14-2985-CV

United States Court of Appeals

for the

Second Circuit

In the Matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation,

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF VERIZON COMMUNICATIONS INC., CISCO SYSTEMS, INC., HEWLETT-PACKARD CO., EBAY INC., SALESFORCE.COM, INC., AND INFOR, AS *AMICI CURIAE* IN SUPPORT OF APPELLANT

RANDAL S. MILCH
VERIZON COMMUNICATIONS INC.
1095 Avenue of the Americas
New York, NY 10036
Counsel for Verizon Communications Inc.

MICHAEL VATIS
JEFFREY A. NOVACK
STEPTOE & JOHNSON LLP
1114 Avenue of the Americas
New York, NY 10036
(212) 506-3900
Counsel for Verizon Communications Inc.

(For Continuation of Appearances See Inside Cover)

KRISTOFOR T. HENNING
HEWLETT-PACKARD COMPANY
1550 Liberty Ridge Drive, Suite 120
Wayne, PA 19087
Counsel for Hewlett-Packard Co.

AMY WEAVER
DANIEL REED
SALESFORCE.COM, INC.
The Landmark @ One Market
Suite 300
San Francisco, CA 94105
Counsel for salesforce.com, inc.

ORIN SNYDER
THOMAS G. HUNGAR
ALEXANDER H. SOUTHWELL
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166
Counsel for Infor

MARK CHANDLER
CISCO SYSTEMS, INC.
170 W. Tasman Drive
Building 10
San Jose, CA 95134-1706
Counsel for Cisco Systems, Inc.

AARON JOHNSON
EBAY INC.
2065 Hamilton Avenue
San Jose, California 95125
Counsel for eBay Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel for *amici curiae* certify the following information:

Verizon Communications Inc. is a publicly held corporation and has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

Cisco Systems, Inc. is a publicly held corporation and has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

Hewlett-Packard Co. is a publicly held corporation and has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

eBay Inc. is a publicly held corporation and has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

salesforce.com, inc. is a publicly held corporation and has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

Infor (US), Inc. ("Infor"), is a wholly owned subsidiary of Infor, Inc. The shares of Infor, Inc. are beneficially owned by investment funds affiliated with Golden Gate Capital and Summit Partners through these funds' ownership of all stock in the ultimate entity of Infor.

Table of Contents

TABLE OF AUTHORITIES

RULES

INTERNATIONAL TREATIES AND OTHER SOURCES

ARTICLES AND NEWS RELEASES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICI CURIAE*

Verizon Communications Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., salesforce.com, inc., and Infor submit this *amicus* brief in support of Appellant Microsoft Corporation and seeking reversal of the District Court's judgment.[1]

The *amici* provide cloud computing services internationally. These services allow foreign customers to store and process their electronic information on computer servers located outside the United States. The *amici* are therefore subject to various foreign laws regarding data privacy and data transfer. The confidence of foreign customers in the *amici*'s ability to operate within the requirements of those laws is important to their businesses.

Verizon Communications Inc. is a global leader in delivering communications services to consumer, business, government, and wholesale customers and provides integrated business solutions to customers in more than 150 countries. Moreover, Verizon subsidiaries operate "cloud" storage services

---

[1] All parties have consented to the filing of this amicus brief. Accordingly, this brief may be filed without leave of court, pursuant to Rule 29(a) of the Federal Rules of Appellate Procedure.

Pursuant to Rule 29.1 of this Court's Local Rules, the *amici* certify that (1) this brief was authored entirely by counsel for the *amici*, and not by counsel for any party, in whole or part; (2) no party and no counsel for any party contributed money intended to fund preparing or submitting the brief; and (3) apart from the *amici*, no other person contributed money intended to fund preparing or submitting the brief.

internationally, which allow business customers in other countries to store their data on Verizon servers located abroad.

Cisco Systems, Inc. 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.

Hewlett-Packard Co. ("HP") is the world's largest information technology company. It offers personal computers, enterprise storage and servers, networking devices, IT management software, IT services and imaging and printing-related products. HP also provides cloud computing services internationally.

eBay Inc. is a global commerce platform and payments leader, whose businesses include the core e-commerce platform located at www.eBay.com, PayPal, StubHub, and eBay Enterprise (a leading provider of e-commerce and interactive marketing services to enterprise clients). eBay Inc. businesses facilitate hundreds of millions of transactions and payments globally each year.

salesforce.com, inc. is a leading provider of enterprise cloud computing services headquartered in San Francisco, California. salesforce has offices and data centers located internationally to service its customers.

Infor is a leading technology company, headquartered in New York City, with annual revenues of approximately $2.8 billion and in excess of 13,000 employees. Infor provides enterprise software solutions and related services to more than 70,000 customers in over 200 countries.

As described above, the services offered by the *amici* are different from the email service operated by Microsoft which is at issue in this case. But the logic of the District Court's ruling extends beyond email services. By increasing suspicions that information foreign customers store with U.S.-owned cloud providers in foreign countries is easily accessible by the U.S. government, the District Court's order will have a significant detrimental impact on the businesses of the *amici* and many other companies similarly situated.

Moreover, because they operate in multiple countries, and locate at least some of their servers outside the United States, the *amici* are subject to foreign data protection and privacy laws, which at times may conflict with U.S. law. The District Court's ruling threatens to force companies like the *amici* to choose between complying with a U.S. search warrant and violating foreign law, on the one hand, or complying with foreign law and disobeying a U.S. court order, on the other.[2]

---

[2] Some of the *amici* may not be subject to the same statutory provisions at issue in this case, or in the same manner. But they are nonetheless concerned that the position taken by the government here could also be asserted under other laws, which could similarly force companies into the impossible position of having to choose between violating either U.S. or foreign law.

For these reasons, the *amici* have a strong interest in the outcome of this appeal.

INTRODUCTION

The District Court's decision allowing the U.S. government to demand the disclosure of the contents of customer communications (as opposed to Microsoft's own business records) stored in overseas data centers is extraordinarily sweeping in its scope and impact. It affects not only the e-mail service at issue in the case, but a host of other communication services, data storage providers, and technology companies. It will expose American businesses to legal jeopardy in other countries and damage American businesses economically. It will upset our international agreements and undermine international cooperation. And it will spur retaliation by foreign governments, which will threaten the privacy of Americans and non-Americans alike.[3]

The importance of law enforcement's ability to acquire evidence abroad is indisputable. That is why governments have for decades maintained formal and informal mechanisms for law enforcement-to-law enforcement cooperation. Mutual Legal Assistance Treaties (MLATs), for example, obligate each nation to respond to requests for assistance in obtaining evidence, including electronic communications.

[3] A U.S. government demand for a cloud provider's own business records located abroad may raise similar policy concerns. But because Microsoft's business records are stored in the United States, that issue is not presented in this case.

Many nations are also parties to the Council of Europe Convention on Cybercrime (also known as the "Budapest Convention"), which obligates signatory nations to expeditiously preserve and disclose electronic evidence to a requesting nation.[4] Moreover, the Convention set up a "24/7 Network," which consists of points-of-contact for each signatory nation, who are available twenty-four hours a day, seven days a week "to ensure the provision of immediate assistance . . . for the collection of evidence in electronic form of a criminal offence."[5]

Though such arrangements are not perfect, they have enabled the U.S. government regularly to obtain evidence located abroad by engaging the assistance of the relevant foreign government—just as it could have done here.[6] But the U.S. government in this case seeks to circumvent this long-established system and unilaterally obtain foreign evidence (i.e., the contents of communications owned by

---

[4] *See* Council of Europe, Convention on Cybercrime, Nov. 23, 2001, ETS No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/html/185.htm. The title of the Convention is in fact a misnomer, since the Convention is not limited to "cybercrime," but establishes a framework for assisting in the investigation of any crime for which evidence may be found in "electronic form." *Id.* art. 14(2)(c).

[5] *Id.* art. 35(1).

[6] Contrary to the District Court's apparent assumptions, the U.S. government frequently and effectively utilizes the MLAT process. In addition, the FBI has legal attachés in 64 locations across the globe. These officials "help ensure a prompt and continuous exchange of information." FBI, *Crime and Terror have gone global. And so have we,* FBI.GOV, http://www.fbi.gov/about-us/international_operations (last visited Dec. 12, 2014). And many MLATS provide for expedited requests. *See Agreement on Mutual Assistance Between the European Union and the United States of America*, art. 7, June 25, 2003, T.I.A.S. 10-201.1.

a third-party customer) by serving a search warrant on a U.S. company—not because it could not otherwise obtain the evidence, but because it believes its unilateral approach is faster and easier.

Congress *could* conclude that the needs of law enforcement outweigh the detrimental economic consequences for U.S. businesses and the harm to international comity and individual privacy. But this is a decision for Congress, not the courts. Because Congress has not clearly expressed in any law an intention that search warrants for customer information apply to information located abroad, the judgment of the District Court should be reversed and the search warrant vacated in this case.

ARGUMENT

I. The Presumption Against Extraterritoriality And The *Charming Betsy* Doctrine Militate Against Construing ECPA As Permitting Searches And Seizures Of Customer Data Located Outside The United States

As Microsoft has demonstrated in its opening brief (App. Br. at 18-33), this case should begin and end with the presumption against extraterritoriality. The Supreme Court has reiterated many times that a statute is presumed *not* to have extraterritorial application "'unless there is the affirmative intention of the Congress clearly expressed' to give [the] statute extraterritorial effect." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 248 (2010) (citation omitted). There is nothing in the plain language of the Electronic Communications Privacy Act ("ECPA") or in its

legislative history that evinces any congressional intent that the Act apply to the contents of customer-owned communications and data outside the United States. To the contrary, the legislative history reveals that Congress intended the Act *not* to apply extraterritorially. *See* App. Br. at 21-26

The *Charming Betsy* doctrine independently requires courts to construe a statute to avoid creating conflicts with the laws of other nations. *See Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) ("[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains."). As the Supreme Court reiterated in *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, courts should "assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws." 542 U.S. 155, 164 (2004). This assumption "helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *Id.* at 164–65.

This case perfectly demonstrates why the presumption against extraterritoriality and the *Charming Betsy* doctrine are so important. For the district court's decision, if affirmed, will hurt American communications and technology companies and create conflicts with the laws of other nations. Yet, there is no indication whatsoever that Congress ever intended that search warrants for electronic communications apply to the contents of customer-owned

communications and data stored outside the United States. It is not the province of the courts to construe a statute in a manner that would have such dramatic repercussions without any grounding in the words or history of that statute simply because the Executive Branch, however well-intentioned the motives, wishes it were so.

It is no answer to say that the government is not seeking to apply ECPA extraterritorially because it served the search warrant in the United States and the emails would be handed over to the government in the United States. As Microsoft's brief makes clear, a seizure and a search of those emails would still occur in Ireland, where the emails are stored and from where they would be taken at the direction of the U.S. government. *See* App. Br. at 26-35.

Moreover, the Supreme Court has said that a statute can be regarded as applying extraterritorially even when a significant portion of the required actions will occur in the United States. *See Morrison*, 561 U.S. at 266 ("[I]t is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States.... [T]he presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case."). Thus, in *Morrison* the Court found that the government was seeking to apply the Securities Exchange Act of 1934 extraterritorially even though the deceptive conduct at the heart of the transaction originated in the U.S.

Moreover, the Court based its finding that the Act was being applied extraterritorially in large part on the fact that the government's position would create a conflict with foreign laws. *See id.*, at 269 ("The probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures.'") (citation omitted). *See also Kiobel v. Royal Dutch Petroleum Co.,* 133 S. Ct. 1659, 1664 (2013) ("The presumption [against extraterritoriality] 'serves to protect against unintended clashes between our laws and those of other nations which could result in international discord.'") (citation omitted); *Parkcentral Global Hub Ltd. v. Porsche Auto. Holdings SE*, 763 F.3d 198, 214-17 (2d Cir. 2014) (concluding that, notwithstanding domestic component of transaction, the statute was being applied extraterritorially because it would trigger conflict with foreign law).

Microsoft and other U.S.-based cloud service providers would face significant legal exposure due to conflicts between U.S. and foreign laws should the government prevail in this case. This underscores that the government is indeed seeking to apply ECPA extraterritorially.

II. The District Court's Ruling Would Harm American Businesses Economically And Potentially Subject Them To Civil And Criminal Liability Abroad

Recent revelations about U.S. intelligence practices have heightened foreign sensitivities about the U.S. government's access to data abroad, generated distrust of U.S. companies by foreign officials and customers, and led to calls to cease doing business with U.S. communications companies and cloud service providers. This has put U.S. companies at a competitive disadvantage with respect to their foreign competitors. Studies have estimated that this distrust will result in tens of billions of dollars in lost business by U.S. companies over the next few years.[7]

The District Court's ruling threatens to exacerbate these already heightened tensions. It would mean that foreign customers' communications and the contents of

---

[7] *See, e.g.,* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies,* N.Y. TIMES, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html. Forrester Research estimates U.S. losses at up to $180 billion due to the fear and distrust of U.S. authorities. *See* Clint Boulton, *NSA's Prism Could Cost IT Service Market $180 Billion*, WALL ST. J. (Aug. 16, 2013), http://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion. EU Commissioner for Digital Affairs Neelie Kroes has warned, "It is often American providers that will miss out, because they are often the leaders in cloud services. If European cloud customers cannot trust the United States government, then maybe they won't trust US cloud providers either. If I am right, there are multibillion-euro consequences for American companies. If I were an American cloud provider, I would be quite frustrated with my government right now." Ian Traynor, *European firms 'could quit US internet providers over NSA scandal'*, THE GUARDIAN (July 4, 2013), http://www.theguardian.com/world/2013/jul/04/european-us-internet-providers-nsa (quotation marks omitted).

other electronic data would be available to hundreds or even thousands of federal, state, and local law enforcement agencies, regardless of the laws of the countries where the data is stored. Foreign customers will respond by moving their business to foreign companies without a presence in the United States, ultimately frustrating the interests of the U.S. government in general even if its aims are served in the instant case.

In addition, if a U.S. search warrant could be used to obtain the content of customer data or communications stored abroad, it would create a dramatic conflict with foreign data protection and privacy laws. Those conflicts would expose U.S. companies and their personnel to potential civil and criminal liability.

Many countries highly value the privacy of communications, even considering privacy a fundamental human right. *See, e.g.* Council of Europe, 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, *available at* http://conventions.coe.int/treaty/en/treaties/html/005.htm.[8] Accordingly, they have enacted strict laws to protect the privacy of electronic communications and to severely limit sending personal data outside the countries' borders and disclosing the

[8] Ireland's Data Protection Commissioner Helen Dixon has written on Ireland's Data Protection Commission website that "[d]ata protection is about your fundamental right to privacy." Helen Dixon, Message from Ireland's Data Commissioner on *Data Protection*, DATAPROTECTION.IE, https://www.dataprotection.ie/viewdoc.asp?DocID=4 (last visited Dec. 12, 2014).

data without consent. The European Union's "e-Privacy Directive" and Data Protection Directive and the national laws implementing them are just a few examples. *See* Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC); Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC).[9] And many countries have adopted, or are considering adopting, laws specifically designed to protect the information of their citizens from disclosure to foreign governments. For example, a recently enacted Brazilian law prohibits the disclosure, absent a Brazilian court order, of: (1) communications that are stored, collected, or processed in Brazil; and (2) communications in which one party is in Brazil. *See* Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12.965, Apr. 23, 2014 (Braz.).[10]

The District Court's decision threatens to put companies that comply with

---

[9] *See also, e.g.,* Data Protection Act 1988, Section 10 (Act No. 25/2008) (Ir.), *available at* http://www.irishstatutebook.ie/1988/en/act/pub/0025/sec0010.html# (providing for investigation and enforcement of violations of Irish Data Protection Act); CODE PÉNAL art. 314 (Belg.) (protecting privacy of electronic communications); Act on the Protection of Privacy in Electronic Communications (Finland) (516/2004) (same); CODE PÉNAL art. 226 (Fr.) (same); Nomos (2006:3471) Protection of Personal Data and Privacy in the Electronic Telecommunications Sector and Amendment of Law 2472/1997, 2006 A:4 (Greece) (same); Luxembourg Law of 2005 Privacy in Electronic Communications (same); Poland Telecommunications Act Art. 159 (same); CÓDIGO PENAL art. 197 (Spain) (same).

[10] Unofficial English translation, *available at* https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf (last visited Dec. 12, 2014)

orders like the one in this case in conflict with these foreign laws. As the European Commission spokeswoman for justice, fundamental rights, and citizenship stated: "The commission's position is that this data should not be directly accessed by or transferred to US law enforcement authorities outside formal channels of co-operation, such as the mutual legal assistance agreements or sectoral EU–US agreements authorising such transfers . . . . The European Parliament reinforced the principle that companies operating on the European market need to respect the European data protection rules - even if they are located in the US." *Microsoft 'must release' data held on Dublin server*, BBC NEWS TECHNOLOGY (Apr. 29, 2014), http://www.bbc.com/news/technology-27191500 (internal quotation marks omitted). Ireland's Minister for Data Protection Dara Murphy voiced a similar sentiment in reaction to this case: "When governments seek to obtain customer information in other countries they need to comply with local laws in those countries."[11]

This is not just rhetoric. Companies face real legal risk for complying with U.S. demands for data stored beyond the borders of the United States. For example, when European regulators learned that the Society for Worldwide Interbank Financial Telecommunications ("SWIFT"), the Belgium-based international bank

[11] Pamela Newenham, *Implications of Microsoft losing email case*, IRISH TIMES, Oct. 13, 2014, *available at* 2014 WLNR 28450327.

consortium, had been complying with U.S. subpoenas and providing data to the U.S. government about the financial transactions of European residents, SWIFT was subjected to numerous investigations by European and other governments for violations of their data protection and privacy laws.[12] Ultimately, SWIFT was forced to restructure its network to prevent the passage of intra-European data through the U.S (which we note serves no purpose of the United States government).[13] *See also In re Avocat "Christopher X"*, Cour de cassation [supreme court for judicial matters] crim, Dec. 12, 2007, Bull. crim., No. 07-83228 (Fr.), available at http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000017837490&fastReqId=2062651721&fastPos=1 (finding American-trained lawyer liable for violating France's "blocking" statute by contacting witness in France and obtaining economic information in support of investigation by California Insurance Commissioner); *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-braz

---

[12] *See* John Rega & Jones Hayden, *Swift's bank-data transfers to U.S. violated privacy rules, EU says; Swift ordered to stop infringement; Action highlights security rift*, TORONTO STAR, Nov. 24, 2006, *available at* 2006 WLNR 20358390; Dan Bilefsky, *Belgian leader orders bank inquiry Ministry to investigate release of details on money transfers*, INTERNATIONAL HERALD TRIBUNE, June 27, 2006, *available at* 2006 WLNR 11105900.

[13] *See SWIFT to stop processing EU banking data in the US*, THE REGISTER (Oct. 15, 2007), http://www.theregister.co.uk/2007/10/15/swift_processing_halt.

il-faces-arrest-over-video.html (reporting on Brazilian court's issuance of arrest order for Google executive for failing to comply with Brazilian law by taking down YouTube video).

The District Court's decision thus would force companies to choose, at their own peril, between conflicting U.S. and foreign legal obligations.

III. The District Court's Decision Would Undermine International Agreements And Understandings And Spur Retaliation By Foreign Governments.

Permitting the U.S. government unilaterally to obtain the content of customer data stored abroad would also upset a carefully constructed structure of formal and informal cooperation set up by law enforcement agencies worldwide, and invite retaliation by foreign governments.

For example, MLATs between the U.S. and foreign governments typically have specific provisions requiring the "requested" party to obtain evidence on behalf of the "requesting" party, including by using search warrants or other court orders. These provisions presuppose that the requesting party will not bypass the MLAT and unilaterally obtain evidence in the territory of the requested state, and will act in compliance with the law of the requested state. Ireland, where the data sought by the government here is stored, specifically added language to the U.S.-Ireland MLAT providing that searches be carried out in accordance with the law of the requested

party.[14] And Irish law requires authorization from an Irish District Court Judge in order to obtain the content of emails from an electronic communications provider. *See* Criminal Justice Act 2011 (Act No. 22/2011) (Ir.) § 15, *available at* http://www.irishstatutebook.ie/pdf/2011/en.act.2011.0022.pdf.

These MLATs are expressions of longstanding, basic principles of state sovereignty. As the Restatement (Third) of Foreign Relations Law puts it: "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent." Restatement (Third) of the Foreign Relations Law of the United States § 432, cmt. b (1987). This principle specifically applies to law enforcement investigations: one state's "law enforcement officers ... can engage in criminal investigation in [another] state only with that state's consent." *Id.*

The fact that a search is conducted via a computer connection does not eliminate the infringement on state sovereignty. "A search of one's hard drive by a

---

[14] *See* S. Exec. Rep. 107-15, at 28 (2002), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-107erpt15/pdf/CRPT-107erpt15.pdf ("The Irish delegation requested that language that states that searches and seizures be ''carried out in accordance with the law of that [Requested] Party,'' be added to reiterate this important requirement....'") (alteration in original); 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., art. 14(1), Jan. 18, 2001, T.I.A.S. 13137, *available at* http://www.state.gov/documents/organization/129536.pdf ("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.").

foreign law enforcement agency from abroad . . . has the same effect as a traditional search of premises, a law enforcement measure reserved to the territorial sovereign. . . . As territorial sovereignty serves, inter alia, to protect the residents from physical persecution of other states, this protection must be extended when persecution no longer needs to physically enter foreign territory." Stephen Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?* 50 FED COMM. L.J. 117, 174 (1997).

Such international understandings are not mere niceties to reassure foreigners. They protect Americans, too, in ways that the District Court's decision would undermine. If U.S. law enforcement may now obtain the content of foreign customers' data stored abroad by serving a search warrant on a provider in the United States, foreign governments will be certain to assert the same authority. The Russian government, for example, might demand that a local affiliate of a U.S. cloud services provider disclose the data of a U.S. company negotiating a large corporate transaction with a Russian state-owned enterprise, or that of an American human rights group that has challenged an action of the Russian government in a fashion deemed to violate Russian law. Following the District Court's reasoning, Russian officials could order the provider's Russian affiliate to obtain the target's data from the U.S. and turn it over to the Russian authorities in Moscow. This is not a result

that the U.S. government—or American companies or citizens—would find tolerable. Yet it is precisely what the District Court's decision invites.[15]

Moreover, these effects would not be limited to American companies or citizens. If the District Court's position in this case is adopted, the U.S. government also could require *foreign*-based companies with a presence in the U.S. to turn over customer data stored abroad. Similarly, applying the same principles, foreign governments could force any companies doing business in their territory to disclose customer data stored outside that territory, regardless of where the companies are based. The government's position would thus result in an international free-for-all, with conflicts of law becoming the norm rather than the exception.

It is possible that Congress *could* decide that making it easier for U.S. law enforcement to obtain customer data stored abroad, without the assistance of foreign law enforcement, outweighs the adverse effects on American businesses,

---

[15] The government has previously recognized these concerns, even if the prosecutors in this case have not. *See, e.g.*, U.S. DEP'T OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, A REPORT OF THE PRESIDENTS WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET (FEBRUARY 2000), *available at* http://www.politechbot.com/docs/unlawfulconduct.html ("If law enforcement agents in the United States . . . remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? . . . [C]onsider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts.").

international relations, and privacy. But Congress has not made that decision.[16] And it certainly has not clearly expressed an intent that search warrants apply extraterritorially, as explained in Microsoft's brief. Thus, the presumption against extraterritoriality and the *Charming Betsy* doctrine dictate that ECPA not be construed as permitting a search warrant to be used to obtain a customer's electronic communications located abroad. As the Supreme Court recently reiterated in *Kiobel*:

> For us to run interference in . . . a delicate field of international relations there must be present the affirmative intention of the Congress clearly

---

[16] Instead, Congress and the Administration have sought to reinforce and improve existing mechanisms for law enforcement-to-law enforcement cooperation. In 2009, Congress passed the Foreign Evidence Request Efficiency Act of 2009 to streamline the MLAT process and make it easier for the Justice Department to obtain evidence on behalf of foreign counterparts. It did so in part to encourage foreign nations to similarly streamline their processes for assisting U.S. law enforcement. *See* 155 Cong. Rec. S6807-01 ("Setting a high standard of responsiveness will allow the United States to urge that foreign authorities respond to our requests for evidence with comparable speed."). In addition, in March 2014, the Administration sought an increase in its budget for processing MLAT requests. *See* U.S. Dep't of Justice, *Attorney General Holder Announces President Obama's Budget Proposes $173 Million for Criminal Justice Reform*, JUSTICE.GOV (Mar. 4, 2014), http://www.justice.gov/opa/pr/2014/March/14-ag-224.html. In doing so, the Attorney General recognized that, "These resources are critical to supporting the President's National Security Strategy, which recognizes the centrality of international mutual cooperation in criminal justice and counterterrorism matters, by building the 'new framework for international cooperation' envisioned by that strategy." *Id.* And in September 2014, a bi-partisan group of Senators introduced the "The Law Enforcement Access to Data Stored Abroad Act" (LEADS Act), which would ensure that non-U.S. person data located abroad is accessed only through the MLAT process. *See* S. 2871 113th Cong. (Sep. 18, 2014), *available at* http://www.hatch.senate.gov/public/_cache/files/1f3692d5-f41f-4c73-acf2-063c61da366f/LEADS%20Act,%20September%2018,%202014.pdf.

> expressed. It alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord are so evident and retaliative action so certain. The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches.

133 S. Ct. at 1664 (citations and internal quotation marks deleted).

IV. The *Bank of Nova Scotia* Doctrine Is Inapplicable To Customers' Communications And Data

The District Court's decision relied, in large part, on *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983), which enforced a grand jury subpoena requiring a company in the U.S. to produce its business records even though the records were located abroad. Other courts have similarly enforced subpoenas for business records held outside the United States under the so-called *Bank of Nova Scotia* doctrine. *See United States v. Bank of Nova Scotia (In re Grand Jury Proceedings Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (*"BNS"*). But, as Microsoft's brief explains, the *Bank of Nova Scotia* doctrine has never been extended beyond a company's own business records to reach information belonging to a company's customers. *See* App. Br. at 41-43. This Court should not be the first to effect such an extension.

Bank of Nova Scotia was premised on the reduced privacy interests in the company's business records, the company's "pervasive" contact with the United States, and a careful balancing of the interests of the United States and the foreign

country at issue. *See Bank of Nova Scotia*, 740 F.2d at 826-829. As Microsoft's brief elucidates (App. Br. at 44-48), the calculus is far different when the data at issue belongs to the company's *customer*, particularly one who may have no ties to the United States. The customer has a very substantial privacy interest in the content of his or her communications or other information stored with a third party—whether it be a personal diary kept in a bank safe deposit box, a love letter kept in a purse in a hotel room, emails stored with a communications provider, or confidential medical information stored with a cloud storage service. It would be inappropriate to extend a rule based in part on a company's reduced privacy interests in its own business records to wholly different situations involving information owned by the company's *customers*'—information in which those customers have the highest imaginable privacy interests.[17]

As discussed above, there is no indication whatsoever in ECPA that Congress ever contemplated, let alone intended, that U.S. law enforcement could obtain the contents of a customer's electronic communications located abroad by serving a warrant on a communications provider in the U.S. This Court therefore should not

[17] Moreover, it is doubtful that the *BNS* doctrine itself is still good law even with regard to a company's own business records, given the Supreme Court's strong reaffirmation of the presumption against extraterritoriality in *Morrison* and *Kiobel*. The Court need not address that issue here, however, as this case does not involve Microsoft's own business records, but the contents of a customer's communications.

countenance such an unprecedented expansion of *Marc Rich* and *Bank of Nova Scotia*.

CONCLUSION

The search warrant at issue in this case is no run-of-the-mill investigative measure. It purports to reach across the Atlantic Ocean and into the sovereign nation of Ireland and to compel the disclosure of the contents of communications owned by Microsoft's foreign customers. If enforced, it would harm American business, violate international understandings, subject American companies and citizens to potential liability abroad, and invite foreign governments to unilaterally obtain electronic communications and data of Americans in the United States. There is no reason to believe that Congress intended these results when it enacted ECPA. Certainly nothing in ECPA clearly expresses such an intention. The District Court's judgment should be reversed and the warrant vacated.

Respectfully submitted,

/s/ Michael Vatis
Michael Vatis
Jeffrey A. Novack
Steptoe & Johnson LLP
1114 Avenue of the Americas
New York, NY 10036
(212) 506-3900
Counsel for Verizon Communications Inc.

Randal S. Milch
Verizon Communications Inc.
1095 Avenue of the Americas
New York, NY 10036
Counsel for Verizon Communications Inc.

Kristofor T. Henning
Hewlett-Packard Company
1550 Liberty Ridge Drive, Suite 120
Wayne, PA 19087
Counsel for Hewlett-Packard Co.

Mark Chandler
Cisco Systems, Inc.
170 W. Tasman Drive
Building 10
San Jose, CA 95134-1706
Counsel for Cisco Systems, Inc.

Aaron Johnson
eBay Inc.
2065 Hamilton Avenue
San Jose, California 95125
Counsel for eBay Inc.

Amy Weaver
Daniel Reed
salesforce.com, inc.
The Landmark @ One Market
Suite 300
San Francisco, CA 94105
Counsel for salesforce.com, inc.

Orin Snyder
Thomas G. Hungar
Alexander H. Southwell
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166
Counsel for Infor

Dated: December 15, 2014

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P 32(a)(7)(b)(i) because this brief contains 5,264 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman 14-point font.

/s/ Michael Vatis
Michael Vatis
Counsel for Verizon Communications Inc.

CERTIFICATE OF SERVICE

I hereby certify that I caused the electronically filing of the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system on December 15, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Michael Vatis
Michael Vatis
Counsel for Verizon Communications Inc.