THE HIGH COURT

COMMERCIAL

Record No. 2016/4809P

BETWEEN

THE DATA PROTECTION COMMISSIONER

Plaintiff

- and -

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

Defendants

AFFIDAVIT OF THOMAS BOUÉ

EXHIBIT "TB1"

Referred to in the Affidavit of Thomas Boué sworn this 22 day of June 2016.

THOMAS BOUÉ

Deponent

Sarah Fleming

Practising Solicitors/
Commissioner for Oaths

William Fry
Solicitors
2 Grand Canal Square
Dublin 2
www.williamfry.com

024205.0001.DCU.JFM

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

TABLE OF AUTHORITIES

CASES

TABLE OF AUTHORITIES
(continued)

STATUTES, RULES AND REGULATIONS

TREATIES, CONVENTIONS, AND FOREIGN LAW

TABLE OF AUTHORITIES
(continued)

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

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.[1]

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

---

[1] 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.[2]

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

---

[2] 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.[3] In the government's view, the presence of a cloud

---

[3] 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.[4]

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

---

[4] 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.[5] 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.[6] 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

---

[5] 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.

[6] 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,[7] 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").

---

[7] *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).[8]

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.

---

[8] 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."[9]

---

[9] 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."[10] The relevant rule—Rule 41—is limited, with exceptions not relevant here, to property located within the United States,[11] and expressly defines "property" to include "information."[12]

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

---

[10] 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."

[11] 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).

[12] 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.[13]

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

[13] 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

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 OF AMICUS CURIAE IRELAND

Peter D. Stergios
McCarter & English, LLP
245 Park Ave., 27th Floor
New York, NY 10167
Tel. (212) 609-6800

Charles D. Ray
McCarter & English, LLP
CityPlace I
Hartford, CT 06103
Tel. (860) 275-6700

Counsel for Amicus Curiae Ireland

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATEMENT REGARDING AMICUS CURIAE

Ireland is an internationally-recognized sovereign nation state. The United States recognizes and maintains diplomatic relations with Ireland.

The warrant under appeal orders Appellant to produce in the United States documents that it maintains reside in Ireland. Ireland has a genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its territory.

Ireland files this *amicus curiae* brief with the consent of both parties, and pursuant to a Motion for Leave To File *Amicus* Brief dated December 15, 2014.

STATEMENT OF THE AMICUS CURIAE[1]

The subject of this appeal is an oral ruling unsupported by a written opinion. At pages 54 through 60 of that transcript of the hearing in the court below (A317-A323), the parties and the Court discuss *inter alia* the potential impact of the relevant subpoena on Irish sovereignty.

Ireland respectfully makes three points in this *amicus* brief.

First, Ireland does not accept any implication that it is required to intervene into foreign court proceedings to protect its sovereignty.

Second, Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and, in this regard, Ireland and the United States are parties to a treaty addressing the subject of this appeal.

Third, Ireland notes that no party below cited or argued the Supreme Court of Ireland case of *Walsh v National Irish Bank* [2013] 1 ESC 2, which may be relevant to the subject of the appeal.

---

1 Pursuant to Rule 29(c)(5) of the Federal Rules of Appellate Procedure and Local Rule 29.1(b), the *amicus curiae* states that:

(A) A party's counsel has not authored this brief in whole or in part;

(B) Neither a party nor a party's counsel contributed money that was intended to fund preparing or submitting this brief; and

(C) No person – other than the *amicus curiae*, its members, or its counsel – contributed money that was intended to fund preparing or submitting this brief.

ARGUMENT

I. National Sovereignty Is Never Waived By Non-Intervention in Foreign Domestic Court Proceedings

The implication of Appellee's argument at Tr. 54-60 (A317-A323) (and also Tr. 31-32 (A294-A295)) is that any conflict between United States and Irish law is speculative unless Ireland actively asserts it within United States legal proceedings. Ireland does not accept any implication that it is required to intervene into foreign court proceedings to protect its sovereign rights in respect of its jurisdiction, or that Ireland not intervening is evidence of consent to a potential infringement thereof. Ireland respectfully asserts that foreign courts are obliged to respect Irish sovereignty (and that of all other sovereign states) whether or not Ireland is a party or intervener in the proceedings before them. *See, e.g.*, *Restatement 3d of the Foreign Relations Law of the U.S.* § 442(2) (describing appropriate deference to conflicts in disclosure law between sovereign states).

II. Ireland Is Willing To Apply The MLAT Process To This Warrant

In the proceeding below, the parties and district court at length discussed the potential applicability to this warrant of the relevant Mutual Legal Assistance Treaty between Ireland and the United States. Tr. at 34-36, 60-62 (A297-A299, A323-A325).

Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and, in this regard, has enacted legislation giving effect to a large number of international treaties and instruments providing for mutual legal assistance in criminal matters. As noted by both the parties and other *amici*, Ireland and the United States are parties to a treaty addressing the subject of this appeal. Ireland would be pleased to consider, as expeditiously as possible, a request under the treaty, should one be made.[2]

---

[2] The law enabling Ireland to provide mutual legal assistance to, and seek mutual legal assistance from, other countries is contained in the Criminal Justice (Mutual Assistance) Act 2008. In brief, the Act primarily includes provisions:

- relating to the sharing of information and monitoring of financial transactions for criminal investigation purposes;
- enabling the enforcement in Ireland of orders for the freezing and confiscation of property that could be evidence or the proceeds of crime;
- permitting the Minister to request an Irish court to take evidence for use in criminal proceedings or a criminal investigation in another country;
- enabling the transfer of a prisoner to give evidence or assist a criminal investigation in Ireland and enabling the transfer of a prisoner to give evidence or assist an investigation outside Ireland;

III. The Supreme Court of Ireland case of *Walsh v National Irish Bank* [2013] 1ESC 2

It appears the potentially relevant Supreme Court of Ireland case of *Walsh v. National Irish Bank* [2013] 1ESC 2 was not considered during the underlying proceedings.

It is incumbent on Ireland to acknowledge that the Supreme Court of Ireland did make an order in the case of *Walsh v National Irish Bank* [2013] 1ESC 2, [3] which may be of some relevance to the proceedings before this Court. In *Walsh*,

---

- enabling the Minister to request an Irish court to summon a witness to give evidence for use outside Ireland by a television link or telephone link;
- permitting the taking of identification evidence in Ireland for use in criminal proceedings or criminal investigations outside Ireland;
- empowering the Minister to cause a document requiring a person to appear as a defendant or witness in criminal proceedings in another country or any other document issued by a court or authority in another country in relation to criminal proceedings to be served on the person in Ireland;
- providing for a request from other countries for the examination of an object or site in Ireland for such purposes to be complied with;
- enabling requests for the restitution of stolen property to be made to other countries and such requests to be made to Ireland; and,
- enabling representatives of other countries to be present at the execution of a request in Ireland and enabling members of the Garda Síochána (Irish police) to be present at the execution of a request in other countries.

See Criminal Justice (Mutual Assistance) Act of 2008, No. 7 of 2008, *available at* http://www.irishstatutebook.ie/2008/en/act/pub/0007/index.html.

[3] The *Walsh* decision is available at http://www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/eafa348512d6d95a80257afe00587a09?OpenDocument.

the taxation authorities in Ireland (the Revenue Commissioners) applied under section 908 of the Taxes Consolidation Act 1997 for an order for disclosure of details of an account with the National Irish Bank. *Walsh v National Irish Bank* [2013] 1ESC 2, ¶ 1.2 The branch in question was situated outside Ireland (in the Isle of Man, which is a British crown dependancy). *See id.* The High Court (the trial-level court) refused the order on the grounds that this is a matter for the courts of the Isle of Man. *See id.* ¶¶ 4.1 to 4.5.

The Supreme Court of Ireland held that, *in the absence of alternative means* of obtaining information required for a criminal or similar investigation, there may be circumstances in which an Irish court would order the production of records from an Irish entity on foreign soil, but would do so only after being competently apprised of whether the execution of the order would violate the law of the foreign sovereign. *See id.* ¶¶ 7.6, 9.3-9.6.

A significant factor in the case was that the branch did not have a separate corporate identity:

> *The fact is that the Bank chose to conduct its business (or at least part of it) in the Isle of Man by means of a branch rather than by means of a separate legal entity incorporated in the Isle of Man and operating as part of the same group of companies. Doubtless, there were good reasons for the Bank choosing so to do. However, such choices have consequences. The fact remains that the same legal entity was doing business in the Isle of Man through one of its branches as did business through its ordinary branch network in Ireland. The banking obligations undertaken through the Isle of Man branch (such as the obligation to repay monies deposited) were obligations of the Bank in*

> *just the same way as obligations undertaken through a branch in Dublin or elsewhere in Ireland.*

Id. ¶ 5.6 (emphasis added).

As noted above, there is a Treaty in place between the United States and Ireland which addresses the subject of the appeal.

In *Walsh*, the Irish Supreme Court accepted that, in general, a court does not order inspection of documents in a foreign country and that, where possible courts should avoid coming into conflict. However on the central point whether it had power to order production of documents by an Irish registered company by one of its branches situated in a foreign country, the Supreme Court found that it did. The Supreme Court found that the Taxes Consolidation Act empowers the Irish taxation authorities to seek an order that an Irish bank produce records of accounts held by its customers wherever the information is situated.

It appears that in certain circumstances, an Irish court is prepared to order the disclosure by an Irish corporation of information in its possession, notwithstanding that the information is physically located in another jurisdiction, provided certain matters are demonstrated.

CONCLUSION

Ireland does not accept any implication that it is required to intervene into foreign court proceedings to protect its sovereignty. Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and would be pleased to consider, as expeditiously as possible, a request under the treaty, should one be made.

RESPECTFULLY SUBMITTED,

By: */s/ Charles D. Ray*
Charles D. Ray
McCARTER & ENGLISH, LLP
CityPlace I
Hartford, CT 06103
Tel.: 860-275-6700

Peter D. Stergios
McCARTER & ENGLISH, LLP
245 Park Ave., 27th Floor
New York, New York 10167
Tel.: 212-609-6800

Counsel for Amicus Curiae Ireland

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(c) of the Federal Rules of Appellate Procedure, the undersigned counsel hereby certifies that:

1. This brief complies with the type-volume limitations of Rule 32(a)(7)(B) of the Rules of Appellate Procedure in that this brief contains 1,579 words, excluding parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Microsoft Word 2000 in Times New Roman, 14 point font.

/s/ Charles D. Ray
Charles D. Ray
McCARTER & ENGLISH, LLP
CityPlace I
Hartford, CT 06103
Tel: 860-275-6700

Peter D. Stergios
Charles D. Ray
McCARTER & ENGLISH, LLP
245 Park Ave., 27th Floor
New York, New York 10167
Tel.: 212-609-6800

Counsel for Amicus Curiae Ireland

CERTIFICATION OF SERVICE

I hereby certify that a true and accurate copy of the foregoing brief was filed electronically. Notice of this filing will be sent by electronic mail to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF system.

/s/ Charles D. Ray
Charles D. Ray
McCARTER & ENGLISH, LLP
CityPlace I
Hartford, CT 06103
Tel: 860-275-6700

Peter D. Stergios
Charles D. Ray
McCARTER & ENGLISH, LLP
245 Park Ave., 27th Floor
New York, New York 10167
Tel.: 212-609-6800

Counsel for Amicus Curiae Ireland

List of BSA's Members

Adobe Systems, Inc.

ANSYS, Inc.

Apple Inc.

Autodesk, Inc.

Bentley Systems, Inc.

CA Technologies

CNC Software, Inc.

DataStax, Inc.

Dell Inc.

IBM Corporation

Intuit Inc.

Microsoft Corporation

Minitab Inc.

Oracle

salesforce.com

SAS Institute

Siemens PLM Software Inc.

Splunk

Symantec Corporation

Tekla

The MathWorks, Inc.

Trend Micro

Workday

883400

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF CONSUMER AND REGULATORY AFFAIRS
BUSINESS REGULATION ADMINISTRATION

CERTIFICATE

THIS IS TO CERTIFY that all applicable provisions of the DISTRICT OF COLUMBIA NONPROFIT CORPORATION ACT have been complied with and accordingly, this CERTIFICATE of INCORPORATION is hereby issued to

BSA BUSINESS SOFTWARE ASSOCIATION, INC.

as of JULY 14TH , 1988 .

Donald G. Murray
Director

Henry C. Lee, III
Administrator
Business Regulation Administration

Vandy L. Jamison, Jr
Assistant Superintendent of Corporations
Corporations Division

Marion Barry, Jr.
Mayor

ARTICLES OF INCORPORATION

OF

BSA BUSINESS SOFTWARE ASSOCIATION, INC.

To: Department of Consumer and Regulatory Affairs
Washington, D.C. 20001

We, the undersigned natural persons of the age of eighteen years or more, acting as incorporators of a corporation under the NON-PROFIT CORPORATION ACT (D. C. Code 1981 edition, Title 29, Chapter 5), adopt the following Articles of Incorporation:

FIRST: The name of the corporation is BSA Business Software Association, Inc.

SECOND: The period of duration is perpetual.

THIRD: The purposes for which the corporation is organized are not for profit and are

(a) to advance free and open trade in legitimate business software by combating piracy, promoting strong intellectual property laws, and reducing trade barriers, through means including but not limited to (i) aiding the enforcement of relevant laws by working with local governments and law enforce-ment agencies, instituting private civil actions, publicizing such actions, and conducting and coordinating educational campaigns to improve the attitude of users, and (ii) supporting the enactment of strong intellectual property laws by working with U.S. and foreign governments and urging them to combat piracy, reduce trade barriers, and maintain high intellectual property standards;

(b) to make members aware of other government--related matters that may have a significant impact on the members, and to act on such matters as the members determine;

(c) to engage in such other activities as are necessary and proper to further the aforesaid purposes and to advance in every lawful manner the interests of the business software industry, its employees, and the public.

FOURTH: The corporation shall have members.

FILED

JUL 14 1988

BY:

FIFTH: There may be one or more classes of members. The designation of each class of members, the manner of election or appointment, and the qualifications and rights, including voting rights, of the members of each class shall be set forth in the bylaws.

SIXTH: The affairs of the corporation shall be managed by a Board of Directors. The number of directors and the manner in which directors shall be elected or appointed shall be set forth in the bylaws, except that the initial Board of Directors is named herein.

SEVENTH: The corporation shall have such powers as are provided by law and these articles of incorporation. Notwithstanding any other provision hereof, the corporation shall not engage in any activities that are inconsistent with the qualification of the corporation as a business league exempt from federal income tax in accordance with the provisions of the Internal Revenue Code of 1954 or any successor thereto, and no part of the net earnings of the corporation shall inure to the benefit of any private individual.

EIGHTH: The address, including street and number, of the corporation's initial registered office is CT Corporation System, 1030 - 15th Street, N.W., Washington, D.C. 20005, and the name of its initial registered agent at such address is CT Corporation System.

NINTH: The number of directors constituting the initial board of directors is six and the names and addresses, including street and number, of the persons who are to serve ^Las the initial directors until the first annual meeting or until their successors be elected and qualified are:

NAME	ADDRESS
Ms. Gwen Glessner	Aldus Corporation Suite 200 411 First Avenue South Seattle, WA 98104
Thomas M. Lemberg, Esq.	Lotus Development Corp. 55 Cambridge Parkway Cambridge, MA 02142
William H. Neukom, Esq.	Microsoft Corporation 16011 Northeast 36th Way Box 97017 Redmond, WA 98073-9717
Christopher Record, Esq.	Autodesk, Inc. 2320 Marinship Way Sausalito, CA 94965

R. Duff Thompson, Esq.

WordPerfect Corporation
1555 North Technology Way
Orem, Utah 84057

Stanley P. Witkow, Esq.

Ashton-Tate Corporation
20101 Hamilton Avenue
Torrance, CA 90502

TENTH: The name and address, including street and number, of each incorporator is:

NAME	ADDRESS
JANIS LARUE	11 Linnaean St Cambridge MA 02138
Christine Ciotti	17 Washington Street, Newton MA. 02158
Irwin N. Barnes	501 Beacon St., Newton, MA 02167

Janis LaRue
Christine Ciotti
Irwin N. Barnes
Incorporators

Date July 13, 1988

Commonwealth of)
MASSACHUSETTS) SS
MIDDLESEX)

I, M. GERALDINE ATKINS, a Notary Public, hereby certify that on the 13th day of July, 1988, personally appeared before me JANIS LARUE, CHRISTINE CIOTTI and IRWIN N. BARNES, who being first duly sworn, declared that they signed the foregoing document as incorporators, and that the statements therein contained are true.

(Seal)

M. Geraldine Atkins
Notary Public
M. GERALDINE ATKINS
My Commission expires: 8.25.89

DISTRICT OF COLUMBIA

DEPARTMENT OF CONSUMER AND REGULATORY AFFAIRS

I hereby certify that this is a true and complete copy of the document filed in this office, the Corporations Division of the Business Regulation Administration, and that this document was admitted to record in File # 58340

Date of Certification 3-16 2001

ACT. ASST.

Superintendent of Corporations

William L. Adler

ITI

February 16, 2016

The EU-U.S. Privacy Shield: What's at Stake

On October 6, 2015, the Court of Justice of the European Union (CJEU) effectively invalidated the Safe Harbor Framework, which for 15 years had enabled thousands of companies to provide data services for their customers and to conduct their own operations. Since that time, and building on progress made over the preceding two years, EU and U.S. negotiators worked to reach a resolution on a new data transfer mechanism. On February 2, 2016, they reached a deal called the EU-U.S. Privacy Shield. The agreement helps preserve the largest trading relationship in the world, which is valued at half a trillion dollars of commerce annually, represents half of all U.S. investments abroad, and directly employs 3.5 million Americans.

However, the agreement faces a stringent, months-long approval process involving reviews by stakeholders across the EU and its Member States. The aim of this document is to help stakeholders better understand the economic impacts and consequences of a world without a durable EU-U.S. data transfer mechanism, focusing on the impacts to global trade, Member State economies, and thousands of companies' operations.

Data Flows are Essential to the EU-U.S. Trade Relationship

- Cross-border data flows between the United States and Europe are the highest in the world, 50 percent higher than data flows between the United States and Asia, and almost double the data flows between the United States and Latin America, according to the Brookings Institution.
- 51 percent of U.S. firms that relied on the Safe Harbor Framework did so in order to process data on European employees - for example, transferring the personnel files of overseas workers to the United States for human resource purposes - and most of these firms are in traditional industries.
- In 2012, the United States exported $140.6 billion worth of digitally deliverable services to the EU and imported $86.3 billion worth of such services.
- In 2011, the supply of digitally deliverable services through U.S. affiliates in Europe was worth $312 billion, while Europe supplied $215 billion worth of digitally deliverable services through U.S. affiliates.
- UNCTAD estimates that about half of all services trade is enabled by the ICT sector, including cross-border flow of data. Applied to the EU, this would mean about $600 billion (€465 billion) could depend on the openness of the digital economy (nearly six times total EU automotive exports).

Potential Macroeconomic Costs of Disruption

- If services trade and cross-border data flows are seriously disrupted – for example, if Europe's regulators and courts refuse to recognize binding corporate rules (BCRs), model contract clauses (MCCs), and the EU-U.S. Privacy Shield – the negative impact on EU GDP could reach -0.8 to -1.3 percent. This is roughly equivalent to three to four times the economic decline that Europe experienced during the 2012 euro crisis.

- EU services exports to the United States would be expected to drop by -6.7 percent due to loss of competitiveness, while EU manufacturing exports to the United States could decrease by up to 11 percent, depending on the industry.
- The direct welfare effects in such a scenario for consumers would be equivalent to a loss of $102-170 billion (€78-131 billion), which is up to $338 (€260) per EU citizen, or $1,353 (€1,041) for a household of four people.

Examples of impacts on companies [if no legal basis exists to transfer data from Europe]

- EU-based online advertising firms that send data to U.S. partners to generate ads or to draft email marketing campaigns may no longer be able to do so.
- Business-to-business software providers may no longer be able to process the financial, tax, and contact data of partner European small and medium-sized enterprises (SMEs).
- U.S.-based banks may no longer be able to lend in Europe because they are unable to access the data needed to manage their risk profiles.
- Insurance companies may not be able to write new policies in European or U.S. markets without access to the data and the digital documents of their policyholders.
- U.S.-based industrial design firms may no longer be able to license their products to European manufacturers, because they will be unable to easily send schematics across borders.
- Online communities of European coders collaborating with others outside of the EU may no longer be able to write open-source software, where the code is hosted on U.S. servers.
- Business-to-consumer "distance-learning" companies based in the United States may no longer be able to authenticate the contact and payment information of Europeans who subscribe to online training courses.
- Business-to-consumer travel and tourism companies based in the United States may be unable to receive flight itineraries and hotel reservations of European customers booking through their EU subsidiaries.
- U.S.-based clinical software firms may no longer be able to integrate reports from hospitals, universities, physicians' offices, and clinical research organizations on medical device trials being held in the EU.
- Identity document authenticators based in the United States may not be able to assist European immigration or law enforcement officers seeking to test passports they have scanned for additional accuracy.

About ITI. The Information Technology Industry Council (ITI) is the global voice of the tech sector, celebrating its 100th year in 2016 as the premier advocacy and policy organization for the world's leading innovation companies. In both the U.S. and in countries around the world, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more and follow us on Twitter for the latest ITI news @ITI_TechTweets.

- ***Samsung Elecs. v. Apple, Inc.* (S. Ct. June 8, 2016).** BSA submitted an amicus brief **in support of neither party** to provide the Supreme Court information about how design patents are used in the software industry to promote innovation.

- **In the Matter of the Search of an Apple Iphone Seized During the Execution of a Search warrant (U.S. District Court, Central District of California, March 3, 2016).** This case involved an attempt by the U.S. Government to compel Apple to assist in providing access to an encrypted Iphone of potential relevance to a terrorism investigation. BSA submitted this amicus brief to highlight the privacy and security risks that would be created if Apple were required to design a means to undo encryption protections.

- ***Thales Visionix, Inc., v. United States* (Fed. Cir. Jan. 21, 2016)**. BSA submitted an amicus brief **in support of neither party** to explain how innovation is incentivized by patents in the software industry and articulate a workable patentability standard for software-related inventions.

- *Halo Elecs. Inc. v. Pulse Elecs. Inc.* (S. Ct. Jan. 20, 2016). Under U.S. patent law, a plaintiff can receive enhanced damages if the defendant acted willfully. BSA submitted this amicus brief to support a willfulness standard that would deter infringement without chilling innovation.

- *McRo, Inc. d/b/a Planet Blue v. Bandai Namco Games America Inc.* (Fed. Cir. Mar. 6, 2015). This case also involved the proper standard for evaluating patentability of software-related inventions. BSA's brief explained the importance of patent protection for software innovation.

- *Microsoft Corp. v. United States* (2d Cir. Dec. 14, 2015). BSA submitted this amicus brief to oppose U.S. law enforcement's use of warrants to obtain data stored on non-U.S. servers. BSA's brief explained how the extraterritorial reach could harm the adoption of cloud computing technology.

- ***United States v. Nosal* (9th Cir. Dec. 9, 2014).** BSA submitted an amicus brief **in support of neither party**. U.S. law makes it illegal for an unauthorized person to access a computer. The brief explained how cloud computing functions, so that the court would not adopt a per se rule making it illegal when using an authorized user's credentials to access a computer.

- *ClearCorrect Operating Inc. v. ITC* (Fed. Cir. Oct. 17, 2014). The International Trade Commission (ITC) can prevent the importation of articles that infringe IP rights. The ITC applied this authority to digital goods. BSA's brief argued that the ITC's jurisdiction is and should be limited to tangible goods.

- ***American Broadcasting Corp. v. Aereo* (S. Ct. Mar. 3, 2014)**. This case had to do with whether an over-the-top provider of video services was infringing copyright by transmitting programs. BSA submitted an amicus brief **in support of neither party** to explain how an overly interpretation of the Copyright Act could harm cloud computing more generally.

- *Alice Corp. Pty., Ltd. v. CLS Bank Int'l* (S. Ct. Feb. 27, 2014). BSA submitted this amicus brief to explain the societal benefits of software patentability.

- *Highmark v. Allcare Health Mgmt. Sys.* (S. Ct. Jan. 24, 2014). This case and *Octane* (below) related to the standard for shifting attorneys fees to the prevailing party in patent litigation. BSA's amicus brief explained the problems flowing from abusive patent litigation and why, as a result, the ability to shift fees to the prevailing party is important.

- *Octane Fitness LLC v. Icon Health & Fitness, Inc.* (S. Ct. Dec. 9, 2013). This case covered similar issues to *Highmark*, above.

- *Kornkrumpf v. Adobe Systems Inc.* (Fed. Cir. July 5, 2013). This case questioned whether the grant of a copyright license covering software should be considered a "sale" rather than a license. BSA's amicus brief explained the importance of licensing to the software industry's ability to meet consumer demands.

- *CBT Flint Partners, LLC v. Return Path, Inc.* (Fed. Cir. May 3, 2013). This case involved the cost of discovery in patent litigation. BSA argued that some discovery costs should be shifted to the plaintiff in patent litigation cases to deter meritless lawsuits.

- *Apple Inc. v. Motorola* (Fed. Cir. Mar. 20, 2013). Injunctions are typically available to prevent ongoing patent infringement. BSA argued that injunctions are not appropriate if the patent owner has committed to licensing patents on reasonable and non-discriminatory ("RAND") terms, as part of the patentee's involvement in a standard-setting process.

- *Bowman v. Monsanto Co.* (S. Ct. Jan. 23, 2013). This case dealt with the exhaustion of a patent right after a product is sold. BSA argued that patent protection should continue to exist in the technology after the sale and that, in the case of software, it would chill innovation to exhaust the patent right and permit copying of the patented technology.

- *CLS Bank Int'l v. Alice Corp. Pty. Ltd.* (Fed. Cir. Dec. 7, 2012). [This case was the intermediate court decision that led to the *Alice* case in the Supreme Court discussed above.]

- *Kirtsaeng v. John Wiley & Sons, Inc.* (S. Ct. Sept. 7, 2012). This case involved the importation to the U.S. of a copyrighted book sold overseas. BSA argued that for digital works, in particular, the ability to adapt the content to the local market is essential, and would be impossible if creators cannot prevent importation of works tailored for other national markets.

PRIVILEDGED AND CONFIDENTIAL

Recent BSA Submissions on International Privacy and Related Issues

- **Australia (March, 2016) - Privacy Law Amendment Bill:** BSA submitted comments on the Draft Bill which focuses on data breach notifications. BSA suggested amendments to the Bill to align Australia's regulatory framework to global best practices regarding breach notification procedures.

- **Brazil (July, 2015) – Personal Data Protection Bill (Draft Bill – Ministry of Justice):** BSA submitted comments highlighting the importance of a balanced privacy regulatory framework. The submission stressed the importance of cross-border data flows and of mechanisms such as SCCs should a system based on the EU adequacy model be adopted in Brazil.

- **Brazil (August, 2015) – Personal Data Protection Bill (Senate Bill):** BSA submitted comments to Brazil's Senate reinforcing the comments submitted in July 2015 to the Brazilian Ministry of Justice – *see previous item*.

- **Brazil (February, 2016) – Decree Implementing Internet Framework Bill:** BSA submitted comments to Brazil's Ministry of Justice reinforcing the importance of data privacy and data security.

- **China (August, 2015)- Draft Cybersecurity Law:** BSA submitted comments urging the Government of China to adopt an effective cybersecurity strategy that enhances the cybersecurity that is consistent with international standards and approaches, does not impose unnecessary administrative compliance burdens, and does not impede data flows – *English text starts on page 2*.

- **China (November, 2015) - Supervision Rules on Insurance Institutions Adopting Digitalized Operations (CIRC Rules)**: BSA submitted comments to the Government of China urging the adoption of a policy that is (a) risk-based and prioritized; (b) technology-neutral; (c) practicable; (d) flexible; and (e) respectful of privacy and other important consumer rights.

- **India (April, 2015)** - **Mobile to Mobile Roadmap**: BSA submitted comments requesting unnecessary and counter-productive data localization requirements be removed from the draft as they did not increase data security or privacy. The final Mobile to Mobile Roadmap issued in May 2015 removed the references to data localization.

- **Indonesia (August, 2015) – Draft Regulation on the Protection of Personal Data in Electronic Systems:** BSA submitted comments highlighting, among other issues, the importance of data stewardship based on the accountability model established by the OECD, as well as the use of a number of mechanisms to legitimize data treatment, including legitimate interest.

- **Japan (January, 2015) Amendments to Japan Personal Information Protection Act (PIPA):** BSA submitted comments on Japan's PIPA amendments highlighting, among other issues, the importance of international data flows. Japan is currently working on implementing amendments to PIPA and BSA continues to engage with the Japanese government through a working group that focus on how to best implement provisions regarding international data transfers.

- **Korea (June 10, 2015) Cloud Computing Promotion Act:** BSA submitted comments and has held multiple meetings with government officials in Korea regarding privacy and other aspects of the Cloud Computing Promotion Act.

- **Thailand (March, 2015) Personal Data Protection Act:** BSA has submitted comments on the draft legislation highlighting the importance of protecting personal information, through an accountability model, and of preventing misuse of such information for fostering the trust and confidence necessary for growth of the digital economy. Original comments were followed by additional written contributions shared with the Government of Thailand as well by multiple meetings.

- **Vietnam (June, 2015) - Cross-Border Supply of Public Information:** BSA submitted comments raising concerns about regulation that would require information to be stored in Vietnam to allow for inspection, storage, and provision of information at the request of competent authorities.

- **Vietnam (October, 2014) – Information Technology Services Decree:** BSA submitted comments on a draft decree that regulates IT services in Vietnam highlighting concerns about international data transfer restrictions, unnecessary requirements to localize hardware (e.g., servers) in Vietnam, and unwieldy certification requirements for IT service professionals, among other issues.

- **Vietnam (May, 2016) – Information Security Law:** BSA and other associations submitted joint comments suggesting the law be improved to remove broad requests to provide access to user's encrypted or other password protect information in order to ensure privacy rights among other things.

BSA challenges to US Government Surveillance

BSA support for the USA FREEDOM Act. The Act made several changes to the US surveillance regime, including ending bulk collection and increasing transparency around government requests for data. See:

- BSA Urges Action on USA FREEDOM Act to End Bulk Collection and Increase Transparency (May 23, 2015, press statement)
- Joint Industry letter in support of USA FREEDOM Act (May 11, 2015)
- Pass Surveillance Reform Now (Nov. 14, 2014, TechPost and Sept. 8, 2014, joint industry letter)

BSA supportive of the Email Privacy Act (reforming ECPA). BSA supported a bipartisan, bicameral legislation requiring US Law Enforcement authorities to obtain a warrant for all electronic content. It also provides clarity to data services companies on their legal obligations to law enforcement, so that providers can be transparent about how they treat customers' information. See:

- Victoria Espinel's testimony to the Senate on ECPA (September 2015)
- Letter to Senate Judiciary leaders on ECPA reform (May 24, 2016)
- BSA | The Software Alliance Statement on the House Judiciary Committee Hearing on ECPA Reform (Nov. 30, 2015)
- BSA one-pager (October 2015)
- BSA Applauds Introduction of ECPA Reform Legislation (Feb. 4, 2015)

BSA support for the Judicial Redress Act. BSA fully supported passage of new rules providing appropriate access to court under the Privacy Act for citizens of designated countries. See:

- Joint industry letter to the House of Representatives re: passage of JRA (April 2015)
- Joint industry letter to the Senate re: passage of JRA (June 2015)
- BSA one-pager on the Judicial Redress Act

BSA support for the Law Enforcement Access to Data Stored Abroad Act (LEADS Act). BSA pushed for passage of this bipartisan, bicameral legislation to ensure an ECPA warrant can be used for data stored abroad providing that the warrant seeks the content of a U.S. subscriber. For non-U.S. subscribers, LEADS would ensure that law enforcement can still obtain the data through the Mutual Legal Assistance Treaty ("MLAT") process. See:

- BSA one-pager (October 2015)
- BSA Welcomes House Introduction of LEADS Act (Feb. 27, 2015, press release)
- BSA Urges Congressional Action as Hatch Re-Introduces LEADS Act (Feb. 12, 2015, press release)

BSA call for reform of MLATs. BSA urged reform of the Mutual Legal Assistance Treaties ("MLATs") must to remain effective for legitimate law enforcement needs. We are also supporting increased resources, as requested by the Department of Justice, and structural

changes to the MLAT process so that assistance is provided in a timelier manner in the digital world. See:

- Letter to Congress on MLAT funding (April 2015)
- BSA one-pager (October 2015)

BSA calls to resist attempts at undermining the security of online services. See:

- Letter to the Senate Judiciary Committee on encryption and LE access to data (July 2015)
- BSA Board Chair Letter to President Obama on encryption (May 15, 2015)
- BSA Amicus Brief in Support of Apple in the San Bernardino iPhone case (March 3, 2016)

A copy of the documents referenced above are publically available.