14-2985-cv

IN THE

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 IN SUPPORT OF APPELLANT MICROSOFT, INC. BY APPLE INC. AS *AMICUS CURIAE*

Marc J. Zwillinger
Pro hac vice pending
ZWILLGEN PLLC
1900 M St NW, Suite 250
Washington, DC 20036
Tel. 202.296.3585
Fax 202.706.5290

Kenneth M. Dreifach
Counsel of Record
ZWILLGEN PLLC
232 Madison Ave, Suite 500
New York, NY 10016
Tel. 646.362.5590
Fax 202.706.5290

Counsel for Amicus Curiae
Apple Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* Apple Inc. states that it is a publicly-traded corporation, has no parent corporation, and no publicly-traded corporation owns more than 10% of its stock.

Dated: December 15, 2014

Respectfully submitted,

/s/ Kenneth M. Dreifach

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.

TABLE OF CONTENTS

SUMMARY OF THE ARGUMENT 1

INTEREST OF *AMICI CURIAE* AND AUTHORITY TO FILE 5

STATEMENT OF FACTS 6

ARGUMENT 8

I. The District Court Improperly Ignored Conflicts of Laws and International Comity 10

1. The District Court Did Not Consider All Relevant Factors Before Ordering Production 11

2. Failing to Consider All Relevant Factors Is Troubling Where, As Here, a Provider Holds Confidential Communications on its Users' Behalf 15

3. Foreign Sovereigns Have a Strong Interest In Protecting the Privacy of Their Citizens' Communications from Governmental Intrusion. 17

II. ECPA Does Not Provide a Basis to Forego a Comity Analysis 20

CONCLUSION 22

CERTIFICATE OF COMPLIANCE 23

TABLE OF AUTHORITIES

CASES **PAGE(S)**

Aerospatiale v. U.S. Dist. Court for Southern Dist. of Iowa,
482 U.S. 522 (1987) 12

EEOC v. Arabian Am. Oil Co.,
499 U.S. 244 (1991) 20, 21

Ex parte Jackson,
96 US 727, 733 (1877) 16

Hartford Fire Insurance Co. v. California,
113 S.Ct. 2891 (1993) 13

Hilton v. Guyot,
159 U.S. 113 (1895) 11

In re Grand Jury Proceedings Bank of Nova Scotia,
740 F. 2d 817 (11th Cir. 1984) ..... *passim*

In re French,
440 F.3d 145 (4th Cir. 2006) 13

In re Maxwell Commc'n Corp.,
93 F.3d 1036 (2d Cir. 1996) 13

In re U.S. for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013) 15

In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.,
809 F. Supp. 2d 113 (E.D.N.Y. 2011) 16

Lauritzen v. Larsen,
345 U.S. 571 (1953) 19

Linde v. Arab Bank, PLC,
706 F.3d 92 (2d Cir. 2013) 12

Morrison v. Nat'l Austl. Bank Ltd.,
130 S.Ct. 2869 (2010) 21

Murray v. The Schooner Charming Betsy,
6 U.S. 64 (1804) 19

Smith v. United States,
507 U.S. 197 (1993) 20

Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court of Iowa,
482 U.S. 522 (1987) 11, 12

Trade Development Bank v. Continental Ins. Co.,
469 F.2d 35 (2d Cir.1972) 8

United States v. Chase Manhattan Bank,
584 F. Supp. 1080 (S.D.N.Y. 1984) 22

United States v. Davis,
767 F.2d 1025 (2d Cir.1985) 8, 13, 15

United States v. First National City Bank,
396 F.2d 897 (2d Cir.1968) 8

United States v. Jackson,
208 F.3d 633 (7th Cir. 2000) 16

United States v Jacobsen,
466 U.S. 109 (1984) 16

United States v. Miller,
425 U.S. 435 (1976) 15

United States v. Vetco Inc.,
691 F.2d 1281 (9th Cir. 1981) 14

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 10, 15, 16

CASES, CONTINUED

U.S. Commodity Futures Trading Comm'n v. Trade Exch. Network Ltd.,
CV 12-1902 (RCL), 2014 WL 4693408 (D.D.C. June 24, 2014)..... 13

Zheng v. Yahoo! Inc.,
No. C-08-1068 MMC, 2009 WL 4430297 (N.D. Cal. 2009) 9, 21

STATUTES AND RULES

Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq.* ..... *passim*

§ 2701 2

§ 2702 2

§ 2711(4).....2, 21

31 U.S.C. § 5313 15

Fed. R. App. P. 29(a)..... 6

Fed. R. Crim. P. 41 7

Fed. R. Civ. P. 44.1 11

LEGISLATIVE MATERIALS

H.R. Rep. No. 99-647 (1986) 16, 21

TREATIES AND INTERNATIONAL MATERIALS

Code Pénal [C.Pén.] art. 314 (Belg.) 10, 17

Code Pénal [C. Pén.] art. 226 (Fr.) 10, 17

Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185..... 18

European Convention for the Protection of Human Rights and Fundamental Freedoms (Nov. 1950) ETS No. 5 17

TREATIES AND INTERNATIONAL MATERIALS, CONTINUED

Directive 95/46/EC of the European Parliament and of the Council (24 Oct. 1995) [Data Protection Directive] 18

Ireland Data Protection Act, (1988) Section 10 10

Law on Networks and Electronic Communications Services (Luxembourg) [*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 17

Lei No. [Law No.]12.965, *de* 23 *Abril de* 2014, *Col. Leis Rep. Fed. Brasil*, [Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*)] 4, 19

Nomos (2006:3471) Protection of Personal Data and Privacy in the Electronic Telecommunications Sector and Amendment of Law 2472/1997, 2006 A:4 (Greece)..... 10, 17

Penal Code Section 197 (Spain) 10, 17

Prawo Telekomunikacyjne [Poland Telecommunications Act art. 159], *Dz. U. z* 2000 *Nr* 171, *poz*. 1800, *available a*t http://isap.sejm.gov.pl/ Download?id=WDU20140000243&type=2 17

Restatement (Third) of Foreign Relations Law § 101 (1987)..... 11

Restatement (Third) of Foreign Relations Law § 403 (1987)..... 14

Restatement (Second) of Foreign Relations Law § 40 (1965)..... 12, 13

Sähköisen viestinnän tietosuojalaki [Act on Data Protection in Electronic Communications] Act No. 516/2004 of 16 June 2004 (Finland) 10, 17

OTHER AUTHORITIES

Apple, *Report on Government Information Requests* (2014), *available at* http://images.apple.com/privacy/docs/government-information-requests-20140630.pdf 5

Eric Pfanner, *Google Faces a Different World in Italy*, N.Y. Times (Dec. 13, 2009) 6

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 19

Kashmir Hill, *The Downside of Being a Google Executive*, Forbes (Sept. 27, 2012), ... 6

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) 18

Reuters, *Top Google Executive in Brazil Faces Arrest Over Video*, N.Y. Times (Sept. 25, 2012), *available at* http://www.nytimes.com/2012/09/26/business/global/top-google-executive-in-brazil-faces-arrest-over-video.html 6

SUMMARY OF THE ARGUMENT

One reason this case has garnered so much amicus attention is that the district court gave short shrift to an enormously complex issue relating to the power of the U.S. government to compel global companies in an interconnected world to turn over data related to their foreign users, stored in foreign data centers, under the legal control of foreign subsidiaries, with no significant consideration of the international consequences of imbuing the U.S. government with such power.[1] And it did so absent any clear statutory language specifically authorizing the application of the only relevant U.S. law in such a scenario.

In rejecting Microsoft's motion to vacate the search warrant, the District Court wrote no opinion, but merely adopted the decision of the Magistrate before it. Neither in its oral remarks, nor in the magistrate's opinion, did the lower court give much weight to the fact that foreign corporations, including foreign subsidiaries of U.S. parent companies, are subject to foreign data privacy laws which may prevent the transfer of data to third-parties to respond to government requests for information – much as U.S. data privacy laws themselves operate.[2]

---

[1] Amicus states that no party's counsel authored this brief in whole or in part, nor did any party other than Apple Inc. contribute money intended to fund preparing or submitting this brief.

[2] This legal fact is one that runs both ways across the Atlantic Ocean.: the Electronic Communications Privacy Act (ECPA) – the U.S. statute at issue in this case – itself prohibits internet providers subject to U.S. jurisdiction from disclosing the contents of emails they maintain on behalf of their users, subject to certain exceptions. ECPA provides no exception for disclosures to foreign governments (even if a foreign corporate parent has access to such data). Thus, if this decision had been handed down by a court in the U.K., and a British parent

Nor did the court consider the impact of what would happen if every country reached the same conclusion. Instead, the District Court attempted to bypass these complicated issues by focusing myopically on the single question of "control" by the United States-based corporate parent over the data at issue. Dkt. 84 at 69. This signaled to the rest of the world that the United States government intends to force U.S. companies to reach into foreign territories to turn over foreign user data with no regard for, or consideration of, the legal interests of foreign governments or their citizens.[3] But the District Court failed to take into account the crucial legal fact that a company's ability to access data is not the same as the right to disclose it.

Rather than focusing solely on whether Microsoft had the technical ability to retrieve user data stored overseas from its U.S. offices, the court should have analyzed: (a) the nature of the relationship between the user and the foreign subsidiary processing data on behalf of the user; (b) whether that relationship was a one of direct control by the foreign subsidiary (the "Data Controller"), creating binding obligations on it; (c) the effect of any compelled production on that entity; (d) the interests of the foreign sovereign where that entity is located, here Ireland;

---

corporation was forced to retrieve data maintained in the U.S. by one if its U.S. subsidiaries, that act of production could likely violate U.S. law. 18 U.S.C. § 2702; 18 U.S.C. § 2711(4) (defining governmental entity to include only federal and state governments).

[3] This may or may not be the course Congress ultimately chooses – but it is clear that Congress did not expressly speak to this issue in 1986 when it passed ECPA.

and (e) any intercompany restrictions on transferring such data. The court should also have examined the availability of other mechanisms to obtain the data, and whether those mechanisms are more consistent with the actual language of the Electronic Communications Privacy Act ("ECPA"), given the established principles against interpreting statutes to have an extraterritorial effect and long-standing precedent considering international comity before applying United States law abroad. Only after considering these factors should it have reached a decision or, alternatively, determined that it could do nothing until Congress spoke more plainly on the issue.

By failing to factor these issues properly into its analysis—and by essentially dismissing international sovereignty and comity concerns out of hand—the District Court placed the burden of reconciling conflicting international laws solely on U.S. providers. The result is a situation that is not only legally problematic, but practically unmanageable. For this will not be the last time that a U.S. provider is faced with compulsory process purporting to require it to access user data stored abroad. And in future occasions the laws of the local country, even more so than Irish law,[4] may plainly prohibit disclosure and subject local employees to arrest and prosecution. *See, e.g.*, Brazilian Civil Rights Framework for the Internet

[4] The extent to which Irish law may prohibit this disclosure was not clear from the record and decisions below, likely because it was irrelevant to the court's analysis.

(*Marco Civil da Internet*), Law No. 12.965.[5] To hold that principles of international comity and reciprocity should play no role in the legal analysis contradicts the very precedents upon which the lower court relied. Special Appendix ("SA") 29 (relying on *In re Grand Jury Proceedings Bank of Nova Scotia*, 740 F.2d 817, 829 (11th Cir. 1984) ("*BNS*")). By excluding considerations related to the laws of the country where data is stored and to which the data controller would be subject, the District Court's analysis places providers and their employees at risk of foreign sanctions with no clear answers on resolving the inevitable conflicts between United States and foreign law. This analysis should not stand.

The lower court's decision is particularly problematic as to individual user privacy, where, as here, the records sought are not business records of the parent corporation but private communications to which neither the parent corporation nor its foreign subsidiary are a party. This Court should reverse the district court and remand for determination of whether the Government's interest in obtaining this data outweighs potential conflicts of law issues and the foreign sovereign's interest in data stored within its borders.

[5] *Available at* https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf (last visited Dec. 14, 2014). Unofficial English translation, *available at* http://direitorio.fgv.br/sites/direitorio.fgv.br/files/Marco%20Civil%20ingl%C3%AAs.pdf (last visited Dec. 14, 2014).

INTEREST OF *AMICI CURIAE* AND AUTHORITY TO FILE

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 the iPhone, iPad, Mac computer, and iPod, 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 and are operated by foreign subsidiaries, Apple's foreign subsidiaries control data stored abroad and may be subject to foreign laws regarding data transfer. Apple is committed to transparency and strives to provide straightforward disclosures about these laws and the circumstances under which it is compelled to comply with legal process.[6]

[6] *See e.g.,* Apple, *Report on Government Information Requests* (2014), *available at* http://images.apple.com/privacy/docs/government-information-requests-20140630.pdf (last visited Dec. 14, 2014).

The foreign laws to which Apple and its foreign subsidiaries are subject can often conflict with U.S. law, placing Apple 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.[7] The District Court's 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.[8] Apple should be granted leave to participate as *Amici* in these proceedings pursuant to Fed. R. App. P. 29(a), and the District Court's decision should be reversed and remanded for consideration of international comity and foreign law on the production of evidence the United States government seeks. Apple has the authority to file because all parties have consented to the filing of this brief.

STATEMENT OF FACTS

The Government served Microsoft with a search warrant directing it to produce the contents of a customer's email account. Appendix ("A") 40, 44-48. Microsoft determined that it had stored the responsive email content on a server in

[7] *See e.g.*, Reuters, *Top Google Executive in Brazil Faces Arrest Over Video*, N.Y. Times (Sept. 25, 2012), *available at* http://www.nytimes.com/2012/09/26/business/global/top-google-executive-in-brazil-faces-arrest-over-video.html (last visited Dec. 14, 2014); Eric Pfanner, *Google Faces a Different World in Italy*, N.Y. Times (Dec. 13, 2009), *available at* http://www.nytimes.com/2009/12/14/ technology/internet/14google.html?pagewanted=all&_r=0 (last visited Dec. 14, 2014).

[8] Kashmir Hill, *The Downside of Being a Google Executive*, Forbes (Sept. 27, 2012), *available at* http://www.forbes.com/sites/kashmirhill/2012/09/27/the-downside-of-being-a-google-executive/ (last visited Dec. 14, 2014).

Dublin, Ireland, which was leased and operated by its wholly-owned Irish subsidiary. A 36. In response, 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 exterritorial search at the government's behest. SA 12.

The Magistrate denied Microsoft's motion, upheld the warrant and commanded Microsoft to produce data stored in Ireland. SA 12. Microsoft appealed to the District Court, which affirmed the Magistrate's ruling. SA 29-30, 32. In doing so, the District Court treated the warrant as it would a subpoena[9] and held that Microsoft Corporation in the United States had "possession, custody, or control" over information stored in Ireland and held by its Irish subsidiary, and must produce the email content. SA 31, 32. Subsequently, the District Court entered an order holding Microsoft in contempt, and Microsoft filed this appeal. SA 36.

The District Court's decision did not examine Microsoft's corporate structure, explore possible conflicts with international law, or weigh the burden on providers of complying with conflicting legal regimes. The District Court did not even analyze which entity – foreign or domestic – contracted with the user whose data was demanded (and therefore was the "Data Controller"). Instead, the District

[9] 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.

Court held that "production" of information by a United States-based company is "not an intrusion on the foreign sovereign" because the information was in Microsoft's possession and was being produced within the United States, Dkt. 84 at 69, notwithstanding the fact that it was being copied or seized while it physically sat on a foreign server under the legal and physical control of a foreign subsidiary, and subject to foreign law.

ARGUMENT

The District Court'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, and regularly do, examine possible conflicts of law, consider 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, and the interests of foreign stakeholders, such that the government may circumvent U.S. treaty obligations.[10]

[10] *See, e.g., Trade Development Bank v. Continental Insurance Co.*, 469 F.2d 35, 40–41 (2d Cir.1972) (balancing interests and holding that a party need not produce irrelevant information whose production would violate Swiss law); *United States v. Davis*, 767 F.2d 1025, 1034–35 (2d Cir.1985) ("because such an order may also trench upon the interests of another state, a court is required to strike a careful balance between the competing national interests and the extent to which these interests would be impinged upon by the order"); *United States v. First National City Bank*, 396 F.2d 897, 901 (2d Cir.1968) ("what is required is a careful balance of the interests involved and a precise understanding of the facts and circumstances of the particular

Indeed, the court in the key case that both the Government and the District Court relied upon to support production, *Bank of Nova Scotia*, engaged in precisely such an analysis before ordering a bank to produce its own transaction records. *See BNS*, 740 F.2d at 829. The District Court did not. But in a case not involving the production of the provider's own records, but the emails of its customers, the analysis should have been at least as rigorous. The District Court's failure to include an international law and comity analysis has serious consequences and, if followed by other courts in this circuit (and potentially elsewhere), 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 District Court's decision to apply ECPA extraterritorially has no statutory basis either. Rather (as briefed extensively by Microsoft), ECPA contains no express statement about extraterritoriality. It makes no reference to seeking data abroad. Brief of Appellant at 18-26. Yet 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. Dec. 2, 2009)), the District Court simply noted that compelled disclosure would have an "incidental" effect, even where a foreign subsidiary subject to and regulated by foreign law

---

case").

must produce documents maintained on behalf of foreign users. Dkt. 84 at 69. The privacy intrusion, however, is more than incidental. It directly affects core privacy interests of foreign citizens, at a level protected by the Fourth Amendment's Warrant clause in the United States, and perhaps even to a greater degree in other jurisdictions where privacy is a fundamental human right.[11] *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). Rather than using ECPA as a basis to reject comity concerns, the District Court should have recognized that other sovereigns may have laws just like ECPA, which restrict the disclosure of the contents of user communications to third parties and those laws must be considered.

I. The District Court Improperly Ignored Conflicts of Laws and International Comity.

In determining that the Government may compel a United States-based parent company to turn over data in foreign countries and held by foreign subsidiaries because the parent company ordered to produce documents is in the United States, the District Court departed from established precedent by failing to

[11] *See also, e.g.*, Ireland Data Protection Act, 1988, Section 10 (providing for investigation and enforcement of violations of Irish Data Protection Act), *available at* http://www.irishstatutebook.ie/1988/en/act/pub/0025/sec0010.html#sec10(last visited Dec. 14, 2014); *Code Pénal [C.Pén.]* art. 314 (Belgium) (protecting privacy of electronic communications); [Act on the Protection of Privacy in Electronic Communications] (Finland) (516/2004) (same); *Code Pénal [C. Pén.]* 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; Poland Telecommunications Act Art. 159 (same); Spain Penal Code Section 197 (same).

consider the impact on the foreign jurisdiction and comity concerns before compelling production. The District Court's focus on the location of the parent 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 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); *see also* Fed. R. Civ. P. 44.1 (specifically allowing parties to raise foreign law issues in civil proceedings). "'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).

1. The District Court Did Not Consider All Relevant Factors Before Ordering Production

The comity analysis is a case-by-case, fact intensive inquiry that should have been employed here. "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).

Following *Aerospatiale*, courts have regularly applied a multi-factor test to examine the balance between the foreign government's interest and the United States' government's need before ordering production of materials located abroad. *See, e.g.*, *BNS*, 740 F.2d 817, 829. In *BNS*, on which the Government and the District Court rely heavily, the Government served the Miami office of a bank headquartered in Toronto with a subpoena seeking documents related to individuals and companies that were customers of the bank's branches in the Bahamas, the Cayman Islands, and Antigua. *Id.* at 820. Before ordering production of the documents in the United States, the Eleventh Circuit examined the United States' government's interest in seeking the documents, the Cayman Islands' interest in (and the strength of its laws enforcing) bank secrecy, and held that "enforcement of the subpoena and the sanctions imposed in this case are

proper under the balancing approach of Section 40" of the Restatement (Second) of Foreign Relations Law of the United States (1965).

Similarly, in *United States v. Davis*, this Court examined the Cayman Islands' interest in protecting bank secrecy before ordering a defendant to direct his bank in the Cayman Islands to produce records in response to a subpoena. *United States v. Davis*, 767 F.2d 1025, 1036 (2d Cir. 1985). In doing so, this Court considered the five factors in § 40 of the Restatement before exercising the power to hold a party in contempt for failing to respond to a subpoena for documents located abroad: (1) the vital national interests of each country that are implicated; (2) the nature and hardship of the inconsistent legal requirements imposed on the person; (3) the extent to which the required conduct is to take place in the territory of the other country; (4) the nationality of the person; and (5) the extent to which enforcement by either country can reasonably be expected to achieve compliance with that country's law. *Id.* at 1034; *see also U.S. Commodity Futures Trading Comm'n v. Trade Exch. Network Ltd.*, No. CV 12-1902 (RCL), 2014 WL 4693408, at *5 (D.D.C. June 24, 2014) (analyzing Irish Data Protection law in depth prior to compelling even an Irish party to the lawsuit to produce documents in Ireland in response to a civil discovery request); *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, 1288-90 (9th Cir. 1981).

Rather than focus solely on Microsoft's ability to access the data, the Court should have analyzed these potential conflicts of laws and applied the factors in Restatement (Third) of Foreign Relations Law § 403 (1987) before determining whether the Government could use ECPA to compel compliance. Instead of addressing these factors, the District Court's decision seems to focus almost exclusively on "the extent to which the required conduct is to take place in the territory of the other country," finding that the actual production would take place solely within the United States. This simplistic approach creates a considerable risk for providers like Microsoft and Apple who have foreign subsidiaries located abroad that control personal communications that the Government may seek. Failure to analyze these factors places the burden on providers, not the Government to balance and address complicated issues of conflicts between foreign and United States law.

2. Failing to Consider All Relevant Factors Is Troubling Where, As Here, a Provider Holds Confidential Communications on its Users' Behalf

The District Court's failure to consider comity concerns or apply the Restatement's balancing test because the intrusion is "incidental at best" is troubling for providers like Microsoft and Apple because, although providers do hold emails on users' behalf, the contents of such emails are not the business records of the foreign subsidiary (or the corporate parent). In *BNS*, by contrast, the Government sought bank records, which are undisputedly business records to which the bank is a party and in which customers have a lowered expectation of privacy. *See United States v. Miller*, 425 U.S. 435, 443 (1976) (finding lowered expectation of privacy in bank records). Further, the Bank Secrecy Act requires banks to retain deposit transactions and *affirmatively report them to the government* in certain instances—even without legal process. *See, e.g.*, 31 U.S.C. § 5313. When balancing interests then, *BNS* and *Davis* more readily found that any foreign law interest in secrecy of these business records was outweighed by United States law requiring the production of bank records in response to a subpoena.

Confidential communications like those Microsoft's foreign subsidiary holds here, are altogether different. As the Sixth Circuit observed in *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010), users have a significant privacy interest in their confidential communications distinct from the attenuated privacy

interest in bank records. Further, "emails are communications between two subscribers, not communications between the service provider and a subscriber that would qualify as business records." *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 611 (5th Cir. 2013) (citing *Warshak*). Unlike *BNS*, this case does not order the incidental production of a business record controlled by the parent, but the contents of a communication held by a foreign subsidiary and neither the parent nor the subsidiary is a party to the communication. *Warshak*, 631 F.3d at 286 (distinguishing *Miller* and noting that providers are not parties to email communications, and thus those communications are not providers' business records); *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 125 n.5 (E.D.N.Y. 2011) (noting same); *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (holding that website postings are not an ISP's business records). Even ECPA's own legislative history recognizes that contents of email communications are not business records and are distinct from the corporate records at issue in *BNS*. *See* H. Rep. 99-647 (1986) at 68 (noting that the house provided less protection to email content stored more than 180 days because it was "closer to a regular business record.")[12] Applying the

[12] Likewise, consistent with these cases, Courts have long held that, unlike regular business records, the Government must obtain a warrant before accessing property held by one party on behalf of another. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages ... are as fully guarded

same balancing test as the court applied in *BNS* could lead to a different result here where the corporation itself is not a party to the underlying communications.

3. Foreign Sovereigns Have a Strong Interest In Protecting the Privacy of Their Citizens' Communications from Governmental Intrusion.

The District Court's failure to consider the nature of the information held by providers like Microsoft and Apple and failure to apply the Restatement balancing test ignores the equities of foreign governments in protecting the privacy of their citizens' communications and the laws those sovereigns have passed to protect those interests, many of which are inconsistent with ECPA. By interpreting ECPA to override foreign law, the District Court's decision ignores issues faced by providers, like Apple, who often find themselves in true conflict of laws scenarios. Providers with a global customer base who utilize cloud computing services regularly, and subsidiaries located outside the United States that contract with and hold data on behalf of these consumers, face conflicting laws when U.S. law enforcement demands the production of data stored outside the United States.

Like the United States, other countries have passed laws—some with criminal penalties—that prevent the wiretapping or monitoring of communications in that country without obtaining legal process in that country. And some consider

---

from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles.").

the secrecy of such communication privacy a fundamental human right.[13] The European Union's Directive on protection of personal data and protection of privacy in the electronic communications sector, Data Protection Directive 95/46/EC, requires EU member countries to provide protections for electronic communications in their laws and all EU member countries have such laws.[14] 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

[13] *See, e.g.,* Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, art. 8, Nov. 1950, ETS No. 5; *Code Pénal [C.Pén.]* art. 314 (Belg.) ("*Wiretapping of Private Communications*"—Belg. Crim. Code protecting privacy of communications); Act on the Protection of Privacy in Electronic Communications (Finland) (516/2004) (Law on Protection of Privacy in Electronic Communications); *Code Pénal [C. Pén.]* art. 226 (Fr.) (France Crim. 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 (Luxembourg), *Mémorial*, A-703, June 7, 2005, *available at* www.legilux.public.lu/leg/a/archives/2005/073070 6/0730706.pdf (last visited Dec. 14, 2014); [*Poland Telecommunications Act*] art. 159 (Secrecy of Communications), *available at* http://isap.sejm.gov.pl/Download?id=WDU20140000243& type=2 (last visited Dec. 14, 2014); Spain Penal Code Section 197 (Prohibiting interception of communications), *available at* http://www.cybercrimelaw.net/Spain.html (last visited Dec. 14, 2014).

[14] *Available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (last visited Dec. 14, 2014). 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 activities.

subject to U.S. law;[15] 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. 12.965[16]; *see also* 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).[17] The United States' demands for data stored abroad are increasingly likely to violate foreign laws prohibiting data disclosure—and are likely to do so regularly.

By failing to consider conflicting laws applicable to foreign subsidiaries with control over foreign users' data, the District Court created a standard that ignores comity issues, creates conflicts of law, and discourages cooperation between governments. Interpreting ECPA to avoid analyzing foreign law issues in

---

[15] *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 Dec. 14, 2014).

[16] Unofficial English translation, *available at* http://direitorio.fgv.br/sites/direitorio.fgv.br/files/Marco%20Civil%20ingl%C3%AAs.pdf (last visited Dec. 14, 2014).

[17] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067 (last visited Dec. 14 2014). "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." *Id.*

all cases not only exacerbates conflicts issues, but threatens to violate 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 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," the District Court should have considered the full international ramifications of upholding the warrant, including its impact on providers and their foreign subsidiaries.

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

ECPA alone provides no basis to forego a comity analysis, nor does the fact that Microsoft's parent corporation, which itself does not hold the data, is located in the United States. 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.[18] ECPA contains no express statement that it has extraterritorial application. It excludes foreign governments from its definition of governmental entities.[19] 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 should 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"). ECPA should not be read to give U.S. law enforcement a unilateral right to seek data stored abroad without regard to

---

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

[19] 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."

privacy and legal protections afforded to that data in the nations where it is stored—particularly in the face of precedent like *BNS*, which uniformly examines the impact of foreign law and comity before ordering production.

CONCLUSION

Given the private nature of these communications, the comity concern and balancing analysis is even more important in cases involving Internet services companies who are likely to be the target of multiple requests for data, rather than a one-time or infrequent request. As courts have recognized, a foreign sovereign's interests may be greater where there is a continuing course of conduct—such as repeated demands for documents located abroad. *See United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080, 1086 (S.D.N.Y. 1984).

The District Court's opinion circumvents any balancing analysis, omits any consideration of Irish law, ignores the impact on foreign sovereignty, as well as the ramifications that may be faced by foreign subsidiaries and their employees who may be forced to violate local laws applying to the data that they may be deemed to control in the local jurisdiction. Finally, it ignores the "Golden Rule" of reciprocity, so effectively highlighted in the opening of Microsoft's brief. Because of these failures, this case should be reversed and remanded for the additional findings necessary to conduct a proper analysis of the effect of applying ECPA in this manner.

Dated: December 15, 2014

Respectfully submitted,

/s/ Kenneth M. Dreifach

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.

Certificate of Compliance with Type-Volume Limitation, Typeface Requirements, and Type Style Requirements

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 5,642 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 it has been prepared in a proportionally spaced typeface using Microsoft Word 2007, 14 point Times New Roman.

Dated: December 15, 2014

Signature: /s/ Kenneth M. Dreifach

Kenneth M. Dreifach
ZWILLGEN PLLC
232 Madison Ave, Suite 500
New York, NY 10016
Tel. 646.362.5590
Fax 202.706.5290

CERTIFICATE OF SERVICE

I certify that on December 15, 2014, I caused the foregoing Brief for Amicus Apple Inc. in Support of Appellant Microsoft Corporation to be served upon counsel for all parties using the CM/ECF system.

Dated: December 15, 2014

Signature: /s/ Kenneth M. Dreifach

Kenneth M. Dreifach
ZWILLGEN PLLC
232 Madison Ave, Suite 500
New York, NY 10016
Tel. 646.362.5590
Fax 202.706.5290