

**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

Case No. 13-MAG-2814

**Memorandum of Law in Support of
Motion by Apple Inc. and Cisco Systems, Inc. to Participate as *Amicus Curiae*
and Microsoft Inc.'s Motion to Vacate Search Warrant**

Marc J. Zwillinger (*Pro Hac Vice Pending*)
Kenneth M. Dreifach (SBN 2527695)
ZWILLGEN, PLLC
232 Madison Avenue, Suite 500
New York, NY 10016
(646) 362-5590 (tel)
(202) 706-5298 (fax)

*Counsel for Apple Inc. and Cisco Systems,
Inc.*

TABLE OF CONTENTS

- I. INTEREST OF *AMICI CURIAE*2
- II. BACKGROUND3
- III. ARGUMENT.....4
 - A. The Magistrate Ignored Conflicts of Laws and International Comity In Dismissing the MLAT Process.....5
 - 1. ECPA Does Not Provide a Basis to Forego a Comity Analysis.....7
 - 2. The Magistrate Failed to Consider Possible Conflicts with Foreign Law Which Have Substantial Impact on Providers.....8
 - 3. The Magistrate Improperly Rejected the MLAT Process in All Cases 11
 - B. Allowing the Government to Avoid the MLAT Process in All Cases Will Place Providers at Greater Risk of Sanction in Foreign Countries 12
 - C. Requiring Government to Use the MLAT Process Has Ancillary Benefits 13
- IV. CONCLUSION 14

TABLE OF AUTHORITIES

CASES	PAGE(S)
<i>Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa</i> , 482 U.S. 522 (1987)	6, 7
<i>DeGeorge v. U.S. Dist. Court for Cent. Dist. of California</i> , 219 F.3d 930 (9th Cir. 2000)	12
<i>EEOC v. Arabian Am. Oil Co.</i> , 499 U.S. 244 (1991)	7
<i>Hartford Fire Insurance Co. v. California</i> , 113 S.Ct. 2891 (1993).....	7
<i>Hilton v. Guyot</i> , 159 U.S. 113 (1895)	6
<i>In re French</i> , 440 F.3d 145 (4th Cir. 2006)	7
<i>In re Maxwell Commc'n Corp. plc by Homan</i> , 93 F.3d 1036 (2d Cir. 1996)	7
<i>Lauritzen v. Larsen</i> , 345 U.S. 571 (1953)	10
<i>Linde v. Arab Bank, PLC</i> , 706 F.3d 92 (2d Cir. 2013)	6
<i>Morrison v. Nat'l Austl. Bank Ltd.</i> , 130 S.Ct. 2869 (2010).....	7
<i>Murray v. The Schooner Charming Betsy</i> , 6 U.S. 64 (1804)	10
<i>Smith v. United States</i> , 507 U.S. 197 (1993)	7
<i>Soci�t� Nationale Industrielle A�rospatiale v. U.S. Dist. Court of Iowa</i> , 482 U.S. 522 (1987)	6
<i>Suzlon Energy v. Microsoft Corp.</i> , 671 F.3d 726 (9th Cir. 2011)	12

CASES, CONTINUED	PAGE(S)
<i>United States v. Vetco Inc.</i> , 691 F.2d 1281 (9th Cir. 1981)	7
<i>Zheng v. Yahoo! Inc.</i> , No. C-08-1068 MMC, 2009 WL 4430297 (N.D. Cal. 2009)	5, 8
 STATUTES AND RULES	
18 U.S.C. § 2701	3, 4, 11
18 U.S.C. § 2703	12, 14
18 U.S.C. § 2711(4)	8
18 U.S.C. § 3292	12
Electronic Communications Privacy Act (“ECPA”)	<i>passim</i>
Fed. R. Crim. P. 41	3, 4
 LEGISLATIVE MATERIALS	
H.R. Rep. No. 95-647 (1986)	8
 TREATIES AND INTERNATIONAL MATERIALS	
Code Pénal [C.Pén.] art. 314 (Belg.)	8
Code Pénal [C. Pén.] art. 226 (Fr.)	9
Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185	9, 12
European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, art. 8, Nov.1950, E.T.S. 5	8
Directive 2000/36/EC of the European Parliament and of the Council of 23 June 2000 on the Processing of Personal Data and the Protection of Privacy in the Electronic .Communications Sector and Repealing Council Directive 97/66/EC, 2002 O.J. (L 201) 37-47	9
Law on Networks and Electronic Communications Services (Luxembourg) (<i>Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques</i>), <i>Mémorial</i> , A-073, June 7, 2005, available at http://www.legilux.public.lu/leg/a/archives/2005/0730706/0730706.pdf ...	9
<i>Lei No.</i> [Law No.]12.965, de 23 Abril de 2014, <i>Col. Leis Rep. Fed. Brasil</i> , [Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet)]	9, 10

Mutual Legal Assistance Agreement with the European Union art. 7,
 U.S.-E.U. June 25, 2003, Treaty Doc. 109-13..... 12

Nomos (2006:3471) Protection of Personal Data and Privacy in the Electronic
 Telecommunications Sector and Amendment of Law 2472/1997, 2006 A:4 (Greece) 9

Penal Code Section 197 (Spain) 9

Prawo Telekomunikacyjne [Poland Telecommunications Act art. 159],
Dz. U. z 2000 Nr 171, poz. 1800, available at
<http://isap.sejm.gov.pl/Download?id=WDU20140000243&type=2>..... 9

Restatement (Third) of Foreign Relations Law § 101 (1987) 6

Restatement (Third) of Foreign Relations Law § 403 (1987) 6, 7

Sähköisen viestinnän tietosuojalaki [Act on Data Protection in Electronic Communications] Act
 No. 516/2004 of 16 June 2004 (Finland)..... 9

Treaty Between the Gov’t. of the United States of America and the Gov’t. of Ireland on
 Mutual Legal Assistance in Criminal Matters, U.S.–Ir., Jan. 18, 2001, T.I.A.S. No. 13137 5

OTHER AUTHORITIES

Apple, Report on Government Information Requests (2013) *available at*
<http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf> 2

Eric Pfanner, *Google Faces a Different World in Italy*, N.Y. Times (Dec. 13, 2009),
http://www.nytimes.com/2009/12/14/technology/internet/14google.html?pagewanted=all&_r=0
 3

Facebook Operational Guidelines: Information for Law Enforcement Authorities
<https://www.facebook.com/safety/groups/law/guidelines/> (last visited June 12, 2014). 13

Federal Bureau of Investigation—International Operations,
http://www.fbi.gov/about-us/international_operations (last visited June 12, 2014). 11

Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*,
 Queen Mary School of Law Legal Studies Research Paper No. 74/2011 (Nov. 14, 2011),
<http://dx.doi.org/10.2139/ssrn.1781067> 9

Kashmir Hill, *The Downside of Being a Google Executive*, Forbes (Sept. 27, 2012),
<http://www.forbes.com/sites/kashmirhill/2012/09/27/the-downside-of-being-a-google-executive/> 3

Partnerships Pay Dividends at Nordic Outpost, FBI.gov,
<http://www.fbi.gov/news/stories/2013/december/partnerships-pay-dividends-at-copenhagen-legal-attache/partnerships-pay-dividends-at-copenhagen-legal-attache> (last visited June 13, 2014)..... 11

Orin S. Kerr, *The Next Generation Communications Privacy Act*,
 162 U. Pa. L. Rev. 373 (2014)..... 13

Paulo Marcos Rodriguez Brancher & Douglas Cohen Moreira, *Brazilian Superior Court of Justice decision and the disclosure of Gmail data for investigation*, Lexology (Apr. 29, 2013),
available at <http://www.lexology.com/library/detail.aspx?g=793d848f-5877-4675-9336-aa28eec3d971> (last visited June 12, 2014) 9

Reuters, *Top Google Executive in Brazil Faces Arrest Over Video*,
 N.Y. Times (Sept. 25, 2012), <http://www.nytimes.com/2012/09/26/business/global/top-google-executive-in-brazil-faces-arrest-over-video.html> 3

Robin Wauters, *Yahoo Fined By Belgian Court For Refusing To Give Up E-mail Account Info.*,
 TechCrunch (Mar. 2, 2009), <http://techcrunch.com/2009/03/02/yahoo-fined-by-belgian-court-for-refusing-to-give-up-e-mail-account-info/> 13

U.S. Dept. of Justice, FY 2015 Budget Request, Mutual Legal Assistance Treaty Process Reform,
available at <http://www.justice.gov/jmd/2015factsheets/mut-legal-assist.pdf> 12

Apple Inc. (“Apple”) and Cisco Systems, Inc. (“Cisco”) (collectively “*Amici Curiae*”) submit this memorandum of law in support of: (1) its motion for leave to participate as *amicus curiae* in Case No. 13-MAG-2814 and (2) of Microsoft’s Objections to the Magistrate’s Order denying Microsoft’s Motion to Vacate Search Warrant in the above-referenced case.

In rejecting Microsoft’s motion to vacate the search warrant, the Magistrate erred by failing to consider the conflicting obligations under foreign and domestic law that arise when courts order providers to produce data about foreign users stored in foreign countries. By omitting this evaluation—and by dismissing the Mutual Legal Assistance Treaty (“MLAT”) process out of hand with no factual findings regarding the Irish MLAT at issue—the Magistrate placed the burden of reconciling conflicting international laws squarely on U.S. providers. Yet the government, not private parties, is best suited to navigate complex sovereignty issues, especially those caused by a novel extraterritorial application of U.S. law. And it has chosen to use the MLAT process to strike the correct balance. By disregarding that process, and the laws of the country where data is stored, the Magistrate’s analysis places providers and their employees at significant risk of foreign sanctions, and threatens a potential loss of customer confidence in U.S. providers generally. It also encourages foreign law enforcement to take reciprocal actions by using equivalent foreign laws to require production of data stored in the United States, despite disclosure prohibitions in U.S. law.

Rather than simply analyzing whether the recipient has “information in its possession and control, regardless of the location of that information,” Order at 12, this Court should instead find that the Electronic Communications Privacy Act (“ECPA”) was not intended to apply extraterritorially, and that principles of comity and reciprocity require the Government to comply with the MLAT process when foreign user data is stored abroad.

I. INTEREST OF *AMICI CURIAE*

Apple is committed to bringing the best user experience and highly secure hardware, software and servers to its customers around the globe. The Company's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software, and services to provide customers products and solutions with superior security, ease-of-use, seamless integration, and innovative design. In addition to selling iPhones, iPads, and personal computers, Apple also offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups and more, keeping everything up to date and available to customers on whatever device they are using. To offer these services Apple relies on a worldwide network of computer servers to provide its users with fast, efficient services. Because some of those servers are located outside the United States, Apple is subject to, or may become subject to, various foreign laws regarding data transfer. At the same time, Apple is committed to transparency and enabling users to clearly understand how it handles their personal information. Apple strives to provide straightforward disclosures regarding when it is compelled to comply with legal process around the world.¹

Cisco is the worldwide leader in providing infrastructure for the Internet. It also offers various services managed from data centers operated by Cisco which allow its customers to use, among other things, remote data centers, wireless internet services, internet security services, and collaboration tools which drive efficiency in their business. It too relies on servers located outside the United States, and is subject to, and must comply with, various foreign laws regarding data transfer. The confidence of customers in Cisco's ability to operate within the requirements of those laws is important to its business.

¹ See e.g., Apple, Report on Government Information Requests (2013), available at <http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf>.

The foreign laws to which *Amici* are subject often conflict with U.S. law, placing *Amici* and other providers in positions where compliance with one law may lead to a serious violation of another. Because of such conflicts, other providers have already faced potential criminal sanctions abroad.² The Magistrates' failure to address issues of international comity, reciprocity and to properly consider the ramifications of applying ECPA extraterritorially, makes it difficult for Apple to navigate overlapping international laws.³ Apple and Cisco should be granted leave to participate as *Amici* in these proceedings, and the Magistrate's analysis should be rejected.

II. BACKGROUND

The Government served Microsoft with a search warrant directing it to produce the contents of a customer's email account. Microsoft determined that it had stored the responsive email content on a server in Dublin, Ireland, which was leased and operated by its wholly-owned subsidiary. Rather than produce the email content, Microsoft produced only non-content data stored in the United States and moved to quash the warrant to the extent it required Microsoft to conduct an extraterritorial search at the government's behest. Order at 5.

The Magistrate denied Microsoft's motion, upheld the warrant and commanded Microsoft to produce data stored in Ireland. In doing so, the Magistrate held that the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* creates a special "SCA warrant" that is a hybrid between a Rule 41 Warrant and a subpoena.⁴ *Id.* at 12. The Magistrate treated the "warrant" as a subpoena and held that Microsoft had "possession, custody, or control" over

² See e.g., Reuters, *Top Google Executive in Brazil Faces Arrest Over Video*, N.Y. Times (Sept. 25, 2012), <http://www.nytimes.com/2012/09/26/business/global/top-google-executive-in-brazil-faces-arrest-over-video.html>; Eric Pfanner, *Google Faces a Different World in Italy*, N.Y. Times (Dec. 13, 2009), http://www.nytimes.com/2009/12/14/technology/internet/14google.html?pagewanted=all&_r=0.

³ Kashmir Hill, *The Downside of Being a Google Executive*, Forbes (Sept. 27, 2012), <http://www.forbes.com/sites/kashmirhill/2012/09/27/the-downside-of-being-a-google-executive/>.

⁴ Apple takes no position on the hybrid warrant issue, or whether the territorial limitations of Rule 41 apply to search warrants that call for content from electronic communication service providers.

information stored in Ireland, and must produce the email content. *Id.* at 13, 18. The Magistrate examined ECPA's structure and legislative history and found it trumped Rule 41's limitations, erroneously concluding that Congress intended the SCA to apply extraterritorially because it was "unlikely" to have intended for the Government to comply with the MLAT process. *Id.*

The Magistrate's decision did not mention international law, possible conflicts of laws, or the burden on providers of complying with conflicting legal regimes. The Magistrate made no findings regarding (1) whether there were any treaties between Ireland and the United States; (2) whether the Irish government was slow to respond to U.S. law enforcement requests; or (3) whether the Irish government would refuse this request.

III. ARGUMENT

The Magistrate's analysis improperly ignores the interplay of foreign and domestic laws when determining whether the government can use a warrant to require a U.S. company to produce *data about a non-U.S. citizen when the data is held by a foreign subsidiary and stored in a foreign location*. Rather than ignoring foreign law, courts should examine possible conflicts of law, inquire into the weight of the U.S. government's interest in each case, and determine whether those interests are sufficiently compelling to outweigh principles of international law, comity, sovereignty, and reciprocity, such that the government may circumvent U.S. treaty obligations. The Magistrate's failure to include a more thorough international law and comity analysis has serious consequences and, if followed by other courts, is likely to put Apple and other providers in the untenable situation of being forced to violate one nation's laws to comply with another.

The Magistrate's error is compounded by the weak reasoning underlying his decision to apply ECPA extraterritorially. ECPA contains no express statement about extraterritoriality. It

makes no reference to seeking data abroad. Instead of relying on ECPA's plain text and canons of construction that weigh against extraterritorial application of laws, or existing case law finding no extraterritorial application (*Zheng v. Yahoo! Inc.*, No. C-08-1068 MMC, 2009 WL 4430297 (N.D. Cal. 2009)), the Magistrate found that Congress was "unlikely" to have intended to require law enforcement to use the MLAT process because, (1) it is sometimes slow; (2) member states may refuse requests; and (3) it is unavailable when no treaty is in place. *Id.* at 19-21.

The Magistrate further justified his decision to compel Microsoft to produce data stored abroad based on speculation about how U.S. law enforcement efforts could be thwarted by users and providers in the future. The Magistrate considered activities that did not occur here: whether users can give false addresses to providers to effectuate foreign storage, what would happen if a nation refuses an MLAT request, and what happens when no treaty exists. Order at 18-20. Rather than speculating and using ECPA to reject the MLAT process unilaterally, this Court should evaluate the MLAT with Ireland,⁵ the relevant provisions of Irish data protection law, and determine whether the MLAT process was appropriate for this case.

A. The Magistrate Ignored Conflicts of Laws and International Comity In Dismissing the MLAT Process.

In determining that ECPA applies to the production of data stored abroad in all cases, the Magistrate ignored the realities of cross-border criminal prosecutions, which, by definition, involve interests between sovereigns, and allowed the government to obtain data without considering the impact on international law. The Magistrate's focus on ECPA without reference to foreign law is contrary to the Supreme Court's admonition in *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa*, 482 U.S. 522, 546 (1987) that, "in

⁵ Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, U.S.-Ir., Jan. 18, 2001, T.I.A.S. No. 13137, available at <http://www.state.gov/documents/organization/129536.pdf>.

supervising pretrial proceedings ... American courts should ... take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality **or the location of its operations**, and for any sovereign interest expressed by a foreign state.” (emphasis added). When determining whether to apply domestic law to activities in a foreign country, courts apply a comity analysis. “‘Comity,’ in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protection of its laws.” *Hilton v. Guyot*, 159 U.S. 113, 163-64 (1895). See also, Restatement (Third) of Foreign Relations Law § 101 (1987).

The comity analysis is a case-by-case, fact intensive inquiry. “International comity calls for more than an examination of only *some* of the interests of *some* foreign states. Rather, as the Supreme Court explained in *Aérospatiale*, “‘the concept of international comity’ requires a ‘particularized analysis of the respective interests of the foreign nation and the requesting nation.’” 482 U.S. at 543–44 (footnote omitted). Put another way, the analysis involves weighing *all* the relevant interests of *all* of the nations affected by the court's decision. *Linde v. Arab Bank, PLC*, 706 F.3d 92, 111-12 (2d Cir. 2013).

Resolving conflicts in law also require balancing the interests of nations. Courts apply the factors in Restatement (Third) of Foreign Relations Law § 403 (1987), which look to “the extent to which the activity takes place within the territory” of the regulating state, “the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated,” “the extent to which other

states regulate such activities” or “may have an interest in regulating [them],” the “likelihood of conflict with regulation by another state,” and “the importance of regulation to the regulating state.” *Hartford Fire Ins.*, 509 U.S. at 799 (Scalia, J., dissenting); *In re French*, 440 F.3d 145, 152-53 (4th Cir. 2006) (applying the factors outlined in the Restatement); *Maxwell Commc'n Corp. plc v. Societe Generale PLC (In re Maxwell Commc'n Corp.)*, 93 F.3d 1036, 1047–48 (2d Cir.1996). Courts have also considered “whether substantially equivalent alternate means for obtaining the requested information are available,” including “obtaining consents to the disclosure, issuance of letters rogatory, use of treaty procedures.” *United States v. Vetco Inc.*, 691 F.2d 1281, 1288-91 (9th Cir. 1981). The Magistrate’s opinion omits such balancing, and therefore leads to the incorrect conclusion.

1. ECPA Does Not Provide a Basis to Forego a Comity Analysis

ECPA alone provides no basis to forego a comity analysis. It is a “longstanding principle of American law ‘that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.’ ” *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) (“*Aramco*”). That presumption expresses a canon of construction rooted in the “commonsense notion that Congress generally legislates with domestic concerns in mind.” *Smith v. United States*, 507 U.S. 197, 204 n. 5 (1993). The canon “serves to protect against unintended clashes between our laws and those of other nations which could result in international discord,” *Aramco*, 499 U.S. at 248, 111 S.Ct. 1227, and “preserv[es] a stable background against which Congress can legislate with predictable effects.” *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 261 (2010).

ECPA's plain language gives no reason to ignore this presumption.⁶ ECPA contains no express statement that it has extraterritorial application. It excludes foreign governments from its definition of governmental entities.⁷ It consistently and exclusively refers only to process issued by U.S. courts or U.S. law enforcement. And, its legislative history is consistent with the conclusion that no parts of ECPA were intended to have extraterritorial effect. *See* H.R. Rep. No-95-647 at 32-33 (1986) (stating that the criminal prohibitions of ECPA are intended to apply to actions "within the territorial United States"). Accordingly, ECPA should not be read to give U.S. law enforcement a unilateral right to seek data stored abroad without regard to privacy and legal protections afforded to that data in the nations where it is stored.

2. The Magistrate Failed to Consider Possible Conflicts with Foreign Law Which Have a Substantial Impact on Providers.

The Magistrate's opinion does not consider a key issue in the comity analysis: whether foreign law conflicts with United States law. By interpreting ECPA to override foreign law in *all* cases, the Magistrate's decision ignores issues faced by providers, like Apple, who often find themselves in true conflict of laws scenarios. Providers like *Amici* with a global customer base who utilize cloud computing services regularly face conflicting laws when U.S. law enforcement demands the production of data stored outside the United States.

Like the United States, other countries value the secrecy of communications and some consider such privacy a fundamental human right. *See, e.g.* Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by

⁶ *See Zheng v. Yahoo! Inc.*, 2009 WL 4430297, at *2-3 (N.D. Cal. September 18, 2010) (finding no extraterritorial application).

⁷ 18 U.S.C. § 2711(4), defining "governmental entity" to mean "a department or agency of the United States or any State or political subdivision thereof."

Protocols Nos. 11 and 14, art. 8, Nov. 1950, E.T.S. 5.⁸ The European Union’s Directive on processing of personal data and protection of privacy in the electronic communications sector (“e-Privacy Directive”) (Directive 2002/58/EC, Repealing Directive 97/66/EC, 2002 O.J. (L 201) 37-47) requires EU member countries to provide protections for electronic communications in their laws and all EU member countries have such laws.⁹ In response to the recent revelations about U.S. surveillance activities through the Snowden leaks, some countries are considering or have enacted laws specifically designed to a) address the long-standing difficulties foreign governments face when seeking electronic communications data stored in the United States and subject to U.S. law¹⁰; and b) to ensure that information about their own citizens is protected by their legal standards even if the information is collected by a company located abroad and the data is stored abroad. *See* Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12.965¹¹; *see also* Professor Ian Walden, *Accessing Data in the Cloud: The*

⁸ *See also, e.g., Code Pénal [C.Pén.] art. 314 (Belg.) (“Wiretapping of Private Communications”—Belg. Criminal Code protecting privacy of communications); Sähköisen viestinnän tietosuojalaki [Act on Data Protection in Electronic Communications] Act No. 516/2004 of 16 June 2004 (Finland); Code Pénal [C. Pén.] art. 226 (Fr.) (France Criminal Code relating to violations of privacy of communications); Nomos (2006:3471) Protection of Personal Data and Privacy in the Electronic Telecommunications Sector and Amendment of Law 2472/1997, 2006 A:4 (Greece); Law on Networks and Electronic Communications Services (Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques), Mémorial, A-073, June 7, 2005, available at <http://www.legilux.public.lu/leg/a/archives/2005/0730706/0730706.pdf> (Luxembourg Law of 2005 Privacy in Electronic Communications); Prawo Telekomunikacyjne [Poland Telecommunications Act], Dz. U. z 2000 Nr 171, poz. 1800, available at <http://isap.sejm.gov.pl/Download?id=WDU20140000243&type=2> (Article 159 Polish Act of 16 July 2000 on Telecommunications Law, published in Journal of Laws (Dziennik Ustaw) No 171, item 1800 with subsequent amendments; Spain Penal Code Section 197 (Prohibiting interception of communications).*

⁹ Signatories to the Council of Europe’s Convention on Cybercrime, which include the United States, have also been urged to adopt protections for electronic communications similar to those that exist in the United States. *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185 at Chap. 2. Nothing in this brief is intended to suggest that any laws or Directives cited herein apply specifically to Apple’s or Cisco’s activities.

¹⁰ *See e.g.,* Paulo Marcos Rodriguez Brancher and Douglas Cohen Moreira, *Brazilian Superior Court of Justice decision and the disclosure of Gmail data for investigation*, Lexology (Apr. 29, 2013), available at <http://www.lexology.com/library/detail.aspx?g=793d848f-5877-4675-9336-aa28eec3d971> (last visited June 12, 2014).

¹¹ Unofficial English translation, available at <http://diretorio.fgv.br/sites/diretorio.fgv.br/files/Marco%20Civil%20ingl%C3%AAAs.pdf>.

Long Arm of the Law Enforcement Agent, University of London, UK.¹² The United States' demands for data stored abroad are increasingly likely to violate foreign laws prohibiting data disclosure.

The Magistrate's decision ignores that such conflicts of laws are likely to occur¹³ and that the MLAT process plays a vital role in defusing such conflicts. By focusing on the burden on law enforcement without considering the balance of interests between sovereigns or providers' conflicting obligations, the Magistrate rejected a process designed to address comity issues, avoid conflicts of law, and foster cooperation between governments. In both directions, the MLAT process resolves a complex web of jurisdictional questions and conflict of law issues through a binding, mutual treaty. Interpreting ECPA to avoid this treaty obligation in *all cases* not only exacerbates conflicts issues, but violates Justice Marshall's admonition "that 'an Act of Congress ought never to be construed to violate the law of nations if any other possible construction remains * * *.'" *Lauritzen v. Larsen*, 345 U.S. 571, 578 (1953) (citing *Murray v. The Schooner Charming Betsy*, 6 U.S. 64 (1804)).

When these conflicts exist, providers and their employees are at increased risk of criminal sanctions for producing data, particularly where courts demanding production do not consider foreign law. Employing a comity analysis allows courts to ensure that the right balance is struck

¹² "The launch of Microsoft's Office 365 in June 2011, for example, was accompanied by expressions of concern that Microsoft would not guarantee that data of European customers could not be accessed by agencies acting under US jurisdiction. Similar such concerns were behind the Dutch government appearing to suggest that US-based suppliers of cloud services may be 'excluded' from supplying public authorities handling government or citizen data due to the risk of access by US authorities. In addition, some European providers have even tried to make a virtue out of their 'non-US' status, calling for certification schemes that would indicate where data is protected from such access." Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, Queen Mary School of Law Legal Studies Research Paper No. 74/2011 (Nov. 14, 2011), available at <http://dx.doi.org/10.2139/ssrn.1781067>

¹³ Instead of considering the legitimate interests of foreign governments in passing laws to restrict the disclosure of locally stored data about their citizens, which has actually occurred, the magistrate focuses on the theoretical potential for U.S. citizens to falsely claim foreign residence to cause their data to be stored overseas without any factual basis to suggest that such misrepresentations would be effective. See Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12.965

between the United States law enforcement interests and its treaty obligations especially when ignoring those obligations places U.S. providers in unresolvable conflict of laws situations. In weighing the “practical considerations” in this case, the Magistrate should not have considered only the burden the MLAT process places on the government, but instead the full international ramifications of upholding the warrant, including its impact on providers.

3. The Magistrate Improperly Rejected the MLAT Process in All Cases

The Magistrate’s decision improperly disregarded the MLAT process on an insufficient factual basis. Rather than consider possible conflicts of law, or balancing the interests of the United States and Ireland, the Magistrate erred by focusing solely on the burden on U.S. law enforcement if it could not, in all cases, compel providers to produce email content stored abroad with an “SCA Warrant.” The Magistrate speculated that Congress was “unlikely” to have intended to require the Government to comply with the MLAT *in any case*, because doing so would be inconvenient. Not only does that consideration ignore comity principles, it is incorrect in at least some subset of cases. The MLAT process is not as streamlined as obtaining a domestic warrant, but it is not necessarily so burdensome that it should be dismissed completely.¹⁴ An MLAT request may often adequately serve law enforcement needs and not raise any of the Magistrate’s concerns. It is possible to receive a prompt response to an MLAT in many countries. The FBI has legal attaché offices that cooperate with foreign law enforcement in sixty-four (64) locations across the globe.¹⁵ Those offices “help ensure a prompt and continuous exchange of information.”¹⁶ As an FBI official in one of these offices in Denmark has stated, “Treat your partners well and work with them and you will get stuff turned

¹⁴ To the extent that the MLAT process is not serving the government’s needs, it is important to remember that the government designs and administers the process and it is within the government’s capability to improve it.

¹⁵ See *Federal Bureau of Investigation—International Operations*, http://www.fbi.gov/about-us/international_operations (last visited June 12, 2014).

¹⁶ *Id.*

around very quickly.”¹⁷ The DOJ has recently sought funding to improve its ability prevent delays in responding to MLAT requests and to foster increased international cooperation.¹⁸

And while the United States does not have MLATs with every country, it has MLATs with Ireland, every other country in the European Union, many countries in the Organization of American States, and numerous other countries throughout the world. United States Dept. of State, *Treaties in Force* (2013).¹⁹ Many MLATs provide for expedited requests. *See* Mutual Legal Assistance Agreement with the European Union art. 7, U.S.-E.U. June 25, 2003, Treaty Doc. 109-13 (the ‘‘EU Framework Agreement’’); *see also* Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185 at Art. 23-35 (addressing mutual legal assistance, the 24/7 network, and email and fax requests). And the Government may seek additional time in criminal prosecutions to seek foreign evidence when faced with delays. 18 U.S.C. § 3292; *DeGeorge v. U.S. Dist. Ct. for Cent. Dist. Cal.*, 219 F.3d 930, 937 (9th Cir. 2000).

B. Allowing the Government to Avoid the MLAT Process in All Cases Will Place Providers at Greater Risk of Sanction in Foreign Countries

If U.S. companies must hand over data stored overseas without regard to provisions of foreign law, other countries are likely to reciprocate and demand that U.S. providers comply with local legal demands. But ECPA applies to data stored in the United States and prohibits providers from producing email content except in response to U.S. legal process. *Suzlon Energy v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011); 18 U.S.C. § 2703(a) (‘‘A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication ... only pursuant to a warrant issued using the procedures

¹⁷ *Partnerships Pay Dividends at Nordic Outpost*, FBI.gov, <http://www.fbi.gov/news/stories/2013/december/partnerships-pay-dividends-at-copenhagen-legal-attache/partnerships-pay-dividends-at-copenhagen-legal-attache> (last visited June 13, 2014).

¹⁸ *See* U.S. Dept. of Justice, FY 2015 Budget Request, Mutual Legal Assistance Treaty Process Reform, *available at* <http://www.justice.gov/jmd/2015factsheets/mut-legal-assist.pdf>.

¹⁹ *Available at* <http://www.state.gov/documents/organization/218912.pdf>.

described in the Federal Rules of Criminal Procedure”); 18 U.S.C. § 2711(4) (excluding foreign governments from the definition of “governmental entity”). As a result, U.S. companies regularly advise foreign governments that they must use the MLAT process to comply with ECPA.²⁰ The Magistrate’s decision undermines this position.

If the U.S. judicial system rejects the MLAT process based on the practical considerations cited in the Magistrate’s decision—slow process, ability to refuse requests, and lack of treaties—foreign courts and governments are likely to do the same, as these same concerns affect foreign governments equally. Order at 18-21. And where foreign countries bypass the MLAT process for their own efficiencies, U.S. companies will be forced to either violate ECPA or place U.S. employees located overseas at risk of criminal sanction for refusing to comply.²¹ Further, bypassing ECPA deprives users of levels of privacy protections applicable to users of online services for the customer data, log data, and stored and real-time content they transmit using a third-party service provider, harming U.S. privacy interests.

C. Requiring the Government to Use the MLAT Process Has Ancillary Benefits

There is also inherent value in encouraging all parties to use an MLAT process that benefits the U.S. government, service providers, and user privacy interests.²² By exercising its discretion in whether to enter into an MLAT with a particular country, the U.S. government makes a choice whether it is prepared to offer legal assistance to a particular jurisdiction, which

²⁰A sampling of provider guidelines for law enforcement discussing the need to use MLATs to obtain data include: https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond; <https://www.facebook.com/safety/groups/law/guidelines/>; http://www.snapchat.com/static_files/lawenforcement.pdf; <https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#16>; http://www.tumblr.com/docs/en/law_enforcement; <https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm>.

²¹ See e.g., Robin Wauters, *Yahoo Fined By Belgian Court For Refusing To Give Up E-mail Account Info.*, TechCrunch (Mar. 2, 2009), <http://techcrunch.com/2009/03/02/yahoo-fined-by-belgian-court-for-refusing-to-give-up-e-mail-account-info/>.

²² See, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 418 (2014) (argues in support of a flexible case-by-case approach when discussing the important role the MLAT plays, the alternatives to the MLAT, and importance of a filtering process for foreign government requests for user data).

is a first level filtering function. In addition, the Office of International Affairs in the U.S. Department of Justice vets requests from foreign governments, which adds another layer of filtering. Finally, the legal process issued to service providers in the United States because of the MLAT process is U.S. legal process, issued by U.S. courts consistent with the Constitution and statutory privacy protections such as ECPA. This final step provides the users' whose private data may be sought important privacy protections. It also assures the U.S. provider it is acting within the bounds of U.S. law and will benefit from the protections of U.S. law, including statutorily provided immunity. *See, e.g.*, 18 U.S.C. § 2703(e).

IV. Conclusion

The Magistrate erred by giving undue weight to unsupported concerns about the viability of the MLAT process, while ignoring the reality that U.S. providers frequently receive foreign requests for user data that implicate conflicts of laws. The MLAT process plays a vital role in defusing such conflicts. Accordingly, this Court should reject the magistrate's incomplete reasoning. It should also avoid the temptation to oversimplify what, for both service providers and law enforcement, is a complex web of often conflicting national laws on data privacy and law enforcement access, intricate global data flows to support performance and technical needs, and broader issues of diplomacy and comity in international investigations. Furthermore, viewing the use of warrants in these circumstances as protecting U.S. interests is short-sighted. Neither the broad economic interests nor the political interests of the United States will be served if foreign citizens believe that they are better off not doing business with U.S. based companies. Based on the evolution of the case, the Court should reject the effort to apply ECPA extraterritorially, and conclude that absent further Congressional action, the MLAT process remains the appropriate vehicle for the retrieval of foreign user data stored abroad.

Respectfully submitted,

/s/ _____

Marc J. Zwillinger (*Pro Hac Vice Pending*)
Kenneth M. Dreifach (SBN 2527695)
ZWILLGEN PLLC
232 Madison Avenue, Suite 500
New York, NY 10016
(646) 362-5590 (tel)
(202) 706-5298 (fax)

Counsel for Apple Inc. and Cisco Systems, Inc.

Dated: June 13, 2014