

# 14-2985

---

United States Court Of Appeals  
*for the*  
Second Circuit

---

MICROSOFT CORPORATION,

*Appellant,*

v.

UNITED STATES OF AMERICA,

*Appellee.*

---

Appeal from an Order of the United States  
District Court for the Southern District of New York

Loretta A. Preska, District Judge  
Case No. 13-mj-2814

---

**BRIEF OF BSA | THE SOFTWARE ALLIANCE,  
CENTER FOR DEMOCRACY AND TECHNOLOGY,  
CHAMBER OF COMMERCE OF THE UNITED STATES,  
THE NATIONAL ASSOCIATION OF MANUFACTURERS, AND  
ACT | THE APP ASSOCIATION  
AS *AMICI CURIAE* SUPPORTING APPELLANT**

---

Andrew J. Pincus  
Paul W. Hughes  
James F. Tierney  
*Mayer Brown LLP*  
*1999 K Street NW*  
*Washington, DC 20006*  
*(202) 263-3000*

Counsel for *Amici Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rules 26.1 and 29(c) of the Federal Rules of Appellate Procedure, *amicus* states as follows:

BSA | The Software Alliance has no parent company. No publicly held company owns 10% or more of its stock.

The Center for Democracy and Technology has no parent company. No publicly held company owns 10% or more of its stock.

The Chamber of Commerce of the United States of America has no parent company. No publicly held company owns 10% or more of its stock.

The National Association of Manufacturers has no parent company. No publicly held company owns 10% or more of its stock.

ACT | The App Association has no parent company. No publicly held company owns 10% or more of its stock.

**TABLE OF CONTENTS**

Corporate Disclosure Statement ..... i

Table of Authorities ..... iii

Interest of Amici Curiae ..... 1

Introduction and Summary of Argument..... 3

Argument..... 5

I. Permitting U.S. Law Enforcement To Employ Warrants To Obtain Data Stored On Non-U.S. Servers Will Impede Realization Of The Very Substantial Benefits Of Remote Data Services..... 5

    A. Business And Individual Users Of Internet-Based Data Services Entrust Their Most Intimate And Confidential Information To Third-Party Providers. .... 6

    B. Cloud Computing Technology Promises Dramatic Economic And Societal Benefits. .... 8

    C. Business And Individual Users Will Spurn Cloud Technology If Entrusting Private Information To Providers Will Result In Reduced Legal Protection..... 11

    D. Permitting Extraterritorial Warrants Under Section 2703(a) Will Deprive Cloud Users Of The Privacy Protection They Enjoy Under Local Law..... 14

    E. Endorsing The Government’s Interpretation Of Section 2703(a) Will Deprive the United States’ Economy Of Much Of The Benefit Promised By Cloud Computing. .... 18

II. Section 2703(a) Warrants Cannot Require Production Of Electronic Information Stored Outside The United States..... 21

    A. Fundamental Principles Of International Comity Preclude Unilateral Use Of Section 2703(a) To Obtain Information Stored Extraterritorially. .... 24

    B. Section 2703(a) Does Not Authorize Extraterritorial Warrants..... 30

Conclusion ..... 34

## TABLE OF AUTHORITIES

### CASES

<i>Balintulo v. Daimler AG</i> , 727 F.3d 174 (2d Cir. 2013) .....	33
<i>City of Ontario v. Quon</i> , 560 U.S. 746 (2010) .....	16
<i>In re Grand Jury Proceedings (Bank of Nova Scotia)</i> , 740 F.2d 817 (11th Cir. 1984) .....	15
<i>Hilton v. Guyot</i> , 159 U.S. 113 (1895) .....	24
<i>Kiobel v. Royal Dutch Petroleum Co.</i> , 133 S. Ct. 1659 (2013) .....	30, 32
<i>Mastafa v. Chevron Corp.</i> , 770 F.3d 170 (2d Cir. 2014) .....	33, 34
<i>Microsoft Corp. v. AT&amp;T Corp.</i> , 550 U.S. 437 (2007) .....	30
<i>Morrison v. Nat’l Australia Bank Ltd.</i> , 561 U.S. 247 (2010) .....	32, 33
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014) .....	<i>passim</i>
<i>Societe Nationale Industrielle Aerospatiale v. United States Dist. Ct. for S. Dist. of Iowa</i> , 482 U.S. 522 (1987) .....	24
<i>United States v. First Nat’l City Bank</i> , 396 F.2d 897 (2d Cir. 1968) .....	25
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012) .....	16
<i>United States v. Odeh</i> , 552 F.3d 157 (2d Cir. 2008) .....	31

**TABLE OF AUTHORITIES**  
**(continued)**

*United States v. Verdugo-Urquidez*,  
 494 U.S. 259 (1990) ..... 31

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

**STATUTES, RULES AND REGULATIONS**

Electronic Communications Privacy Act..... 17

Stored Communications Act (18 U.S.C. § 2703) .....*passim*

Fed. R. Crim. P. 41..... 31

**TREATIES, CONVENTIONS, AND FOREIGN LAW**

Agreement on Mutual Legal Assistance Between the United States  
 of America and the European Union, T.I.A.S. 10-201.1 (June 25,  
 2003)..... 27

American Convention on Human Rights, <http://tiny.cc/m55pqx> ..... 11

Convention on Cybercrime, <http://tiny.cc/vs6pqx> ..... 28, 29

Data Retention and Investigatory Powers Act, <http://tiny.cc/xf6pqx>..... 17

E.U. Council Framework Decision 2008/977/JHA (27 Nov. 2008),  
<http://tiny.cc/mq6pqx>..... 25

E.U. Directive on the Protection of Individuals in Relation to the  
 Processing of Personal Data, Directive 95/46/EC (24 Oct. 1995) ..... 25

European Convention for the Protection of Human Rights and  
 Fundamental Freedoms, <http://tiny.cc/s15pqx>..... 11

Explanatory Report to the Convention on Cybercrime (2001),  
<http://tiny.cc/it6pqx> ..... 29

International Covenant on Civil and Political Rights,  
<http://tiny.cc/445pqx> ..... 11

**TABLE OF AUTHORITIES**  
(continued)

S.S. “ <i>Lotus</i> ”, Permanent Court of International Justice, Judgment, Series A, No. 10 (7 Sept. 1927).....	25
Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, T.I.A.S. 13137 (Jan. 18, 2001).....	27, 28
<b>OTHER AUTHORITIES</b>	
Damon C. Andrews & John M. Newman, <i>Personal Jurisdiction and Choice of Law in the Cloud</i> , 73 Md. L. Rev. 313 (2013).....	8
Charles Babcock, <i>NSA’s Prism Could Cost U.S. Cloud Companies \$45 Billion</i> , InformationWeek (Aug. 14, 2013), <a href="http://tiny.cc/jn6pqx">http://tiny.cc/jn6pqx</a> .....	20
Lee Badger et al., Recommendations of the Nat’l Inst. of Standards & Tech., U.S. Dep’t of Commerce, <i>NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations</i> (2012), <a href="http://tiny.cc/nc2ubx">http://tiny.cc/nc2ubx</a> .....	9
Daniel Castro, Information Tech. & Innovation Found., <i>How Much Will PRISM Cost the U.S. Cloud Computing Industry?</i> (Aug. 2013), <a href="http://tiny.cc/k8ehpx">http://tiny.cc/k8ehpx</a> .....	18, 20, 21
Fermin Castro, <i>Best Practices for Oracle FMW SOA 11g Multi Data Center Active-Active Deployment</i> , Oracle White Paper (Sept. 2014), <a href="http://tiny.cc/2b6pqx">http://tiny.cc/2b6pqx</a> .....	14
Center for Democracy & Technology, Submission of Evidence to UK Investigatory Powers Review (Oct. 10, 2014), <a href="http://tiny.cc/8f6pqx">http://tiny.cc/8f6pqx</a> .....	17
Kenneth Corbin, <i>U.S. Cloud Firms Suffer from NSA PRISM Program</i> , CIO (July 25, 2013), <a href="http://tiny.cc/3l6pqx">http://tiny.cc/3l6pqx</a> .....	20
Council of Europe Commissioner for Human Rights, <i>The rule of law on the Internet and in the wider digital world</i> 36-37 (2014), <a href="http://tiny.cc/ur6pqx">http://tiny.cc/ur6pqx</a> .....	26

**TABLE OF AUTHORITIES**  
(continued)

Mckay Cunningham, <i>Diminishing Sovereignty: How European Privacy Law Became International Norm</i> , 11 Santa Clara J. Int'l L. 421 (2013) .....	11
<i>ECPA Reform and the Revolution in Cloud Computing: Hearing before the Subcomm. on the Constitution of the H. Comm. on the Judiciary</i> , 111th Cong. 30 (2010).....	9, 10
Letter from European Union's Article 29 Working Party to Satya Nadella, CEO of Microsoft (Sept. 22, 2014), <a href="http://tiny.cc/6q6pqx">http://tiny.cc/6q6pqx</a> .....	26
<i>Global Infrastructure</i> , Amazon Web Services, <a href="http://tiny.cc/qa6pqx">http://tiny.cc/qa6pqx</a> .....	14
Albert Greenberg et al., <i>The Cost of a Cloud: Research Problems in Data Center Networks</i> , Microsoft Research (Apr. 28, 2010), <a href="http://tiny.cc/ca6pqx">http://tiny.cc/ca6pqx</a> .....	15
H.R. Rep. No. 99-647 (1986) .....	32
Jared A. Harshbarger, <i>Cloud Computing Providers and Data Security Law</i> , 16 J. Tech. L. & Pol'y 229 (2011).....	5
Kashmir Hill, <i>How the NSA Revelations Are Hurting Businesses</i> , Forbes (Sept. 10, 2013), <a href="http://tiny.cc/kp6pqx">http://tiny.cc/kp6pqx</a> .....	20
Intelligence and Security Committee of Parliament, Report on the intelligence relating to the murder of Fusilier Lee Rigby (Nov. 2014), <a href="http://tiny.cc/nlwtqx">http://tiny.cc/nlwtqx</a> .....	17
Paul Lanois, <i>Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?</i> , 9 Nw. J. Tech. & Intell. Prop. 29 (2010).....	9, 10
Nancy J. King & V.T. Raja, <i>What Do They Really Know About Me in the Cloud?</i> , 50 Am. Bus. L.J. 413 (2013) .....	8
Danielle Kehl, New America's Open Technology Institute, <i>Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom &amp; Cybersecurity</i> (July 2014), <a href="http://tiny.cc/7dhhpq">http://tiny.cc/7dhhpq</a> .....	21

**TABLE OF AUTHORITIES**  
**(continued)**

James Manyika et al., McKinsey Global Institute, McKinsey & Company, *Disruptive Technologies: Advances that will transform life, business, and the global economy* (May 2013), <http://tiny.cc/5yh4bx> ..... 19

Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, New York Times (Mar. 21, 2014), <http://tiny.cc/om6pqx> ..... 20

NTT Communications, *NSA After-shocks: How Snowden has changed ICT decision-makers’ approach to the Cloud* (2014), <http://tiny.cc/s95pqx> ..... 14

Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L.J. 1309 (2012) ..... 7

Pew Research Internet Project, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), <http://tiny.cc/t75pqx>..... 13

Letter from Viviane Reding to Sophie in ’t Veld, Member of the European Parliament (June 24, 2014), <http://t.co/Ox2nTcQlyJ> ..... 26

Resolution & Report of the American Bar Association, No. 103 (Feb. 6, 2012)..... 25

Restatement (Third) of the Foreign Relations Law of the United States (1987)..... 25

Sand Hill Group, *Job Growth in the Forecast: How Cloud Computing is Generating New Business Opportunities and Fueling Job Growth in the United States* (2012), <http://tiny.cc/bxotbx>..... 19

Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1623 (2013) ..... 18

Joris V.J. Van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 Me. L. Rev. 487 (2014) ..... 12



**TABLE OF AUTHORITIES**  
**(continued)**

Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761 (2011)..... 8, 10

## INTEREST OF *AMICI CURIAE*

*Amici* are trade associations whose members are businesses that provide remote data services, including cloud computing services, or that rely on those services for their operations; and a public interest organization focused on privacy and civil liberties issues affecting individuals around the world who use communications networks and associated technologies.<sup>1</sup>

They are united in the view that permitting U.S. law enforcement authorities to use a warrant to reach outside the United States to seize—without complying with the legal requirements of the nation in which the information is stored—electronic information stored by non-U.S. individuals and companies will eviscerate trust in U.S. cloud services providers, hampering U.S. companies' ability to compete in this market and inflicting serious harm on the U.S. economy.

BSA | The Software Alliance is an association of the world's leading software and hardware technology companies. BSA promotes policies that foster innovation, growth, and a competitive marketplace for commercial

---

<sup>1</sup> Pursuant to Fed. R. App. P. 29(c)(5), *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici*, their counsel, and their members made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief.

software and related technologies. Many BSA members either design or operate significant cloud computing networks.<sup>2</sup>

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Chamber of Commerce of the United States (Chamber) is the world's largest business federation. It represents 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. The Chamber regularly files *amicus curiae* briefs in cases that raise issues of vital concern to the nation's business community.

The National Association of Manufacturers is the largest association of manufacturers in the United States, representing small and large

---

<sup>2</sup> BSA's members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, salesforce.com, Siemens PLM, Symantec, Tekla, The MathWorks, and Trend Micro.

manufacturers in every industrial sector, and in all 50 states. NAM advocates for sensible approaches to the law that help manufacturers compete in the global economy and create jobs across the United States.

ACT | The App Association is an international grassroots advocacy and education organization representing more than 5,000 small and mid-size app developers and information technology firms. ACT advocates for an environment that inspires and rewards innovation while providing resources to help its members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

## **INTRODUCTION AND SUMMARY OF ARGUMENT**

The U.S. government is wrong in asserting that a warrant issued under 18 U.S.C. § 2703(a) may compel a person or entity within the United States to search and copy electronic data stored in another country, cause the transmission of the copy to the United States, and turn it over to the government.

*First*, the government's position—if adopted by this Court—will significantly deter the use of remote data management technologies by businesses and individuals, particularly their use of U.S. cloud services providers, and thereby undermine a significant contributor to U.S. economic growth.

The data that companies and individuals store with data services providers consists of the most confidential information about their business plans and personal lives, respectively. If fully utilizing data services to improve manufacturing processes, and reaping the associated economic benefits, can occur only if users accept increased access to that information by the U.S. government, then businesses and individuals will be reluctant to store their information “in the cloud.” That means that the benefits of cloud computing—cheaper and more flexible data services, enhanced security, and reduced equipment costs—will not be realized, and the adverse consequences for the U.S. economy will be substantial.

*Second*, there is no basis in law for the extraordinary result sought by the United States. Affording extraterritorial reach to U.S. warrants violates fundamental principles of international comity and the plain language of 18 U.S.C. § 2703(a).

Indeed, the government’s argument here parallels its contention in *Riley v. California*, 134 S. Ct. 2473 (2014), unanimously rejected by the Supreme Court, that the search-incident-to-arrest doctrine developed in the context of physical materials such as wallets and address books should apply in the same manner to the vast amounts of information stored digitally on a cell phone. Here, the government again attempts to leverage a significant

real-world difference between physical evidence and electronic data (the latter's accessibility via the Internet) to expand its authority and diminish privacy protection—to extend warrants extraterritorially and circumvent the laws of the nation in which the data is stored.

## ARGUMENT

### **I. Permitting U.S. Law Enforcement To Employ Warrants To Obtain Data Stored On Non-U.S. Servers Will Impede Realization Of The Very Substantial Benefits Of Remote Data Services.**

“Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself.” *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). These technologies, also known generically as Internet-based data services, permit the user to conduct a wide range of data storage or processing operations that until recently were performed on the user's desktop computer or local server. The physical hardware that performs those tasks is owned by the data services provider and accessed via the Internet, but the user does not perceive any difference in his or her experience. Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law*, 16 J. Tech. L. & Pol'y 229, 232 (2011).

Internet-based data services promise very substantial economic and societal benefits and provide significant incentives for further innovation. But because the data that users store “in the cloud” includes their most

private personal information (for individual users) and confidential business information (for business users), permitting circumvention of local laws protecting users' privacy will deter use of these services, frustrating realization of their economic and societal benefits.

**A. Business And Individual Users Of Internet-Based Data Services Entrust Their Most Intimate And Confidential Information To Third-Party Providers.**

The Supreme Court's opinion in *Riley* describes the highly personal information that individuals can and do store in electronic form: email messages dating back months or even years; thousands of photographs that permit "[t]he sum of an individual's private life [to be] reconstructed"; and health, financial, political and other information that "together can form a revealing montage of the user's life." 134 S. Ct. at 2485, 2487-90.

Although *Riley* addressed this question in the context of cell phones, it recognized that all of this information may be stored securely "in the cloud" rather than in the cell phone itself. 134 S. Ct. at 2491. And the "immense storage capacity" of modern cell phones emphasized in *Riley* (*id.* at 2489) is dwarfed by the essentially limitless storage accessible through cloud technology. Individuals can and do store in the cloud *all* of their email messages, *all* of their photographs and videos, *all* of their personal financial

and health data, as well as *all* of the personal information generated by apps and other software tools.

Prior to the advent of remote data services technologies, this broad swath of information would not have been stored with a third party. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L.J. 1309, 1316 (2012). A government search of the information stored by an individual using cloud technology therefore “would typically expose to the government far more than the most exhaustive search of a house”—not just “many sensitive records previously found in the home” but also “a broad array of private information never found in a home in any form.” *Riley*, 134 S. Ct. at 2491.

The same conclusion applies to electronic information stored by businesses. A company’s most confidential business information—proprietary technology, financial data, intellectual property, business plans, manufacturing processes, acquisition plans and negotiating strategy, customer data, privileged and confidential legal advice regarding pending lawsuits and other sensitive matters—will be embodied in the emails, documents, and other electronic information stored with the company’s cloud services provider.



**B. Cloud Computing Technology Promises Dramatic Economic And Societal Benefits.**

Cloud computing is “one of the most significant technical advances for global business in this decade—as important as PCs were to the 1970s.” Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud?*, 50 Am. Bus. L.J. 413, 418 (2013) (quotation omitted). It provides significant practical benefits to the businesses and individuals that use these services.

*First*, the ability to access data from a remote data center creates significant economies of scale, resulting in reduced costs for business and individual customers. A cloud services provider can provide data backup services, business continuity, security, and other data operation functions far more efficiently than individual businesses. Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761, 1821-1822 (2011). These enhanced capabilities and reduced costs will increase productivity by hundreds of billions of dollars. *See* page 19, *infra*.

*Second*, because “companies share virtual capacity in massive clouds,” large remote data centers provide a better solution to fluctuating demand. Werbach, 60 Duke L.J. at 1822. Cloud service providers offer a pool of servers to customers who then can rapidly harness those servers’ collective computing power when needed (“scaling up”), and then rapidly release that

power when the desired task is completed (“scaling down”). Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 325 (2013). By lowering the barriers to entry for small companies, cloud computing provides new opportunities for innovation across the economy. *ECPA Reform and the Revolution in Cloud Computing: Hearing before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 111th Cong. 30 (2010) [hereinafter *The Revolution in Cloud Computing*] (statement of Michael Hintze, Microsoft Corp.); Harshbarger, 16 J. Tech. L. & Pol’y at 234-235.

*Third*, cloud computing providers’ greater scale enables them to direct vastly greater resources into network protection than a business, university, or government (particularly state and local government) attempting to manage its own computer systems in-house. Harshbarger, 16 J. Tech. L. & Pol’y at 234.

Moreover, Internet-based computing provides businesses with disaster recovery services on a much more cost-efficient basis. See Lee Badger et al., *Recommendations of the Nat’l Inst. of Standards & Tech., U.S. Dep’t of Commerce, NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations*, at Sec. 5-4 (2012), <http://tiny.cc/nc2ubx>.

*Fourth*, “[t]hanks to cloud computing, users no longer have to worry about storage capacity, memory, endless hardware purchases and upgrades, lengthy software downloads, or constant updates . . . because applications all run directly from the cloud, not from the user’s desktop computer.” Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 Nw. J. Tech. & Intell. Prop. 29, 29-30 (2010).

Allowing users to access their data using multiple devices from any location in the world that has Internet access also enhances seamless data portability—the user can create a document on a home laptop, edit it on a tablet, review it on a desktop computer at work, and then share it with colleagues around the world. *See The Revolution in Cloud Computing* 14-15 (statement of Edward W. Felten, Dir., Ctr. for Info. Tech. Policy, Princeton Univ.). And computing devices can be smaller and cheaper when they use data retrieved from network-based services. Werbach, 60 Duke L.J. at 1816.

For all of these reasons, businesses, universities, and governments are choosing to outsource their computer functions to third-party providers in order to reduce cost, enhance flexibility, and improve security.

**C. Business And Individual Users Will Spurn Cloud Technology If Entrusting Private Information To Providers Will Result In Reduced Legal Protection.**

Individuals and businesses are increasingly concerned about maintaining the confidentiality of the electronically-stored data that contains their most private information. If moving that information from a desktop computer to the cloud means that it will have reduced legal protection, then companies and individuals naturally will be more reluctant to use this new technology.

Protecting the confidentiality of personal information has historically been a significant public policy priority in many countries—partly as a reaction to totalitarian governments’ use of compilations of personal information to target individuals and groups for extermination. *See, e.g.,* McKay Cunningham, *Diminishing Sovereignty: How European Privacy Law Became International Norm*, 11 Santa Clara J. Int’l L. 421, 428-29 (2013) (observing that the “extensive accumulation of personal data by the Nazi regime” is one example of the “abuse in recent history of private and personal information” that has “undergird[ed] European vigilance in protecting personal privacy and resisting state intrusions into private life”). Indeed, privacy has the status of a fundamental human right, both in Europe and elsewhere. *See* European Convention for the Protection of Human Rights

and Fundamental Freedoms, art. 8, <http://tiny.cc/s15pqx>; International Covenant on Civil and Political Rights, art. 17, <http://tiny.cc/445pqx>; American Convention on Human Rights, art. 11, <http://tiny.cc/m55pqx>.

Recent revelations about U.S. intelligence services' access to private information have received tremendous attention around the world and led to calls for enactment of new laws and regulations to prevent access by the U.S. government inconsistent with the laws of the countries in which the information is stored or the information's owner resides. "Foreign governments, such as Germany and Brazil, have not only sought clarifications from the U.S. but have also started to propose regulatory measures designed to counter" U.S. government access to information. Joris V.J. Van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 Me. L. Rev. 487, 494 (2014). Ongoing E.U.-U.S. trade negotiations have been adversely affected by these revelations, which also have "emboldened the European Parliament to adopt poison pill amendments to the proposed EU data protection regulation" that would grant European privacy authorities oversight over requests by foreign governments. *Id.*

Disclosures regarding U.S. government access to personal information also have had a significant impact on attitudes within the United States. A recent survey found that “80% of adults ‘agree’ or ‘strongly agree’ that Americans should be concerned about the government’s monitoring of phone calls and internet communications. Just 18% ‘disagree’ or ‘strongly disagree’ with that notion.” Pew Research Internet Project, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), <http://tiny.cc/t75pqx>.

Significantly, “Americans’ lack of confidence in” the privacy of information communicated electronically “tracks closely with how much they have heard about government surveillance programs”—for five of six methods of communicating information, “those who have heard ‘a lot’ about government surveillance are significantly more likely . . . to consider the method to be ‘not at all secure’ for sharing private information with another trusted person or organization.” Pew Research Internet Project, *supra*.

These attitudes have direct consequences for the use of cloud technology. A survey of 1,000 information and communications technology (ICT) professionals demonstrates that “revelations of large-scale cyber-surveillance by US and other governments . . . have had a direct impact on how companies around the world think about ICT and cloud computing in

particular.” NTT Communications, *NSA After-shocks: How Snowden has changed ICT decision-makers’ approach to the Cloud 2* (2014), <http://tiny.cc/s95pqx>. According to that survey, “[a]round six in ten (62 percent) of those not currently using cloud feel the revelations have prevented them from moving their [data] into the cloud.” *Id.*

**D. Permitting Extraterritorial Warrants Under Section 2703(a) Will Deprive Cloud Users Of The Privacy Protection They Enjoy Under Local Law.**

Adoption by this Court of the government’s position regarding the worldwide scope of Section 2703(a) warrants would deprive businesses and individuals of the protections they otherwise would enjoy under other nations’ privacy laws, and would diminish protections under U.S. law as well.

The reduced limitations on government access to confidential information are most obvious with respect to non-U.S. customers of U.S. cloud services providers.<sup>3</sup> In the government’s view, the presence of a cloud

---

<sup>3</sup> The factual circumstances presented here—where a non-U.S. customer’s confidential information is stored on a server located outside the U.S. that is operated by a U.S.-based cloud services provider—will likely recur with increasing frequency. The efficacy of cloud computing services is substantially degraded if data is not stored near the user. Fermin Castro, *Best Practices for Oracle FMW SOA 11g Multi Data Center Active-Active Deployment*, Oracle White Paper, 7 (Sept. 2014), <http://tiny.cc/2b6pqx>. Hosting stored information “closer” to the user reduces the perceived time to load requested material and increases responsiveness to user interactions.

services provider within the United States enables the government to use a warrant to seize electronically-stored data located on servers outside the United States. If the information were stored on a non-U.S. customer's desktop or server, or with a service provider doing business only in the same country as the customer, the government acknowledges that the information could not be seized via a U.S. warrant.

The government relies on cases involving access to documents generated by a company in the course of conducting the company's own business—bank deposit slips, account records, and similar records. *See* U.S. Br. in Supp. of Magistrate Judge's Decision at 12-13 (citing *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984), and other cases).

Here, in sharp contrast, the information the government seeks is created by the user, stored by the user, and remains under the user's control. The data services company simply provides a storage service and facilitates communication between its customer and other parties. This case does *not* concern the “business records” of a cloud services provider—information

---

Providers are therefore deploying data centers globally. Albert Greenberg et al., *The Cost of a Cloud: Research Problems in Data Center Networks*, Microsoft Research (Apr. 28, 2010), <http://tiny.cc/ca6pqx>; *Global Infrastructure*, Amazon Web Services, <http://tiny.cc/qa6pqx>.



produced by the provider in the course of administering its business. To the contrary, the government seeks the records of the cloud services provider's *customer*.

The government's argument is thus the equivalent of asserting that a U.S. bank can be compelled to produce documents stored in a safe deposit box in a foreign branch because they are "the bank's records." Or that a U.S. hotel chain can be required to produce luggage stored at a hotel outside the U.S. in a room rented by non-U.S. parties. That would be an extraordinary expansion of the government's authority to obtain personal information, and a corresponding reduction in privacy protection provided by the laws of the country in which the data is located.<sup>4</sup>

Moreover, the government's approach—if upheld by this Court—is likely to produce a substantial reduction in Americans' privacy as well. Other countries will assert the same authority that the government does here, contending that their domestic legal processes may compel production of Americans' data stored in this country. Indeed, the reduction of

---

<sup>4</sup> Some argue that a user should have a reduced expectation of privacy with respect to electronic information stored with a third party. That contention was rejected by the Sixth Circuit in *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010). The Supreme Court has similarly expressed skepticism about such a reduced privacy expectation. *City of Ontario v. Quon*, 560 U.S. 746, 759-60 (2010); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Americans' privacy would be even more substantial because many countries' laws are significantly less protective of individuals' privacy than U.S. law.

This concern is not hypothetical. Just a few a months ago, the United Kingdom enacted legislation that purports to give extraterritorial effect to warrants issued by the Home Secretary to obtain the content of communications.<sup>5</sup> Even though such disclosure would violate U.S. law—because it is not authorized by the Electronic Communications Privacy Act—authorities in the United Kingdom are pressing U.S. providers to comply.<sup>6</sup> If the argument asserted by the government here were adopted by foreign governments, it could force cloud services providers within the United States into the position of choosing between complying with foreign governments' demands and U.S. privacy laws.

In sum, endorsement of the government's argument will have the immediate effect of making U.S. cloud services providers significantly less attractive to non-U.S. users—because such users' information could become

---

<sup>5</sup> Data Retention and Investigatory Powers Act, <http://tiny.cc/xf6pqx>. Section 4(2) of the Act purports to require companies based abroad to comply with interception warrants issued by the U.K. Home Secretary. An “interception warrant” can compel the disclosure of content.

<sup>6</sup> Center for Democracy & Technology, Submission of Evidence to UK Investigatory Powers Review (Oct. 10, 2014), <http://tiny.cc/8f6pqx>; Intelligence and Security Committee of Parliament, Report on the intelligence relating to the murder of Fusilier Lee Rigby 151-52 (Nov. 2014), <http://tiny.cc/nlwtqx>.

directly accessible by U.S. law enforcement authorities, who would not otherwise have direct access to the information. And the eventual consequence will be the diminution of privacy for Americans, as other countries make the same demands on cloud services providers, so that a cloud services user's private information would potentially be subject to seizure by many more governments around the world than users of non-cloud services.

**E. Endorsing The Government's Interpretation Of Section 2703(a) Will Deprive the United States' Economy Of Much Of The Benefit Promised By Cloud Computing.**

Endorsement in this case of a legal rule that has the practical effect of discouraging use of cloud computing will have a disproportionately adverse effect on U.S. businesses and the U.S. economy because the United States is now the world leader in cloud computing technology and stands to reap the greatest benefits from its adoption. *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1623, 1624 (2013).

In 2014, worldwide spending on cloud computing services will constitute an estimated \$148.8 billion—with spending in the United States reaching \$72.9 billion, or nearly half of the global market. Daniel Castro, Information Tech. & Innovation Found., *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* 6 (Aug. 2013), <http://tiny.cc/k8ehpx>. The

worldwide market is expected to reach \$207 billion and the U.S. market \$93.2 billion in 2016. *Id.*

Cloud computing will enable significant productivity savings. McKinsey estimates that by 2025 those savings will range between \$500 and \$700 billion annually. James Manyika et al., McKinsey Global Institute, McKinsey & Company, *Disruptive Technologies: Advances that will transform life, business, and the global economy* 65 (May 2013), <http://tiny.cc/5yh4bx> (full report). A different study estimates that cloud computing may save U.S. businesses as much as \$625 billion over the next five years, allowing that sum to be reinvested in new business opportunities. Sand Hill Group, *Job Growth in the Forecast: How Cloud Computing is Generating New Business Opportunities and Fueling Job Growth in the United States* 1 (2012), <http://tiny.cc/bxotbx>. Cloud computing could have a total annual economic impact of \$1.7-\$6.2 trillion by 2025. McKinsey, *Disruptive Technologies*, at 61.

U.S. companies' ability to compete in this new market will be injured substantially if businesses and individuals believe that dealing with U.S.-based companies requires the sacrifice of privacy and confidentiality protection. This is not merely supposition—the harm to U.S. companies is already being documented.

A 2013 report, issued shortly after revelations about U.S. government surveillance programs, noted that “[a]lready, domestic cloud providers have been hampered in their overseas expansion, particularly in Europe, by a deficit of trust among businesses and consumers who worry about how their data will be handled when it resides in the cloud.” Kenneth Corbin, *U.S. Cloud Firms Suffer from NSA PRISM Program*, CIO (July 25, 2013), <http://tiny.cc/3l6pqx>.

Neelie Kroes—at the time, the Vice President of the European Commission responsible for Digital Agenda—observed: “If European cloud customers cannot trust the United States government, then maybe they won’t trust U.S. cloud providers either. . . . If I were an American cloud provider, I would be quite frustrated with my government right now.” Charles Babcock, *NSA’s Prism Could Cost U.S. Cloud Companies \$45 Billion*, InformationWeek (Aug. 14, 2013), <http://tiny.cc/jn6pqx>; see also Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, New York Times (Mar. 21, 2014), <http://tiny.cc/om6pqx>; Kashmir Hill, *How the NSA Revelations Are Hurting Businesses*, Forbes (Sept. 10, 2013), <http://tiny.cc/kp6pqx>.

One study projects three-year losses to U.S. revenue as a result of recent surveillance revelations at \$21.5-\$35 billion. Castro, *How Much Will*

*PRISM Cost*, at 6. The “potential impact” of surveillance policy on U.S. businesses is an estimated loss of between “10 percent” and “20 percent of the foreign market to competitors.” *Id.* at 3. And even that estimate might be low, if “U.S. customers—not just foreign companies—would also avoid US cloud providers, especially for international and overseas business.” Danielle Kehl, New America’s Open Technology Institute, *Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity* 9 (July 2014), <http://tiny.cc/7dhhpX>.

Embracing the government’s interpretation of Section 2703(a), on top of the surveillance revelations, would magnify these trends, resulting in the further deterioration of U.S. competitiveness in the cloud computing services market.

## **II. Section 2703(a) Warrants Cannot Require Production Of Electronic Information Stored Outside The United States.**

The law enforcement concern underlying this case—the need for officials of one nation to obtain evidence or witnesses located in another—is not new. Nations’ universally recognized sovereign authority over property and individuals within their borders, and the consequent need for another country seeking evidence or witnesses to gain the cooperation of the country in which the property or individual is located in order to obtain the evidence or testimony, led the United States and other nations to enter into formal

treaties specifying mechanisms for mutual cooperation in obtaining such evidence. These treaties require law enforcement officials of the country receiving a request to invoke that nation's legal processes to enable the requesting country to obtain the evidence.

The fact that the property sought by the United States here consists of electronic data stored in another country, rather than physical pieces of paper, provides no basis for ignoring either the sovereignty of the nation in whose territory the data is stored or the long-recognized limits on extraterritorial assertions of U.S. authority. Indeed, the United States has entered into treaties specifying a variety of mechanisms for obtaining other nations' cooperation in seizing electronic data located within their territory.

The government asserts that there is no intrusion on other nations' sovereignty because the electronic data stored in Ireland can be accessed from the United States and the copying and transmission of the information controlled from the United States. Accordingly, the argument goes, this is an assertion of U.S. authority that is limited to the territory of the United States.

That contention resembles the position advanced by the U.S. government in *Riley*, which the Supreme Court rejected unanimously. The government there urged the reflexive application of the search-incident-to-

arrest principle developed in the pre-digital era, when the amount of personal information subject to government access was closely circumscribed by physical limits on what an individual could carry, to the vast amounts of personal information that digital technology permits to be stored on a cell phone. The Court held that “[a] search of the information on a cell phone bears little resemblance to the type of brief physical search” upheld in pre-digital cases. 134 S. Ct. at 2485.

The government’s assertion here that the warrant does not compel activity outside the United States because Microsoft need not send personnel to Ireland or direct its employees there to take action—as would have been true before the advent of digital technology—similarly attempts to leverage a unique attribute of electronic data (remote access made possible by the Internet) to achieve a dramatic expansion in government authority and a dramatic reduction in the respect accorded to other nations. It ignores the indisputable fact that compliance with the warrant requires actions within the territory of another nation, Ireland, and the transmission of information from Ireland into the U.S.—and thereby intrudes on Ireland’s sovereignty. As in *Riley*, the government’s argument should be rejected.

Two long-settled legal principles confirm the commonsense conclusion that a Section 2703(a) warrant does not authorize the seizure of electronic



data stored outside the United States. First, fundamental principles of international comity preclude interpreting the statute in that manner. Second, the canon against extraterritorial application of U.S. laws requires the same result.

**A. Fundamental Principles Of International Comity Preclude Unilateral Use Of Section 2703(a) To Obtain Information Stored Extraterritorially.**

“Comity refers to the spirit of cooperation in which a domestic tribunal approaches the resolution of cases touching the laws and interests of other sovereign states.” *Societe Nationale Industrielle Aerospatiale v. United States Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522, 543 n.27 (1987). “[N]either a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other,” comity “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).

The government’s position in this case is that prosecutors are free to ignore the laws of other nations and require production of data of non-U.S. individuals and businesses stored in other nations whenever the cloud services provider is subject to the jurisdiction of the United States. That

intrusion into other nations' sovereignty over their own territory is itself inconsistent with international law principles,<sup>7</sup> will inevitably produce conflicts with other nations' laws, and ignores the procedures adopted by the United States and other nations to obtain evidence located outside their borders. Comity principles therefore weigh strongly against according Section 2703(a) the expansive scope advocated by the government.

Many countries—including Ireland—have detailed laws regulating the transfer of personal data outside their territory. *See, e.g.*, E.U. Directive on the Protection of Individuals in Relation to the Processing of Personal Data, Directive 95/46/EC, Article 25 (Oct. 24, 1995) (prohibiting “transfer to a third country of personal data” if that country lacks “adequate level[s] of protection”); E.U. Council Framework Decision 2008/977/JHA (Nov. 27, 2008), <http://tiny.cc/mq6pqx>.

U.S. courts have long recognized these types of statutes in the context of civil discovery. *United States v. First Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968); *see also* Resolution & Report of the American Bar Association, No. 103 (Feb. 6, 2012) (urging U.S. courts to consider “the data protection and privacy laws of any applicable foreign sovereign”).

---

<sup>7</sup> *See generally* S.S. “*Lotus*”, Permanent Court of International Justice, Judgment, Series A, No. 10, at 18 (7 Sept. 1927); Restatement (Third) of the Foreign Relations Law of the United States §§ 432-433 (1987).

Moreover, other nations expect that their laws will be respected when the U.S. government seeks data stored within their borders. The European Union's Commissioner for Justice, Fundamental Rights, and Citizenship has stated—with respect to this case—that “where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectoral EU-US agreements authorising such transfers.” Letter from Viviane Reding to Sophie in 't Veld, Member of the European Parliament (June 24, 2014), <http://t.co/Ox2nTcQlyJ>; *see also* Letter from European Union's Article 29 Working Party to Satya Nadella, CEO of Microsoft (Sept. 22, 2014), <http://tiny.cc/6q6pqx>.

The unilateral use of U.S. process to compel transfer to the U.S. government of private personal information or proprietary business information stored with a third party outside the United States will subject third-party cloud services providers with global operations to conflicting legal obligations—the government's claim regarding the requirements of U.S. law on the one hand, and the obligations imposed by the countries in which the data is located on the other. See Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital*

*world* 36-37, 79, 80 (2014), <http://tiny.cc/ur6pqx> (specifically referencing this case and stating: “A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state . . . is exercising its jurisdiction extraterritorially” and may not do so “without the consent of the second state”). The failure by the U.S. government to respect the effect of the laws of other nations within those nations’ own territory ignores fundamental principles of comity.

Indeed, the U.S. government itself has recognized the need to respect the laws of other nations when it seeks evidence located within their borders. That is why the United States has entered into Mutual Legal Assistance Treaties (“MLATs”), which provide a means of obtaining another country’s assistance in gaining access to data stored in that country—including evidence in criminal and related matters. *See, e.g.*, Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, T.I.A.S. 13137 (Jan. 18, 2001).

Many of those treaties provide for expedited processing of requests. *See, e.g.*, Agreement on Mutual Legal Assistance Between the United States of America and the European Union, Article 4, § 7, T.I.A.S. 10-201.1 (June

25, 2003). They also are flexible, permitting the parties to assist each other through means other than those specified in the agreement—for example, the U.S.-Ireland MLAT at Articles 17 and 18 provides that a party may provide assistance “through the provisions of its national laws” and pursuant to “any bilateral arrangement, agreement, or practice which may be applicable” and “may also agree on such practical measures as may be necessary to facilitate the implementation of th[e] Treaty.”

Even more significantly, the Convention on Cybercrime (2001), to which the United States is a party, confirms the international norm that a nation seeking information stored within another country’s territory must obtain the assistance of the second country in order to seize that information. The treaty commits parties, including the United States, to respect each other’s laws and processes when seeking data across borders—establishing mechanisms for requesting the assistance of the country in which the servers containing the desired information are located. It provides for general mutual assistance where there is no applicable international agreement (Article 27), specifically addresses assistance in preserving and obtaining access to stored data (Articles 29 and 31), and requires each signatory nation to designate a point of contact “available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance” with

regard to, among other things, “the preservation of data” and “the collection of evidence” (Article 35).<sup>8</sup>

Particularly relevant in this case is the fact that the Convention on Cybercrime specifically does *not* authorize the use of domestic warrants to obtain electronic data stored extraterritorially. Article 32, which addresses “[t]rans-border access to stored computer data,” states that one nation may obtain such data without the consent of the other nation only if the data is publicly available or the requesting nation “obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the [requesting nation] through that computer system.” Public availability and voluntary consent were the only circumstances “in which all agreed that unilateral action [by the requesting nation] is permissible.” *Explanatory Report to the Convention on Cybercrime* ¶ 293 (2001), <http://tiny.cc/it6pqx>.

The Convention thus recognizes that a government’s unilateral demand for production of electronic information stored extraterritorially creates conflicts with other nations’ laws and that generally recognized international law principles do not provide for enforcement of a nation’s unilateral demand for such information.

---

<sup>8</sup> The text of the Convention is available at <http://tiny.cc/vs6pqx>.

MLATs and the Convention on Cybercrime provide means of obtaining that information that accord with comity principles by avoiding conflicts with other nations' legal regimes. Given the conflict with other nations' laws that the government's approach would produce and the availability of alternative means to obtain information without generating such conflicts, comity principles plainly require rejection of the government's position.

**B. Section 2703(a) Does Not Authorize Extraterritorial Warrants.**

The “canon of statutory construction known as the presumption against extraterritorial application” provides that “[w]hen a statute gives no clear indication of an extraterritorial application, it has none.” *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013). The canon “reflects the ‘presumption that United States law governs domestically but does not rule the world.’” *Id.* (quoting *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454 (2007)). Interpreting the Stored Communications Act to permit the U.S. government to force Microsoft to reach into data centers outside the United States and copy data stored there would constitute just such an impermissible attempt to “rule the world.”<sup>9</sup>

---

<sup>9</sup> Under Section 2703(a), a warrant is required to compel Microsoft to take actions within the United States, but here key steps occur outside the United States and the warrant cannot compel those actions for the reasons discussed in the text.

Nothing in the text of Section 2703(a) provides the requisite “clear indication” that the provision authorizes the use of warrants to seize data stored outside the United States. To the contrary, the provision expressly states that service providers can be compelled to disclose the contents of communications “only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.”<sup>10</sup> The relevant rule—Rule 41—is limited, with exceptions not relevant here, to property located within the United States,<sup>11</sup> and expressly defines “property” to include “information.”<sup>12</sup>

The Rule’s territorial limit reflects the longstanding principle that “warrants” have only domestic application. *E.g., United States v. Odeh*, 552 F.3d 157, 169-70 (2d Cir. 2008); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 279 (1990) (Stevens, J., concurring) (“American magistrates have no power to authorize” searches of non-citizens’ homes in foreign

---

<sup>10</sup> Section 2703(b)’s authority for the use of a warrant to obtain communication contents similarly refers to “a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.”

<sup>11</sup> Fed. R. Crim. P. 41(b). A 2002 amendment permits issuance of warrants for property located outside the United States in terrorism-related investigations. Fed. R. Crim. P. 41(b)(3).

<sup>12</sup> Fed. R. Crim. P. 41(a)(2)(A).



jurisdictions). Section 2703 thus incorporates the Rule’s limitation to seizures of information located within the United States.<sup>13</sup>

When a statute does not apply extraterritorially, a court must assess whether the particular proposed application of the statute is domestic and therefore permissible, or extraterritorial and therefore unauthorized. The presence of some connection to the United States does not satisfy this standard. *Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. 247, 266 (2010) (“[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.”); *see also Kiobel*, 133 S. Ct. at 1669 (question is whether the proposed application of the statute “touch[es] and concern[s] the territory of the United States . . . with sufficient force to displace the presumption against extraterritorial application”). The critical inquiry is whether the conduct that is “the ‘focus’ of congressional concern” occurs within the United States. *Morrison*, 561 U.S. at 266.

Applying this test in the context of the law addressed in *Kiobel*—the Alien Tort Statute—this Court has held that the determinative factor in ascertaining whether a claim under the statute is extraterritorial and

---

<sup>13</sup> Section 2703’s legislative history confirms that Congress “d[id] not intend that the Act regulate activities conducted outside the territorial United States” and “intended [it] to apply only to access within the territorial United States.” H.R. Rep. No. 99-647, at 32-33 (1986).

therefore impermissible is “the site of the alleged violations of customary international law,” because the focus of that statute is violations of international law. *Mastafa v. Chevron Corp.*, 770 F.3d 170, 184 (2d Cir. 2014). The fact that other conduct not constituting the international law violation might have occurred in the United States is irrelevant. *Id.*; accord *Balintulo v. Daimler AG*, 727 F.3d 174, 189-92 (2d Cir. 2013).

Similarly, the Supreme Court in *Morrison* held that “the focus of the Exchange Act is not upon the place where the deception originated, but upon purchases and sales of securities in the United States.” 561 U.S. at 266. The fact that the plaintiffs purchased the securities in question outside the United States rendered the claim extraterritorial, and therefore impermissible, even though the complaint alleged that the fraud injuring the plaintiffs originated in the United States. *Id.*

The focus of the Stored Communications Act is the storage of electronic communications. The relevant question for determining whether a proposed application of Section 2703(a) is extraterritorial is therefore the place where those communications are stored. If they are stored outside the United States, then any other connection between the United States and the stored communication—such as whether the company storing the communication is a U.S. domiciliary or has the technical ability to access the communications

from within the United States—is irrelevant. *Cf. Mastafa*, 770 F.3d at 184 (fact that defendant was a U.S. corporation is irrelevant in determining whether claim is extraterritorial).

In sum, a long line of Supreme Court decisions establish that Section 2703(a) does not apply extraterritorially. A warrant obtained pursuant to that provision therefore is not by itself sufficient to compel a service provider to turn over communications stored outside the United States.

### **CONCLUSION**

The district court's contempt order should be vacated and the case remanded with instructions to grant Microsoft's motion to vacate the warrant.

Respectfully submitted,

/s/ Andrew J. Pincus

Andrew J. Pincus

Paul W. Hughes

James F. Tierney

*Mayer Brown LLP*

*1999 K Street NW*

*Washington, DC 20006*

*(202) 263-3000*

Counsel for *Amici Curiae*

Dated: December 15, 2014

**CERTIFICATE OF COMPLIANCE WITH RULE 32(a)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), undersigned counsel certifies that this brief:

(i) complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B)(i) because it contains 6,987 words, including footnotes; and

(ii) 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).

Dated: December 15, 2014

/s/ Andrew J. Pincus  
Andrew J. Pincus

**CERTIFICATE OF SERVICE**

I certify that on December 15, 2014, I served the foregoing amicus brief on all counsel via the Court's ECF system.

Dated: December 15, 2014

/s/ Andrew J. Pincus  
Andrew J. Pincus  
Mayer Brown LLP  
1999 K Street NW  
Washington, DC 20006