronic communications are used extensively by criminals of all types in the United States and abroad, from fraudsters to hackers to drug dealers, in furtherance of violations of U.S. law. The ability to obtain electronically stored information from domestic service providers—pursuant to judicial authorization as required by the SCA—is a fundamental component of effective modern law enforcement. Yet such information, like the data sought by the Warrant here, can be maintained in any location and moved around the world easily, at any time and for any reason. Were Microsoft's position adopted, the Government's ability to obtain such information from a provider would turn entirely on whether it happens to be stored here or abroad, even though the provider, based in the United States, maintains control over the data wherever it is. Such a regime would be rife with potential for arbitrary outcomes and criminal abuse.

[14] Microsoft suggests that it is improper to consider here the practical consequences of its crabbed reading of the SCA (Br. 28), but that view has been rejected by the Second Circuit. *See Johnson* v. *United States*, 123 F.3d 700, 702-03 (2d Cir. 1997) ("In determining the meaning of a statute, courts must look not only to the particular statutory language, but also to the design of the statute as a whole and to its object and policy. Thus, the 'appropriate methodology' to employ in interpreting a statute is to look to the common sense of the statute, to its purpose, [and] to the practical consequences of the suggested interpretations . . . .").

Microsoft's own data storage policy provides but one illustration. According to Microsoft, where a user's data is stored depends entirely on which country the user selects when signing up for the account. Microsoft does not require or verify any actual connection between the user and the selected country. As Judge Francis noted, a criminal user can easily manipulate such a policy to evade the reach of U.S. law enforcement "by the simple expedient of giving false residence information, thereby causing the [provider] to assign his account to a server outside the United States." *In re Warrant*, 2014 WL 1661004, at *8.[15]

Of course, a provider need not base the location where it stores a user's data on the user's location at all—whether self-reported or verified. A provider may choose to store user data abroad, for example, simply to take advantage of lower costs associated with foreign server-hosting facilities. Or, on any given day, a provider might move a particular user's data from a U.S.-based server to a foreign server, and perhaps back again, for network maintenance or load-balancing reasons, which is an increasingly common practice with the growth of cloud computing. *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1623, 1629 (May 2013) ("'[C]loud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of

[15] It is no answer to adopt the approach urged by *amicus* AT&T that courts undertake a "fact-specific analysis" of whether "the customer or subscriber has a sufficient nexus to the United States" before issuing an SCA warrant. (AT&T Br. 11-12). First, such a process already exists to the extent that, for every SCA warrant, a judge has already found that there is probable cause to believe that the account will contain evidence of a violation of the criminal laws of the United States. Whatever a "sufficient nexus to the United States" by a customer might mean, determining the true identity and location of an Internet user is a pervasive investigative challenge in the cybercrime context. Through the use of "proxy" services and other anonymizing tools, a user easily can conceal such information, and thus a provider frequently will have no ability to determine whether a user actually resides in the United States or is a U.S. citizen. In any event, even where such information could be ascertained, it is irrelevant to the statutory authorization to compel disclosure through an SCA warrant, which turns not on the nationality or residence of the investigative subject, but simply on whether the data are under the provider's control and whether the provider is within the jurisdiction of the United States.

the world at 4pm.'" (quoting Article 29 Data Prot. Working Party, Opinion 05/2012 on Cloud Computing 17, (EC) No. 01037/12, WP 196 (Jul. 1, 2012))).

A provider may even choose to store user data abroad with the specific intent to place it out of the Government's reach, based, for example, on a desire to avoid the inconvenience of responding to legal process. Indeed, some providers less scrupulous than Microsoft may do so with the specific intent to accommodate criminal users. *See, e.g.*, *United States* v. *Paunescu*, No. 13 Cr. 41 (RPP), Indictment (S.D.N.Y. filed Jan. 17, 2013) (bringing charges under 18 U.S.C. § 1030(b) against operator of "bulletproof hosting service," who, "in exchange for fees, . . . provided cyber criminals with Internet Protocol . . . addresses and servers in a manner designed to enable them to preserve their anonymity and evade detection by law enforcement").

The reason a provider may choose to store data abroad should make no difference to the enforcement of an SCA warrant. When the Government obtains an SCA warrant, it means that a neutral magistrate has determined, on a probable cause standard, that evidence of a crime likely resides in electronic data under the control of a domestic service provider. There is no good reason to believe, and Microsoft offers none, that Congress intended to leave it up to the whim of the provider, or the vagaries of its data storage practices, whether that evidence should be disclosed to law enforcement. No valid privacy interest is vindicated by such an arbitrary approach.

Microsoft's cavalier retort to these practical concerns—that the Government can simply use an MLAT whenever records are unavailable through the SCA (Br. 27-30)—hardly suggests a satisfactory alternative. As an initial matter, Microsoft's rosy view of the efficacy of the MLAT process bears little resemblance to reality. In contrast to an SCA warrant, which can be served upon a provider immediately upon issuance by a judge, an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the

procedural idiosyncrasies of the country's legal system. *See, e.g.*, *In re Grand Jury Subpoenas*, 318 F.3d 379, 381-82 (2d Cir. 2003) (noting that foreign country's response to MLAT request was still incomplete after two years); *United States* v. *Safavian*, 644 F. Supp. 2d 1, 14 n.5 (D.D.C. 2009) (noting the long "length of time that frequently is required to acquire evidence by way of an MLAT"). It is no accident that federal law specifically provides for an exclusion of time under the Speedy Trial Act (for up to a year), as well as the suspension of a criminal statute of limitations (for up to three years), while the Government is waiting to receive foreign evidence in response to an MLAT request. *See* 18 U.S.C. §§ 3161(h)(8) & 3292.

Moreover, there are many countries in the world that do not even have MLATs with the United States. A U.S. provider could easily choose to locate its user data in such a country, either for business reasons or for the specific purpose of evading the reach of U.S. law enforcement. By the same token, a U.S. provider could—again, for legitimate or illegitimate reasons—distribute the contents of a single user account across computers maintained in dozens of countries, making it practically impossible for the Government to collect the account data through international channels, regardless of whether the countries involved have MLATs or not. As Judge Francis observed, it is even conceivable that a provider could establish server locations at sea or otherwise beyond the territorial jurisdiction of any nation. *In re Warrant*, 2014 WL 1661004, at *9. There is no reason to believe that Congress intended for such obstacles to thwart the Government from obtaining evidence of criminal activity, particularly when the providers involved often can, like Microsoft, easily disclose the relevant data through their information systems in the United States, no matter where the original copy happens to reside.

Microsoft asserts that, unless the Government is required to use MLATs to obtain data stored abroad, U.S. foreign relations will be damaged and other countries will retaliate by asserting jurisdiction over electronic data stored here. (Br. 29). Aside from being purely speculative, such

concerns are exclusively for the consideration of the political branches and do not provide a sound basis to graft extra-statutory restrictions on duly enacted legislation. *See generally Oetjen* v. *Cent. Leather Co.*, 246 U.S. 297, 302 (1918) ("The conduct of the foreign relations of our Government is committed by the Constitution to the executive and legislative—'the political'—departments of the government, and the propriety of what may be done in the exercise of this political power is not subject to judicial inquiry or decision."). They do not provide a basis for challenging enforcement of a warrant validly issued under the SCA.

Microsoft also argues that, unless its position is adopted, the U.S. technology sector stands to lose overseas customers who fear "the U.S. Government's extraterritorial access to their user information." (Br. 30). However, an SCA warrant permits the Government to access user information—wherever it may be stored—only after a neutral magistrate judge has found probable cause to believe that the information contains evidence of criminal activity. This is a time-tested manner by which the Government obtains evidence in criminal prosecutions, and nothing could be farther from an unchecked exercise of power. The form of legal process at issue is specifically designed to protect legitimate privacy interests, by requiring that any intrusion on those interests be properly justified by the need to uncover evidence of a crime.

Whether compliance with the SCA will have any negative effect on Microsoft's business, or that of any other service provider, is ultimately beside the point. The fact remains that there exists probable cause to believe that evidence of a violation of U.S. criminal law, affecting U.S. residents and implicating U.S. interests, is present in records under Microsoft's control. Microsoft is a U.S.-based company, enjoying all the rights and privileges of doing business in this country, including in particular the protection of U.S. intellectual property laws. With the benefits of corporate citizenship in the United States come corresponding responsibilities, including the responsibility to comply with U.S. legal process. Microsoft should not be heard to complain that doing so might

harm its bottom line. The production of evidence in response to legal process "is not to be regarded as a gratuity, or a courtesy, or an ill-required favor. It is a duty not to be grudged or evaded." *Kaufman* v. *Edelstein*, 539 F.2d 811, 820 (2d Cir. 1976).

## POINT II

### The Warrant Satisfies Any Possible Application of the Particularity Requirement of the Fourth Amendment

Microsoft also makes a perfunctory attempt to argue that the Fourth Amendment's particularity requirement has been violated because the Warrant "does not limit the Government's search to any specific facility or physical premises." (Br. 26-27). This argument is both procedurally unpreserved, *see Carroll* v. *David*, No. 04 Civ. 307, 2009 WL 666395, at *2 (N.D.N.Y. Mar. 11, 2009) ("It is generally accepted that an argument not raised before the magistrate judge is waived and cannot be asserted for the first time before the district court." (collecting cases)), and substantively lacking in merit, because the Warrant's specification of a particular account fully satisfies any possible application of the particularity requirement here.

The requirement that a warrant particularly describe the "place to be searched," like other provisions of the Fourth Amendment, is "practical and not abstract" and therefore must be applied in a "commonsense and realistic fashion." *United States* v. *Ventresca*, 380 U.S. 102, 108 (1965); *United States* v. *Bianco*, 998 F.2d 1112, 1123 (2d Cir. 1993) ("The Supreme Court . . . has refused to apply the fourth amendment literally, preferring instead a flexible approach designed to keep pace with a technologically advancing society."); *see also United States* v. *Karo*, 468 U.S. 705, 718 (1984) (stating that a search warrant for a tracking device need not specify the place to be searched). For example, in the wiretap context, the particularity requirement is commonly satisfied simply by reference to the telephone number of the line to be monitored, rather than the telephone's physical location (or even physical description). *See United States* v. *Otibu*, No. 02 Cr. 104 (AGS), 2002 WL

1033876, at *1 (S.D.N.Y. May 21, 2002) (holding that wiretap order's identification of phone number satisfied particularity requirement).

Thus, for an SCA warrant, what realistically and practically needs specification is the electronic account containing the data to be reviewed by the Government. Just as the particularity requirement is satisfied by a warrant directed to a physical premises that specifies the street address of the premises to be searched, an SCA warrant specifying the email address (or similar user identifier) associated with the account to be searched also satisfies that requirement. That level of detail is sufficient to ensure that agents do not review accounts belonging to other users, and it therefore adequately describes the "place to be searched" within the meaning of the Fourth Amendment. That is why courts have time and again upheld such warrants against particularity challenges along the lines of the one Microsoft presses here. *See, e.g.*, *United States* v. *Noyes*, No. 08 Cr. 55, 2010 WL 5139859, at *11 (W.D. Pa. Dec. 8, 2010); *United States* v. *Bach*, No. 01 Cr. 221, 2001 WL 1690055, at *2 (D. Minn Dec. 14, 2001), *rev'd on other grounds*, 310 F.3d 1063 (8th Cir. 2002); *see also United States* v. *Bansal*, 663 F.3d 634, 662 (3d Cir. 2011); *United States* v. *Hanna*, 661 F.3d 271, 286-87 (6th Cir. 2011); *United States* v. *Bowen*, 689 F. Supp. 2d 675, 680-81 (S.D.N.Y. 2010).

In light of this authority, there is no requirement that the Warrant further specify the physical location—whether within the United States or abroad—of the storage media where the data is stored. Not only is the Government typically not in a position to know the physical location of electronic data when it obtains an SCA warrant—and not only could that location change at any time before the provider responds—but the location of the data is, in any event, irrelevant to the concerns underlying the particularity requirement. Accordingly, where, as here, a warrant specifies the electronic account to be searched, and further specifies the types of evidence the Government may seize from the account, there can be no violation of the particularity requirement.

## CONCLUSION

For the foregoing reasons, Microsoft's motion to vacate the Warrant should be denied.

Dated: July 9, 2014
New York, New York

Respectfully submitted,

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

By: */s/ Serrin Turner*
SERRIN TURNER
JUSTIN ANDERSON
Assistant United States Attorneys
(212) 637-1946/1035

# EXHIBIT

# A

AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

# 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*

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

| 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.

# EXHIBIT B

TREATIES AND OTHER INTERNATIONAL ACTS SERIES 13137

# MUTUAL LEGAL ASSISTANCE

**Treaty Between the**
**UNITED STATES OF AMERICA**
**and IRELAND**

Signed at Washington January 18, 2001

NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966 (80 Stat. 271; 1 U.S.C. 113)—

". . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof."

# IRELAND

## Mutual Legal Assistance

*Treaty signed at Washington January 18, 2001;*
*Transmitted by the President of the United States of America to the Senate July 11, 2002 (Treaty Doc. 107-9, 107th Congress, 2d Session);*
*Reported favorably by the Senate Committee on Foreign Relations October 8, 2002 (Senate Executive Report No. 107-15, 107th Congress, 2d Session);*
*Advice and consent to ratification by the Senate November 14, 2002;*
*Ratified by the President April 29, 2003;*
*Ratified by Ireland July 24, 2009;*
*Ratifications exchanged at Washington August 11, 2009;*
*Entered into force August 11, 2009.*

# TREATY BETWEEN
# THE GOVERNMENT OF THE UNITED STATES OF AMERICA
# AND
# THE GOVERNMENT OF IRELAND
# ON
# MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

TABLE OF CONTENTS

The Government of the United States of America and the Government of Ireland,

Desiring to improve the effectiveness of the law enforcement authorities of both countries in the investigation, prosecution, and prevention of crime through cooperation and mutual legal assistance in criminal matters,

Have agreed as follows:

**Article 1**

**Scope of Assistance**

1. The Parties shall provide mutual assistance, in accordance with the provisions of this Treaty, in connection with the investigation, prosecution, and prevention of offenses, and in proceedings related to criminal matters.

2. Assistance shall include:

(a) taking the testimony or statements of persons;

(b) providing documents, records, and articles of evidence;

(c) locating or identifying persons;

(d) serving documents;

(e) transferring persons in custody for testimony or other purposes;

(f) executing requests for searches and seizures;

(g) identifying, tracing, freezing, seizing, and forfeiting the proceeds and instrumentalities of crime and assistance in related proceedings;

(h) such other assistance as may be agreed between Central Authorities.

3. Except when required by the laws of the Requested Party, assistance shall be provided without regard to whether the conduct that is the subject of the investigation, prosecution, or proceeding in the territory of the Requesting Party would constitute an offense under the laws of the Requested Party.

4. This Treaty is intended solely for mutual legal assistance between the Parties. The provisions of this Treaty shall not give rise to a right on the part of any private person to obtain, suppress, or exclude any evidence, or to impede the execution of a request.

**Article 2**

**Central Authorities**

1. Each Party shall designate a Central Authority to make and receive requests pursuant to this Treaty.

2. For the Government of the United States of America, the Central Authority shall be the Attorney General or a person designated by the Attorney General. For the Government of Ireland, the Central Authority shall be the Minister for Justice, Equality and Law Reform or a person designated by the Minister.

3. The Central Authorities shall communicate directly with one another for the purposes of this Treaty.

**Article 3**

**Limitations on Assistance**

1. The Central Authority of the Requested Party may deny assistance if:

(a) the Requested Party is of the opinion that the request, if granted, would impair its sovereignty, security, or other essential interests, or would be contrary to important public policy;

(b) the request relates to an offender who, if proceeded against under the law of the Requested Party for the offense for which assistance is requested, would be entitled to be discharged on the grounds of a previous acquittal or conviction;

(c) the request relates to an offense that is regarded by the Central Authority of the Requested Party as:

(i) an offense of a political character; or

(ii) an offense under military law of the Requested Party which is not also an offense under the ordinary criminal law of the Requested Party; or

(d) the request is not made in conformity with the Treaty.

2. Before denying assistance pursuant to this Article, the Central Authority of the Requested Party shall consult with the Central Authority of the Requesting Party to consider whether assistance can be given subject to such conditions as it deems necessary. If the Requesting Party accepts assistance subject to these conditions, it shall comply with the conditions.

**Article 4**

**Form and Contents of Requests**

1. A request for assistance shall be in writing except that the Central Authority of the Requested Party may accept a request in another form in emergency situations. In any such case, the request shall be confirmed in writing within ten days thereafter unless the Central Authority of the Requested Party agrees otherwise. The request shall be in an official language of the Requested Party unless otherwise agreed.

2. The request shall include the following:

(a) the name of the authority conducting the investigation, prosecution, or proceeding to which the request relates;

(b) a description of the subject matter and nature of the investigation, prosecution, or proceeding, including the specific criminal offenses which relate to the matter;

(c) a description of the evidence, information, or other assistance sought; and

(d) a statement of the purpose for which the evidence, information, or other assistance is sought.

3. To the extent necessary and possible, a request shall also include:

(a) information on the identity and location of any person from whom evidence is sought;

(b) information on the identity and location of a person to be served, that person's relationship to the proceedings, and the manner in which service is to be made;

(c) information on the identity and whereabouts of a person to be located;

(d) a precise description of the place or person to be searched and of the articles to be seized;

(e) a description of the manner in which any testimony or statement is to be taken and recorded;

(f) a list of questions to be asked of a witness;

(g) a description of any particular procedure to be followed in executing the request;

(h) information as to the allowances and expenses to which a person asked to appear in the territory of the Requesting Party will be entitled; and

(i) any other information which may be brought to the attention of the Requested Party to facilitate its execution of the request.

4. The Requested Party may ask the Requesting Party to provide any further information which appears to the Requested Party to be necessary for the purpose of executing the request.

**Article 5**

**Execution of Requests**

1. As empowered by this Treaty or by national law, or in accordance with its national practice, the Central Authority of the Requested Party shall take whatever steps it deems necessary to execute promptly requests received from the Requesting Party. The Courts of the Requested Party shall have authority to issue subpoenas, search warrants, or other orders necessary to execute the request.

2. The Central Authority of the Requested Party shall make all necessary arrangements for representation in the territory of the Requested Party of the Requesting Party in any proceedings arising out of a request for assistance.

3. The method of execution specified in the request shall be followed except to the extent that it is incompatible with the laws and practices of the Requested Party.

4. If the Central Authority of the Requested Party determines that execution of a request would interfere with an ongoing criminal investigation, prosecution, or proceeding under the laws of that Party, or prejudice the safety of any person, it may postpone execution, or make execution subject to conditions determined to be necessary after

consultations with the Central Authority of the Requesting Party. If the Requesting Party accepts the assistance subject to the conditions, it shall comply with the conditions.

5. The Central Authority of the Requested Party shall, in accordance with its national law and practice, facilitate the presence in the execution of the request of such persons as are specified in the request.

6. The Requested Party shall, upon request, keep confidential any information which might indicate that a request has been made or responded to. If the request cannot be executed without breaching confidentiality, the Requested Party shall so inform the Requesting Party, which shall then determine the extent to which it wishes the request to be executed.

7. The Central Authority of the Requested Party shall respond to reasonable inquiries by the Central Authority of the Requesting Party concerning progress toward execution of the request.

8. The Central Authority of the Requested Party may ask the Central Authority of the Requesting Party to provide information in such form as may be necessary to enable it to execute the request or to undertake any steps which may be necessary under the laws and practices of the Requested Party in order to give effect to the request received from the Requesting Party.

9. The Central Authority of the Requesting Party shall promptly inform the Central Authority of the Requested Party of any circumstances which make it inappropriate to proceed with the execution of the request or which require modification of the action requested.

10. The Central Authority of the Requested Party shall promptly inform the Central Authority of the Requesting Party of any circumstances which are likely to cause a significant delay in responding to the request.

11. The Central Authority of the Requested Party shall promptly inform the Central Authority of the Requesting Party of the outcome of the execution of the request. If the request is denied, the Central Authority of the Requested Party shall inform the Central Authority of the Requesting Party of the reasons for the denial.

**Article 6**

**Costs**

1. The Requested Party shall pay all costs relating to the execution of the request, including the costs of representation, except for the fees of expert witnesses, the costs of translation, interpretation, and transcription, and the allowances and expenses related to travel of persons pursuant to Articles 10 and 11, which costs, fees, allowances, and expenses shall be paid by the Requesting Party.

2. If, during the execution of a request, it becomes apparent that complete execution will entail expenses of an extraordinary nature, the Central Authorities shall consult to determine the terms and conditions under which execution may continue.

**Article 7**

**Limitations on Use**

1. The Requesting Party shall not use or disclose any information or evidence obtained under this Treaty for any purposes other than those stated in the request without the prior consent of the Requested Party.

2. Nothing in this Article shall preclude the use or disclosure of information to the extent that there is an obligation to do so under the Constitution of the Requesting Party in a criminal prosecution. The Requesting Party shall notify the Requested Party in advance of any such proposed disclosure.

**Article 8**

**Testimony or Evidence in the Territory of the Requested Party**

1. A person in the territory of the Requested Party from whom testimony or evidence is requested pursuant to this Treaty may be compelled, if necessary, to appear and testify or produce items, including documents, records, and articles of evidence.

2. Upon request, the Central Authority of the Requested Party shall furnish information in advance about the date and place of the taking of the testimony or evidence pursuant to this Article.

3. In accordance with its laws and practice, the Requested Party shall permit the presence of such persons as specified in the request during the execution of the request, and shall allow such persons to ask questions directly of the person whose testimony or evidence is being taken or indirectly through a legal representative qualified to appear before the courts of the Requested Party.

4. If the person referred to in paragraph 1 asserts a claim of immunity, incapacity, or privilege under the laws of the Requesting Party, the testimony or evidence shall nonetheless be taken and the claim made known to the Central Authority of the Requesting Party for resolution by the authorities of that Party.

5. Evidence produced in the territory of the Requested Party pursuant to this Article or which is the subject of testimony taken under this Article may be authenticated by an attestation, including, in the case of business records, authentication in the manner indicated in Form A appended to this Treaty. The absence or nonexistence of such records may, upon request, be certified through the use of Form B appended to this Treaty. Records authenticated by Form A, or Form B certifying the absence or nonexistence of such records, shall be admissible in evidence in the Requesting Party. Documentary information produced pursuant to this Article may also be authenticated pursuant to such other form or manner as may be prescribed from time to time by either Central Authority.

**Article 9**

**Records of Government Agencies**

1. The Requested Party shall provide the Requesting Party with copies of publicly available records, including documents or information in any form, in the possession of government departments and agencies in the Requested Party.

2. The Requested Party may provide copies of any documents, records, or information which are in the possession of a government department or agency of that Party,

but which are not publicly available, to the same extent and under the same conditions as such copies would be available to its own law enforcement or judicial authorities. The Requested Party may in its discretion deny a request pursuant to this paragraph entirely or in part.

3. Records produced pursuant to this Article shall, upon request, be authenticated under the provisions of the Convention Abolishing the Requirement of Legalisation for Foreign Public Documents, dated October 5, 1961, or by an official competent to do so through the use of Form C appended to this Treaty. The absence or nonexistence of such records may, upon request, be certified through the use of Form D appended to this Treaty. No further authentication shall be necessary. Records authenticated by Form C, or Form D certifying the absence or nonexistence of such records, shall be admissible in evidence in the Requesting Party. Documentary information produced pursuant to this Article may also be authenticated pursuant to such other form or manner as may be prescribed from time to time by either Central Authority.

**Article 10**

**Testimony in the Territory of the Requesting Party**

1. When the Requesting Party requests the appearance of a person in the territory of that Party, the Requested Party shall invite the person to appear voluntarily before the appropriate authority in the territory of the Requesting Party. The Requesting Party shall indicate the extent to which the expenses will be paid. The Central Authority of the Requested Party shall promptly inform the Central Authority of the Requesting Party of the response of the person.

2. The Central Authority of the Requesting Party may, in its discretion, determine that a person appearing in the territory of the Requesting Party pursuant to this article shall not be subject to service of process, or be detained or subjected to any restriction of personal liberty, by reason of any acts or convictions which preceded his departure from the territory of the Requested Party.

3. The safe conduct provided for by this Article shall cease seven days after the Central Authority of the Requesting Party has notified the Central Authority of the Requested Party that the person's presence is no longer required, or when the person, having left the territory of the Requesting Party, voluntarily returns. The Central Authority of the Requesting Party may, in its discretion, extend this period for up to fifteen days if it determines that there is good cause to do so.

**Article 11**

**Transfer of Persons in Custody**

1. A person in the custody of one Party whose presence in the territory of the other Party is sought for purposes of assistance under this Treaty shall be transferred for those purposes if the person and the Central Authorities of both Parties consent.

2. For purposes of this Article:

(a) the receiving Party shall have the authority and the obligation to keep the person transferred in custody unless otherwise authorized by the sending Party;

(b) the receiving Party shall return the person transferred to the custody of the sending Party as soon as circumstances permit

and in any event no later than the date upon which the person would have been released from custody in the territory of the sending Party, unless otherwise agreed by both Central Authorities and the person transferred;

(c) the receiving Party shall not require the sending Party to initiate extradition proceedings for the return of the person transferred; and

(d) the person transferred shall receive credit for service of the sentence imposed in the sending Party for time served in the custody of the receiving Party.

**Article 12**

**Location or Identification of Persons or Items**

The Requested Party shall use its best efforts to ascertain the location or identity of persons or items specified in the request.

**Article 13**

**Service of Documents**

1. The Requested Party shall use its best efforts to effect service of any document relating, in whole or in part, to any request for assistance made by the Requesting Party under the provisions of this Treaty.

2. Service of any document by virtue of paragraph (1) of this Article shall not impose any obligation under the law of the Requested Party to comply with it.

3. The Requesting Party shall transmit any request for the service of a document requiring the appearance of a person before an authority in the Requesting Party a reasonable time before the scheduled appearance.

4. The Requested Party shall return a proof of service in the manner specified in the Request.

**Article 14**

**Search and Seizure**

1. The Requested Party shall execute a request for the search, seizure, and delivery of any item to the Requesting Party if the request includes the information justifying such action under the laws of the Requested Party and it is carried out in accordance with the laws of that Party.

2. The Requested Party may refuse a request if it relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances.

3. Upon request, every official who has custody of a seized item shall certify, through the use of Form E appended to this Treaty, the continuity of custody, the identity of the item, and the integrity of its condition. No further certification shall be required. The certificates shall be admissible in evidence in the Requesting Party. Certification under this

Article may also be provided in any other form or manner as may be prescribed from time to time by either Central Authority.

4. The Central Authority of the Requested Party may require that the Requesting Party agree to the terms and conditions deemed to be necessary to protect third party interests in the item to be transferred.

**Article 15**

**Return of Items**

The Central Authority of the Requesting Party shall return any items, including documents, records, or articles of evidence furnished to it in execution of a request under this Treaty as soon as possible unless the Central Authority of the Requested Party waives their return.

**Article 16**

**Assistance in Forfeiture Proceedings**

1. If the Central Authority of one Party becomes aware of proceeds or instrumentalities of offenses which are located in the territory of the other Party and may be forfeitable or otherwise subject to seizure under the laws of that Party, it may so inform the Central Authority of the other Party. If that other Party has jurisdiction in this regard, it may present this information to its authorities for a determination whether any action is appropriate. These authorities shall issue their decision in accordance with the laws of their country, and the Central Authority shall report to the Central Authority of the other Party on the action taken.

2. The Parties shall assist each other to the extent permitted by their respective laws in proceedings relating to the forfeiture of the proceeds and instrumentalities of offenses. This may include action to temporarily freeze the proceeds or instrumentalities pending further proceedings.

3. The Party that has custody over proceeds or instrumentalities of offenses shall dispose of them in accordance with its laws. Either Party may transfer all or part of such assets, or the proceeds of their sale, to the other Party, to the extent permitted by the transferring Party's laws and upon such terms as it deems appropriate.

**Article 17**

**Compatibility with Other Arrangements**

Assistance and procedures set forth in this Treaty shall not prevent either Party from granting assistance to the other Party through the provisions of other applicable international agreements, or through the provisions of its national laws. The Parties may also provide assistance pursuant to any bilateral arrangement, agreement, or practice which may be applicable.

**Article 18**

**Consultation**

The Central Authorities of the Parties shall consult, at times mutually agreed to by them, to promote the most effective use of this Treaty. The Central Authorities may also agree on such practical measures as may be necessary to facilitate the implementation of this Treaty.

**Article 19**

**Ratification, Entry Into Force, and Termination**

1. This Treaty shall be subject to ratification, and the instruments of ratification shall be exchanged as soon as possible.

2. This Treaty shall enter into force upon the exchange of instruments of ratification.

3. This Treaty shall apply to any request presented after the date of the Treaty's entry into force, whether the relevant acts or omissions occurred prior to or after that date.

4. Either Party may terminate this Treaty by means of written notice to the other Party. Termination shall take effect six months following the date of notification. Ongoing proceedings at the time of termination shall nonetheless be completed in accordance with the provisions of this Treaty.

IN WITNESS WHEREOF, the undersigned, being duly authorized by their respective Governments have signed this Treaty.

DONE at Washington, in duplicate, this eighteenth day of January, 2001.

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:

FOR THE GOVERNMENT OF IRELAND:

**FORM A** (see Article 8)

CERTIFICATE OF AUTHENTICITY OF
BUSINESS RECORDS

I, _____, attest on penalty of
(Name)

criminal punishment for false statement or false attestation that I am employed by

_____
(Name of Business from which documents are sought)

and that my official title is _____.
(Official Title)

I further state that each of the records attached hereto is the original or a duplicate of the original records in the custody of _____.
(Name of Business from which documents are sought)

I further state that:

(A) such records were made, at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters;

(B) such records were kept in the course of a regularly conducted business activity;

(C) the business activity made such records as a regular practice;

(D) if such record is not the original, such record is a duplicate of the original.

_____ _____
Signature Date

Sworn to or affirmed before me, _____, a

_____ this _____ day of _____, 20____.
(notary public, judicial officer, etc.)

**FORM B** (see Article 8)

CERTIFICATE OF ABSENCE OR NON-EXISTENCE OF BUSINESS RECORDS

I, _____, attest on penalty of criminal punishment for
(Name)

false statement or false attestation that I am employed by

_____ and that my official title
(Name of Business from which documents are sought)

is_____.
(Official Title)

As a result of my employment with the above-named business, I am familiar with the business records it maintains. The business maintains business records that:

(A) are made, at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters;

(B) are kept in the course of a regularly-conducted business activity;

(C) are made by the business as a regular practice.

Among the records so maintained are records of individuals and entities that have accounts or \ otherwise transact business with the above-named business. I have made or caused to be made a diligent search of those records. No records have been found reflecting any business activity between the business and the following individuals and entities:_____

_____.

If the business had maintained an account on behalf of or had participated in a transaction with any of the foregoing individuals or entities, its business records would reflect that fact.

_____ _____
Signature Date

Sworn to or affirmed before me, _____, a
(Name)

_____ this _____ day of _____, 20_____.
(Notary public, judicial officer, etc.)

**FORM C** (see Article 9)

ATTESTATION OF AUTHENTICITY OF FOREIGN PUBLIC RECORDS

I, _____, attest on penalty of criminal
(Name)

punishment for false statement or attestation that my position with the Government of

_____ is _____ and that in that
(Country) (Official Title)

position I am duly authorized to attest that the documents attached and described below are true and accurate copies of original official records which are recorded or filed in

_____, which is a government office or agency of
(Name of Office or Agency)

_____.
(Country)

Description of Documents:

_____
(Signature)

_____
(Title)

_____
(Date)

**FORM D** (see Article 9)

ATTESTATION REGARDING ABSENCE
OR NON-EXISTENCE OF FOREIGN PUBLIC RECORDS

I, _____, attest on penalty of criminal punishment
(Name)

for false statement or attestation that my position with the Government of _____
(Country)

is _____ and that in that position I am duly authorized to make this
(Official Title)

attestation.

I do hereby certify that I am the custodian of records of

_____, and that I have made a diligent
(Name of Public Office or Agency)

search of the said records for the

_____, and that
(Description of Records for Which a Search was Done)

no such records are found to exist therein. I further certify that the records for which a search was conducted set forth matters which are required by the laws of the Government of

_____ to be recorded or filed and reported, and such matters regularly
(Country)

are recorded or filed and reported by _____.
(Name of Public Agency or Office)

_____
Signature

_____
Date

**FORM E** (see Article 14)

ATTESTATION WITH RESPECT TO SEIZED ARTICLES

I, _____, attest on penalty of criminal punishment for
(Name)

false statements or attestation that my position with the Government of _____
(Country)

is _____. I received the articles listed below from
(Official Title)

_____ on _____,
(Name of Person) (Date)

at _____ in the following condition:
(Place)

Description of Article:

Changes in Condition while in my custody:

Official Seal or Stamp

_____
(Signature)

_____
(Title)

_____
(Date)