UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	Case No. 1:13-mj-02814-UA-1

BRIEF *AMICUS CURIAE* OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF MICROSOFT CORPORATION

Hanni Fakhoury (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: hanni@eff.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

INTRODUCTION

At the heart of the magistrate's opinion is a fundamental misunderstanding about how the Fourth Amendment's privacy protections apply in the digital world.

The magistrate wrongly believed that the Fourth Amendment does not come into play until the *government* itself reviews the messages it seeks. *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, --- F. Supp. 2d ---, 2014 WL 1661004, at *6 (S.D.N.Y. Apr. 25, 2014) (hereinafter "*Mag. Opinion*"). But *before* the messages are reviewed and subjected to government "search," they are first subjected to a government "seizure" when they are copied, an event that clearly takes place in Ireland.

By ignoring the seizure and focusing instead on the government agents' review of the emails, the magistrate skipped a fundamental step of the Fourth Amendment analysis in a way that undermines the constitutional protection of electronic communications. "The most consistent way to apply the Fourth Amendment seizure doctrine to computer data is to hold that electronic copying ordinarily seizes it under the Fourth Amendment." Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 711 (2010). Any other rule leaves the government free to collect all the electronic data it wants without the constitutional limitations that would apply to physical, tangible data.

Compounding this mistake was the magistrate's selective incorporation of the warrant requirement into the Stored Communications Act ("SCA"). *See* 18 U.S.C. § 2703(a). By choosing to read out the territorial limitations from the SCA, the magistrate undermined Congress' intent in requiring a warrant for obtaining digitally stored data, ultimately leading to inconsistent application of the SCA.

Finally, the magistrate failed to appreciate that the only way to render the foreign search here "reasonable" was to require the U.S. government to comply with Irish law and the Mutual Legal Assistance Treaty ("MLAT") process in order to obtain the emails it sought. As Internet communications are globalized and American companies place data in numerous jurisdictions, the United States cannot ignore other countries' sovereign interests in protecting the privacy of their citizens' electronic communications and data.

For the reasons described in detail below, the magistrate's decision should be reversed.

ARGUMENT

I. The Magistrate's Conclusion that no Fourth Amendment Event Occurred Until the Government Reviewed the Data in the United States Is Wrong and Dangerous.

The Fourth Amendment protects people from "unreasonable searches and seizures" of their "persons, houses, papers and effects." U.S. Const. amend. IV. A "Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan J., concurring)). As numerous courts have held, people enjoy a reasonable expectation of privacy in email, and so the government's effort to review the messages is a "search." *See, e.g., United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n. 39 (D.D.C. 2012); *United States v. Maxwell*, 45 M.J. 406, 417-18 (C.A.A.F. 1996); *see also In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *3-4 (D. Kan. August 27, 2013) (unpublished).

The magistrate believed that the "search" here did not occur abroad but rather in the U.S. when the messages would be "exposed to possible human observation," and therefore there was no extraterritorial search. *Mag. Opinion*, 2014 WL 1661004, at *6 (quoting Orin S. Kerr,

Searches and Seizures in a Digital World, 119 Harv. L.Rev. 531, 551 (2005)).[1] But before the government could "search" the emails, it had to obtain or "seize" them from Microsoft.

A Fourth Amendment "seizure" occurs when "there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citing *United States v. Chadwick*, 433 U.S. 1, 13, n. 8 (1977)).[2] Ownership is not a requirement of "possession;" a person need only show "dominion and control" over an item in order to demonstrate a possessory interest in it. *See United States v. Perea*, 986 F.2d 633, 639-40 (2d Cir. 1993) (citing *Rakas v. Illinois*, 439 U.S. 128, 144 n. 12, 149 (1978)).

Although "seizure" is often thought of in connection with physical items, it clearly applies to intangible items like data or the content of emails. For example, the Supreme Court has found that the act of recording an aural conversation is both a "search and seizure" of the conversation for purposes of the Fourth Amendment. In *Berger v. New York*, 388 U.S. 41 (1967), the Court found a New York wiretapping statute unconstitutional because it lacked any requirement of particularity. Noting that the "property sought" was intangible conversations, it ruled that the statute's lack of a particularity requirement gave officers "a roving commission to 'seize' any and all conversations." 388 U.S. at 59. *Berger* repeatedly referred to the act of

---

[1] The magistrate's opinion does not make clear which "search" he was focused on: Microsoft's review of emails as the government's agent or the government's review once it obtained the emails from Microsoft. But as explained in more detail below, although the government's literal review of the emails would only occur in the U.S., the magistrate's implicit assumption that Microsoft employees in the U.S. would review the emails before producing them to the government is not necessarily correct. *See* Declaration of Redacted, Doc. No. 16 at ¶¶ 3-5, *see also* Microsoft's Objection to the Magistrate's Order at 7, n. 4.

[2] The Supreme Court's recent revival of the pre-*Katz* focus on physical intrusion onto private property as another way in which the government engages in a "search" also shows that some focus on *where* the government physically accesses information matters for purposes of the Fourth Amendment. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013); *United States v. Jones*, 132 S. Ct. 945, 950-51 (2012).

recording the aural conversations as a "seizure" under the Fourth Amendment. *See id.* at 59-60. The Court did the same thing in *Katz* itself, noting that "electronically listening to and *recording* the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Katz*, 389 U.S. at 353 (emphasis added). As one district court has explained, "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008).

Jefferson is illustrative. There, police executed a search warrant permitting the seizure and search of a number of documents in connection with a bribery investigation. 571 F. Supp. 2d at 699-700. Instructed to only seize items responsive to the search warrant, FBI agents took high-resolution photographs of several items as a substitute for physically removing them under their authority to seize incriminating items in plain view. *Id.* The district court found the act of taking these photographs was a "seizure" under the Fourth Amendment because although the government did not interfere with the defendant's possession of the documents, it did interfere with his *sole* possession of them and in turn, diminished the private nature of that information. *Id.* at 703-04.

The district court in *Jefferson* reached this conclusion in part by relying on *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), where the Supreme Court explained that Federal Rule of Criminal Procedure 41, which governs the issuance of search warrants, was broad enough to "include seizures of intangible items" including the pulses of a telephone dial that can be captured by a pen register. *New York Telephone Co.*, 434 U.S. at 170; *see also Jefferson*, 571 F. Supp. 2d at 702-03. The Supreme Court found that Rule 41 could encompass "a 'search' designed to ascertain the use which is being made of a telephone suspected of being

employed as a means of facilitating a criminal venture and the 'seizure' of evidence which the 'search' of the telephone produces." *New York Telephone Co.*, 434 U.S. at 169. That is, by making a copy of the pulses of the telephone, a pen register "seized" those pulses for later analysis by the government, which was a separate Fourth Amendment "search."[3]

Even Professor Kerr, whom the magistrate relied upon in finding that the government's review and "search" of information was the relevant Fourth Amendment event, has clarified in later literature that copying data is a "seizure" under the Fourth Amendment. In a 2010 article, he noted that in the article specifically referenced by the magistrate below, he previously argued "that mere copying" was not a Fourth Amendment Seizure. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. at 704 (citing Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. at 557-62; *see also Mag. Opinion*, 2014 WL 1661004, at *6 (citing *Searches and Seizures in a Digital World*). But Professor Kerr later came to recognize that his "prior approach was wrong" because it "did not recognize the importance of access to data in the regulation of government evidence collection." Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. at 704.

Instead, "[w]hen the government makes an electronic copy of data, it obtains possession of the data that it can preserve for future use," which "serves the traditional function regulated by the seizure power: it freezes whatever information is copied, preserving it for future access by government investigators." *Id.* at 711. Ultimately, "generating an electronic copy is no different

[3] Similarly, in *United States v. Comprehensive Drug Testing, Inc.*, the Ninth Circuit repeatedly noted that the government had improperly "seized" data when it copied computer files outside the scope of a search warrant. *See, e.g.*, 621 F.3d 1162, 1166 (9th Cir. 2010) (en banc) (per curiam) ("the government *seized* and promptly reviewed" computer files) (emphasis added); *see also United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085, 1093 (9th Cir. 2008) (noting agents "copied" computer files "and removed the copy for later review at government offices").

from controlling access to a house or making an arrest: it ensures that the government has control over the person, place, or thing that it suspects has evidentiary value." *Id.* at 712. And foreshadowing the situation here, "a government request to an ISP to make a copy of a suspect's remotely stored files" would also be a "seizure" because the government's request "changes the path of the communication of contents that would have occurred in the ordinary course of business," in effect "freez[ing] the scene at the government's request, preserving evidence for government's use." *Id.* at 724.[4]

Here, a crucial Fourth Amendment event occurred before the government reviewed the emails: once Microsoft copied the emails, they were "seized" under the Fourth Amendment.[5] As one magistrate judge recently noted in the context of a government request to obtain emails from an online email provider, "when a copy is made, 'the person loses exclusive rights to the data,' and it is at that time that the owner's property interest in the e-mail is affected." *In re Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*,

---

[4] Professor Kerr's example specifically referenced a situation where the government requested a copy be made "while the government obtains a warrant," but his conclusion would be true even where, as here, the government had already obtained a warrant asking for a copy of the contents. *See* Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. at 723. Under either scenario, Microsoft is "freez[ing] the scene at the government's request, preserving evidence for government use" and thus "seizing" data under the Fourth Amendment. *Id.* at 724.

[5] As noted earlier, the magistrate ignored the fact that *Microsoft's* review of the emails, as the agent of the government, is also a "search" because it intrudes on the customer's expectation of privacy in his electronic communications. *See United States v. Bennett*, 709 F.2d 803, 805 (2d Cir. 1983) (Fourth Amendment applies to searches by private actors "acting as an instrument or agent of the Government"); *Warshak*, 631 F.3d at 288 (user has expectation of privacy in the contents of emails stored with an email provider online). Like the "seizure" of the emails, this "search" occurs before the government agent's direct "search" of the emails and could potentially take place abroad. *See* Declaration of Redacted, Doc. No. 16 at ¶¶ 3-5, *see also* Microsoft's Objection to the Magistrate's Order at 7, n. 4. To the extent the magistrate differentiated between the review of the emails by government agents as opposed to Microsoft employees, it never determined whether Microsoft employees in Ireland would be conducting the "search" abroad.

--- F. Supp. 2d ---, 2014 WL 1377793, at *3 (D.D.C. Apr. 7, 2014) (quoting Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. at 703); *see also United States v. Vilar*, 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007) (unpublished), *remanded on other grounds* 729 F.3d 62 (2d Cir. 2013) ("'it is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head,' as computer hardware is seized from a suspect's premises before its content is known and then searched at a later time.") (quoting *In re Search of 3817 W. W. End, First Floor Chicago, Illinois 60621*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004)).

The magistrate failed to consider the "seizure" here and instead skipped ahead to the government agent's review of the emails in the U.S., which it believed to be the relevant Fourth Amendment event. But ignoring the "seizure" that occurs when sensitive and personal data is copied by the government threatens to leave electronic data without constitutional protection. If the act of copying and collecting data is irrelevant under the Fourth Amendment, there is nothing to prohibit the government from copying or "seizing" the contents of any computer or hard drive or "cloud" storage facility it wants without a search warrant, provided it later obtains a warrant to "search" the collected data. This "collect first" approach poses a grave risk to privacy as it becomes easier and faster for the government to copy the large amount of digital data stored both on individuals' personal electronic devices and remotely in the "cloud." As the recent NSA controversy has shown, the government has been more than willing to collect large reams of digital data without probable cause, claiming that it only needs individualized suspicion when it wishes to query or search the records it collects.

The Fourth Amendment was intended to prevent this kind of indiscriminate data collection and was "a response to the English Crown's use of general warrants, which often

allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown." *Ashcroft v. Al-Kidd*, 131 S.Ct. 2074, 2084 (2011). But "if copying is not a seizure, it is outside the scope of the Fourth Amendment's reasonableness requirements and is an activity which can be conducted at will, requiring neither the justification of a warrant nor an exception to the warrant requirement." Susan Brenner and Barbara Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L.Rev. 39, 113 (2002).

To ensure the Fourth Amendment survives in the 21st century, this Court should find that the government's request to Microsoft to copy the contents of emails is a "seizure."

II. A Ruling that a Warrant Seeking the Contents of Electronic Communications under the Stored Communications Act Does Not Incorporate all of the Traditional Warrant Requirements Results in the Selective Application of Fourth Amendment Standards to Digital Data.

It is undisputed that a U.S. magistrate has no authority to issue a warrant to either seize or search data stored abroad. *See United States v. Odeh*, 552 F.3d 157, 169 (2d Cir. 2008) (noting majority of Supreme Court justices in *United States v. Verdugo–Urquidez*, 494 U.S. 259, 278-79, 297 (1990) "endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches"); *see also Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1944) ("With very few exceptions, United States district judges possess no extraterritorial jurisdiction.").

Had the magistrate correctly focused on the "seizure" that must take place before the government could "search" or review the emails, it would have recognized the warrant was defective since it permitted the government to "seize" data stored in another country. The magistrate evaded this jurisdictional barrier by finding that an order to disclose the contents of communications under the SCA" is a "hybrid" judicial order that is part warrant and part subpoena, even though the SCA uses the word "warrant" and refers to procedures governing the

issuance of a "warrant." *Mag. Opinion*, 2014 WL 1661004, at *5. As Microsoft ably explains in its brief, this argument ignores the text of the SCA and Congress' intent in using the word "warrant." *See* Microsoft's Objection to Magistrate's Order at 13-19.

Fundamentally, the magistrate's decision undermines the important constitutional and statutory protections given to data and radically reimagines what search warrants look like in the digital world. "[I]t is a 'cardinal rule of statutory construction' that, when Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'" *F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)); *see also Morissette v. United States*, 342 U.S. 246, 263 (1952). The "cluster of ideas" associated with a search warrant are well known; a warrant must be based on probable cause, supported by a sworn testimony or affidavit and must particularly describe the place to be searched and the items to be seized. *See Groh v. Ramirez*, 540 U.S. 551, 557 (2004). And as explained above, a U.S. judge cannot approve of a warrant purporting to search or seize items or data stored abroad. *See Odeh*, 552 F.3d at 169; *Weinberg*, 126 F.2d at 1006.

The way these "cluster of ideas" are incorporated into the SCA is by Congress' use of the word "warrant" in 18 U.S.C. § 2703(a). The SCA does not specifically mention the word "probable cause" or "particularity" because these ideas are subsumed into the word "warrant." While the magistrate recognized that the word "warrant" in the SCA "cabins the power of the government by requiring a showing of probable cause not required for a subpoena," it rejected the idea that the territorial limitations on warrants applied to warrants issued under the SCA. *Mag. Opinion*, 2014 WL 1661004, at *5. In effect, the magistrate selectively chose which ideas associated with a warrant it believed were included by Congress when it used the word "warrant"

in § 2703(a). But courts are not at liberty to rewrite statutes in order to achieve what they believe Congress intended. *See Lewis v. City of Chicago, Ill.*, 560 U.S. 205, 215 (2010). When the text of the statute is clear and in the "absence of contrary direction" by Congress, the use of a legal term of art in a statute "may be taken as satisfaction with widely accepted definitions, not as a departure from them." *Morissette*, 342 U.S. at 263.

Beyond this specific case, interpreting "warrant" under the SCA to only incorporate some of the "cluster of ideas" associated with search warrants means that the protection of digital data will depend on the whims of the specific judge reviewing the government's request. For example, the warrant at issue here requests all emails stored in the account, including sent emails, from the time the account was opened to the present. *See* Attachment C to Search and Seizure Warrant, 13-mag-2814. This request fails the particularity requirement of the Fourth Amendment. *See, e.g., In re Search of Info. Associated with [Redacted]@mac.com*, 2014 WL 1377793, at *5 (finding warrant seeking to seize all emails unconstitutional because government failed to demonstrate probable cause to search all messages); *see also In re Applications for Search Warrants for Info. Associated with Target Email Address*, 2012 WL 4383917, at *9 (D. Kan. Sept. 21, 2012) (unpublished) (warrant seeking "content of every email or fax sent to or from the accounts" similar "to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant.").

Under the magistrate's own logic, a court could simply believe the particularity requirement was not incorporated into the SCA because the statute never mentions the word explicitly. This selective incorporation leads to inconsistent application of a crucial piece of

constitutional and statutory protection intended to safeguard various forms of important and sensitive personal electronic data throughout the country. In the absence of any ambiguity, the magistrate had to apply all of the concepts associated with the warrant requirement, including extraterritoriality.

III. Since Foreign Searches Must Be "Reasonable," the Government Must Comply With Irish Law and the MLAT Process to Obtain the Emails.

A foreign search or seizure of a U.S. citizen[6] by the U.S. government must be "reasonable" under the Fourth Amendment. *Odeh*, 552 F.3d at 171. To determine "reasonableness," courts must look at the "totality of the circumstances" and balance the "degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* at 172 (quoting *Samson v. California*, 547 U.S. 843, 848 (2006) (quotations omitted)).

Courts deciding these questions have generally found international searches and seizures to be "reasonable" if they satisfy the law of the country in which the search is executed. *See, e.g., United States v. Peterson*, 812 F.2d 486, 491 (9th Cir. 1986) (Kennedy, J.) ("local law" of the foreign country where the search occurred "governs whether the search was reasonable"). For example, in *Odeh*, the Second Circuit found the intrusiveness of a search of a U.S. citizen's home in Kenya was "minimized" in part because U.S. agents searched the home "with the assistance of Kenyan authorities, pursuant to what was identified as a 'Kenyan warrant

[6] It is not clear from the record whether the email account holder is a U.S. citizen, although that was a fact the magistrate needed to resolve in order to assess the reasonableness of the government's request.

authorizing [a search].'" *Odeh*, 552 F.3d at 174 (quoting *United States v. Bin Laden*, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000)). Other courts have reached the same result.[7]

There are important policy reasons why compliance with international law plays a large role in assessing the "reasonableness" of a foreign search. First, it limits the reach of U.S. law and U.S. government actors, preserving the "presumption that United States law governs domestically but does not rule the world." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454 (2007). Second, demanding compliance with international law ensures that the United States respects the sovereignty of other countries and complies with its international legal obligations. *See F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164 (2004) (American laws should be interpreted "to avoid unreasonable interference with the sovereign authority of other nations.").

When it comes to digital data, these concerns are especially important. The rise of global "cloud" computing services means that it is increasingly common for American companies to service users and store data in multiple places across the world. Each of those countries may have their own data protection laws in place to safeguard data and many impose more stringent legal protections than those in American law. Therefore, the MLAT process is the longstanding

[7] *See United States v. Stokes*, 726 F.3d 880, 893 (7th Cir. 2013) *cert. denied*, 134 S.Ct. 713 (2013) (finding foreign search reasonable when executed "pursuant to a valid Thai search warrant"); *United States v. Juda*, 46 F.3d 961, 968 (9th Cir. 1995) ("a foreign search is reasonable if it conforms to the requirements of foreign law"); *United States v. Flath*, 845 F. Supp. 2d 951, 960 (E.D. Wis. 2012) (search "conducted pursuant to a Belizean warrant" reasonable); *United States v. Castro*, 175 F. Supp. 2d 129, 134 (D.P.R. 2001) (upholding use of wiretaps, even though they would be illegal in the United States, because they complied with the law in the Dominican Republic); *see also Vilar*, 2007 WL 1075041, at *54 ("foreign search is reasonable if it meets the requirements of the law of the nation in which the search is executed, as long as those requirements do not permit conscious-shocking conduct.").

and accepted way in which countries are able to access evidence stored in another country without violating that country's specific laws.

Once the government was informed by Microsoft that the emails it sought were stored in Ireland, it should have resorted to the MLAT process rather than attempt to work around it by having the magistrate issue an order authorizing a seizure and search beyond its jurisdiction. The government should have recognized that compliance with the law of the country in which the data is stored was a crucial part of making the foreign seizure and search "reasonable."

Unfortunately, the magistrate accepted the government's arguments, believing that construing "warrant" in the SCA as a genuine warrant would unduly burden law enforcement, simply because "one commentator" – Professor Kerr – observed the MLAT "process generally remains slow and laborious." *Mag. Opinion*, 2014 WL 1661004, at *8 (quoting Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Penn. L.Rev. 373, 409 (2014) (quotations omitted)). The magistrate not only failed to inquire into whether the MLAT process *actually* is "slow and laborious," it never even pointed to any potential obstacles in the U.S.-Irish MLAT itself. *See Mag. Opinion*, 2014 WL 1661004, at *8-9. Instead, it quoted from U.S. MLATs with Canada and the United Kingdom to explain why the MLAT process could be burdensome for the government.

It should take more than speculation to relieve the government of its obligation to comply with its international treaties. Since "warrant" in the SCA actually means "warrant," it was ultimately the government's burden to comply with the U.S.-Irish MLAT – which requires the U.S. government to comply with Irish law – in order for the seizure of the emails in Ireland to be "reasonable." The magistrate's decision improperly permits the U.S. to subvert this process, rendering the seizure of the emails necessarily "unreasonable."

CONCLUSION

The magistrate's decision undermines the constitutional and statutory protections for the data that captures people's most detailed and intimate communications, leads to selective and inconsistent enforcement of the statute that protects these communications from the government, and threatens international comity. This Court should reverse the magistrate's decision.

Dated: June 12, 2014

Respectfully submitted,

Hanni M. Fakhoury (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Fax: 415-436-9993
Email: hanni@eff.org