The Federal Government's Attempt to Force Microsoft to Violate Irish Territoriality[i]

"It's the wrong time, and the wrong place Though your case is charming, it's the wrong case"[ii]

Eric K. Clemons
The Wharton School
University of Pennsylvania
clemons@upenn.edu

Abstract

Questions of data residence have taken on new significance in an era of cloud computing, when data can reside in any location, and indeed can reside in different locations at different times. Microsoft and the Department of Justice are litigating over whether or not Microsoft is obligated to turn over data that does not reside in the US in response to a warrant from a US court. The issues in the case have significance beyond the individual case, and require a comprehensive reexamination of data sovereignty and territoriality. Moreover, this is a weak case, and the Department of Justice should not pursue it further for a variety of reasons.

1. Introduction.

The Federal Government and Microsoft are litigating over the government's attempt to force Microsoft to disclose emails from an account whose owner has allegedly violated US law. Although much information in the warrant has been redacted in the copies available online, it is clear that the case involves narcotics smuggling[1]. On the surface, it seems like an ideal test case to establish the government's right to access data from the Cloud, wherever in the world the data are stored. The owner of the email account, if he is indeed a large-scale international drug dealer, is scarcely a figure that anyone would want to protect. The emails may help convict the drug dealer if he is guilty, and he is certainly not a sympathetic figure. But the case between Microsoft and the US Department of Justice is not about protecting the drug smuggler. It is about data protection and data privacy laws, and indeed about due process and international law. It is about furthering the development of a rational policy towards data sovereignty and data citizenship in the cloud. Protecting international agreements is far more important than providing access to these emails without due process, especially since there are easy ways to obtain the data legally. Furthering the development of policy for data sovereignty is more important than undermining it.[2] This is quite simply the wrong case at the wrong time.

The wrong case: The case is quite complex, which is why it has been in the courts since 2013 [7]. The alleged drug dealer is an Irish citizen. Microsoft has stored the emails on a server located in Ireland for legitimate reasons relating to online performance.[3] Microsoft is arguing that a US warrant does not, cannot, and indeed must not compel it to reveal data that are not located in the US and that do not belong to Microsoft but rather to a client [12]. Microsoft is likewise arguing that the US needs to obtain an Irish warrant [12] to obtain data that reside in Ireland. The US is arguing that they do not need to do so, and that this is burdensome and time consuming [11]. However, the Irish government has repeatedly offered to issue a warrant allowing the US to search Microsoft's data in Ireland and has filed its own *amicus curiae* brief in support of Microsoft's position [8].[4] The US has chosen to delay the

[1] See Attachment C, page 41, of Government's brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records within its Custody and Control, Case 1:13-mj-02814-UA Document 60, https://digitalconstitution.com/wp-content/uploads/2014/09/the-government-brief.pdf.

[2] The significance of resolving issues in data sovereignty becomes clear when examining recent decisions and their implications for US high tech firms. The recent EU decision striking down the safe harbor agreement between the EU and the US makes it illegal to transfer data from the EU to the US, threatening the business model of firms like Google and Facebook, among others [19], in part because there are no assurances that the US government cannot access the data. The concern among US tech firms is obvious [4].

[3] Latency is reduced and overall response time is improved if an account is hosted as near to the account owner's geographic location as practical.

[4] The full text of more than a dozen *amicus curiae* briefs can be found online at the following links, all available at https://digitalconstitution.com/about-the-case/,

URI: http://hdl.handle.net/10125/41768
ISBN: 978-0-9981331-0-2

prosecution of the case by two and a half years by trying to force Microsoft to violate Irish sovereignty. This should thoroughly discredit the government's argument concerning the need for speed. There is a right way for the US to get the data it needs, and that is to rely upon Mutual Legal Assistance Treaties (MLATs), whereby one government can request a warrant from a second country for evidence that is located in the second country. See, for example, the text of the Second Circuit Court's decision [13], noting both the role of MLATs and the presence of such an agreement between the US and Ireland.[5] [6]

Indeed, the Irish

At the wrong time: This is a complicated time for data privacy. Wikileaks [18] and Edward Snowden's disclosures of activities at the CIA [10] have made it clear the extent to which US information companies like Facebook, Google, Microsoft, and Apple have cooperated in the past with US Federal investigations of US and foreign citizens, and there is a general sense of concern among American citizens about these systematic privacy violations [16], and disapproval of government surveillance even as part of counter terrorism activities [5, 17]. The resulting backlash has already made it difficult for the US to obtain the cooperation it needs; consider, for example, Apple's refusal to cooperate with the FBI by unlocking the iPhone belonging to the San Bernardino shooter [9]. If there is a sense that US agencies do not respect international agreements and international privacy laws it will be increasingly difficult to get cooperation from foreign firms and foreign governments.

As reported in the Wall Street Journal, The US Government sees this as a simple case [15]:

The Justice Department, which is seeking the emails as part of a drug-trafficking investigation, sees no international conflict. Microsoft has control over the data from the U.S., where the company is based, and the company is subject to the jurisdiction of the U.S. courts, the agency has argued in court and in legal briefs. At a time when governments around the world are cooperating and sharing data, this may initially appear attractive.

The government sees this as a simple case because it sees it as a straightforward application of the 1986 Stored Communications Act, itself part of the 1986 Electronic Communications Privacy Act (ECPA) [3]. Legal scholars agree on the centrality of the ECPA, but do not uniformly agree on the government's interpretation of the Act; see, for example [7].

It is not a simple case. Courts have been struggling for years on how to apply old laws to the issues created by modern technology (see for example [20]). This case is even more complex because it involves international data sovereignty issues. We will argue for a variety of reasons that this is the wrong case, at the wrong time for the US Department of Justice to use to establish its rights to data in the cloud, regardless of where the data are stored. Rather than strengthen governments' ability to access data in future cases, it may actually impede it.

Computer and Data Science Experts' Amicus Brief (Filed December 15, 2014)
Amazon and Accenture's Amicus Brief (Filed December 15, 2014)
Apple's Amicus Brief (Filed December 15, 2014)
AT&T, Rackspace, Computer & Communications Industry Association, i2Coalition, and Application Developer's Alliance's Amicus Brief (Filed December 15, 2014)
Brennan Center for Justice, ACLU, The Constitution Project and EFF's Amicus Brief (Filed December 15, 2014)
BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the U.S., The National Association of Manufacturers, and ACT | The App Association's Amicus Brief (Filed December 15, 2014)
Anthony J. Colangelo, International Law Scholar's Amicus Brief (Filed December 15, 2014)
ABC, CNN, Forbes, Fox News, National Public Radio, The Guardian, The Washington Post and 23 other media groups' Amicus Brief (Filed December 15, 2014)
Verizon, Cisco, HP, eBay, Salesforce.com and Infor's Amicus Brief (Filed December 15, 2014)
Digital Rights Ireland, Liberty and Open Rights Group's Amicus Brief (Filed December 15, 2014)
Jan Philipp Albrecht, Member of European Parliament's Amicus Brief (Filed December 19, 2014)
Government of Ireland's Amicus Brief (Filed December 23, 2014)

[5] That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. See U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), available at fam.state.gov/FAM/07FAM/07FAM0960.html.

[6] The United States has entered into an MLAT with all member states of the European Union, including Ireland. See Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.

We will not argue as lawyers, though we will rely upon briefs filed in this case and legal precedents. We will rather argue as technologists and strategy professionals, that is, as informed laymen.

The structure of this short paper is as follows. Section 2 will outline the case itself. Section 3 reviews the status of the case and the decisions that have been reached to date. Section 4 reviews why we believe the case should be decided in favor of Microsoft, and section 5 explains why we believe that the US Department of Justice should drop this case. Section 6 provides our policy recommendations regarding international requests for data in similar criminal cases, and section 7 provides our conclusions, our summary, and a terse review of our recommendations for future action.

When we first wrote this paper for the conference we were arguing that the Second Circuit Court of Appeals should decide in favor of Microsoft and against the Department of Justice. Moreover, we were arguing that the Department of Justice should withdraw the case, rather than risk having the Circuit Court decide against them. The Circuit Court did indeed decide in favor of Microsoft [24], agreeing on limits to the applicability of the ECPA to modern searches of the cloud [6]. We are now arguing that the Department of Justice should accept this decision and not seek *cert*, that is should not petition for a writ of *certiorari* and should not seek to have the case reviewed by the last remaining court of appeals, the Supreme Court of the United States. Moreover, we are now arguing that if the Department of Justice does seek *cert*, the Supreme Court should reject the petition and allow the Circuit Court's ruling to stand. The arguments involved in this case are vitally important; indeed, they are too important to be resolved using such a weak case as this one to establish legal precedent.

2. The arguments in the case

The Department of Justice is seeking emails from a Hotmail account, and has served Microsoft with a search warrant demanding Microsoft produce the relevant emails to the Department of Justice. Microsoft has argued that since the data are not the property of Microsoft but of an Irish citizen, and since the data reside in Ireland, the warrant is not valid and has sought to have the warrant vacated [15]. Microsoft has sought to have the warrant vacated, that is ruled invalid. Its attempts to do so have been unsuccessful, and currently Microsoft is being held in contempt of court for its refusal to comply.

Microsoft's legal arguments have three basic components. First, Microsoft is arguing that there is no reason to believe that the Electronic Communications Privacy Act of 1986 was written by Congress to have extraterritorial reach. Legislation of Congress is meant to only apply within the territorial jurisdiction of the United States, to protect against international discord and preserve a stable background. If Congress wanted to have extraterritorial reach, it needed to clearly state that in the legislation, and it has not done so in this case.[7] [8] [9]

Moreover, Congress has historically wanted to maintain international norms: US laws should be interpreted to avoid unreasonable interference with the sovereign authority of other nations[10] in order to avoid "international discord" that "could result" from "unintended clashes between our laws and those of other nations".[11].

Further, there is a presumption against extraterritorial application for a warrant[12] [13] [14] [15]. This presumption historically applies to cases involving the ECPA.[16]

The Federal Government's argument has three principal components. First, Justice Francis accepted the argument that despite being called a warrant, the SCA warrant is actually part warrant and part subpoena [14]. An SCA warrant "is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause" but then "is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the email account in question".

Secondly, the test for the production of documents is control, not location[17], and the US

[7] Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).

[8] EEOC v. Arabian American Oil Co., 499 U.S. 244 (1991).

[9] We will cite legal authorities in line, in the format that would be used in court documents and legal journals.

[10] Hoffmann-La Roche, Ltd. v. Empagran S.A, 2004 WL 1300131 (2004).

[11] Kiobel v. Royal Dutch Petroleum Co., 133 S.Ct. 1659 (2013),

[12] United States v. Vilar, No. S3 05–CR–621(KMK), (2007)

[13] United States v. Usama Bin Laden, 92 F. Supp. 2d 189 (S.D.N.Y. 2000)

[14] United States v. Aquino, No. 1:07cr428, (2008)

[15] United States v. Verdugo-Urquidez 494 U.S. 259 (1990).

[16] Zheng v. Yahoo! Inc.(2009) WL 4430297.

[17] In Re Grand Jury Proceedings the Bank of Nova Scotia.united States of America, Plaintiff-appellee, v.

government has gotten documents despite criminal penalties under Swiss Law[18],and enforced a grand jury subpoena for records stored in a foreign country.[19]

Finally, the MLAT process may be slow and laborious, and certain countries don't have MLATs with the US. The US should not therefore be required to rely upon MLATs when it can obtain a search warrant that allows it to access data held by a US company, whether or not the evidence in question is in the US, provided the US company can directly access that evidence from the US.

Microsoft's response has two components. First, Microsoft asserts that it does not "own" the data, but instead serves as a custodian for the data. It operates the equivalent of a password protected digital lockbox, and therefore fails the "possession, custody, or control regardless of the location" test.[20]

Finally, the warrant served by the court on Microsoft from the Magistrate Judge is a warrant in every sense of the word. In that respect, the warrant violates the Fourth Amendment because it does not identify the place to be searched and thus does not constitute a "reasonable" search. Microsoft asserts that electronic text communication is analogous to letters and telephone conversations. Like other forms of communication, emails have a reasonable expectation of privacy, and with a regular warrant, the US Government could not search every building of Microsoft in order to search for evidence.[21]

3. Status of the case between Microsoft and the Department of Justice to date

The Department of Justice has served Microsoft with a search warrant requiring that it turn over emails from a specific account, relevant to narcotics and international shipping. Microsoft has sought to have the warrant vacated, that is, dismissed as invalid. Microsoft lost its initial suit to have the warrant vacated in 2014, lost its initial appeal in 2015, and appealed the case to the Second Circuit Court of Appeals in 2015. The Second Circuit issued its decision in July 2016, finding in favor of Microsoft. Microsoft's interpretation of the victory and of its significance are summarized in the blog written by their President and Chief Legal Officer Brad Smith, immediately after the decision was announced [21].

4. Factors that might argue for the Department of Justice violating territoriality

There are extraordinary conditions under which the Department of Justice might indeed need to violate territoriality and attempt to force a company to provide data that resides in a foreign nation. Arguing as a technologist and a "reasonable man[22] each of us believes that the following can constitute valid reasons for violating jurisdictions and territorial restrictions.

- ***Hot pursuit*** — When authorities are in hot pursuit of suspects, and there is a danger that the suspects will escape or destroy evidence if not apprehend. Police chasing robbery suspects will now coordinate across jurisdictions but will not routinely allow suspects to escape if they succeed in crossing a municipal, county, or state border. This argument is based largely on the need for speed.
- ***Clear and present danger*** — When authorities believe that the evidence is needed immediately to prevent a major catastrophe, involving significant property damage or loss of life. If authorities believe that coordinating with appropriate counter-parties in separate jurisdictions may result in a dangerous delay, allowing suspects to commit further criminal acts, taking actions that violate extraterritoriality may be justified.
- ***Unresponsive or uncooperative foreign counter-parties*** — When authorities believe that evidence or suspects have been located in foreign jurisdictions where cooperation will be withheld, or where authorities believe that their foreign counterparties will actively participate sheltering fugitives or in the destruction of evidence, violating territorial boundaries may be justified.

---

the Bank of Nova Scotia, Defendant-appellant, 740 F.2d 817 (11th Cir. 1984).

[18] Marc Rich & Co., A.G., 707 F.2d 663 (2d Cir. 1983).

[19] United States v. Chase Manhattan Bank, NA, 584 F. Supp. 1080 (S.D.N.Y. 1984)

[20] Riley v. California, 134 S. Ct. 2473 - Supreme Court 2014

[21] United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010)

[22] See Wikipedia, https://en.wikipedia.org/wiki/Reasonable_person, "In law, a reasonable person (historically reasonable man) or the man on the Clapham omnibus is a hypothetical person of legal fiction whose is ultimately an anthropomorphic representation of the body care standards crafted by the courts and communicated through case law and jury instructions." That is, we are attempting to examine the case as reasonable individuals, not as legal experts.

Indeed, all three have historically been used to ignore territorial boundaries in cases in the past.

- ***Hot pursuit*** — The doctrine of hot pursuit allows competent authorities to pursue suspects if there is a clear reason to believe that they have committed an offense and if there is a clear reason to believe that they will escape if not pursued. The applicability of the hot pursuit doctrine internationally is extremely limited, and it applies in only two areas. Its principal use is the pursuit of a vessel that is believed to have committed an offense within the territorial waters of a nation, when that vessel has escaped into international waters while being pursued by competent authorities of the nation whose territorial boundaries have been violated. The second area of applicability is within the Schengen Area of Europe, including 22 of the 26 member states of the European Union.
- ***Clear and present danger*** — The US chose to send a special operations Seal Team after Bin Laden without the delay that would have resulted from attempting to cooperate with Pakistani authorities. Bin Laden was considered too dangerous to the US for him to be allowed to remain at large and potentially active.
- ***Unresponsive or uncooperative counter-parties*** — The Israeli government's abducting Eichmann, who was sheltering in Argentina can be viewed as ignoring the territorial rights of a sovereign nation [1]. US actions against Marc Rich when he was exploiting Swiss banking secrecy laws can be viewed as a similar but less dramatic example of the same principle. There was also a danger that attempting to coordinate with Pakistani authorities when the US acted against Bin Laden in Pakistan would have been impossible because there was a clear danger that Bin Laden would have been alerted and given time to flee [2]. Interestingly, the analysis of these cases after actions were completed suggests that the use of the principle of extraterritoriality can be contentious, even in cases that may initially appear to be unambiguously legal.

We believe that it is clear that none of the three is relevant in this case.

- ***Hot pursuit*** — The case is two and a half years old. The emails have been archived. There is no time pressure that would justify extraterritoriality. And it is hard to see how international agreements on extraterritoriality would support the position of the US Department of Justice.
- ***Clear and present danger*** — After two and a half years presumably the suspect is in custody somewhere. Presumably he is not going anywhere or harming anyone, and presumably he is no longer engaged in international drug smuggling. And the US government must agree that there is no immediate danger or they would not have refused offers of cooperation from the Irish government, which would have allowed resolution of the cases months earlier.
- ***Unresponsive or uncooperative counter-parties*** — Far from being unresponsive or uncooperative, the Irish authorities have volunteered to provide a warrant that would have allowed the Department of Justice to access the relevant emails. These offers of cooperation to date have all been refused by the US Department of Justice, but surely one cannot argue that the Irish authorities have been unresponsive or uncooperative, or that they have behaved in any way that would justify violation of their territoriality.

5. Why this case should have been decided in favor of Microsoft

We believe that the Second Circuit Court of Appeals decided correctly when it ruled in favor of Microsoft. The case brought by the Department of Justice was not a strong one. Moreover, the interests of numerous parties with an interest in the case were best served by this decision. As we explore below, these parties range from US citizens, US technology companies, and customers of those companies, to the US government itself.

The case brought by the Department of Justice was not a strong one. The cases that the US government uses, and upon which its arguments rely, are old and did not involve electronic evidence. Extending the FBI's reach to electronic data wherever in the world it resides as long as it is administered by an American data services company is too great a reach. It is unjustified. And it is unnecessary. It is easy enough for US authorities to request that the American data services company archive data so that there is little or no danger of the data being destroyed. After that, there is adequate time for US authorities to rely upon MLATs, and to request that a search warrant be issued in the appropriate jurisdiction.

The interests of US citizens around the world would be harmed if this case were decided in favor of the US government. At present, corporations insist, rightly, that foreign governments must obtain valid search warrants issued in the jurisdiction in which data resides before they can be forced to share data on their customers with foreign governments. If this case were decided in favor of the US and against Microsoft, this would establish a precedent that

would enable any foreign government to obtain any data from any company that operated in that country's territory, regardless of where that data resided. US citizens would no longer have any legal protection against illegal search and seizure of their data, using precedents established by the US government. This could be extremely dangerous to citizens traveling abroad, to nations with less established legal protections than our own.

The interests of Microsoft customers around the world would likewise be harmed if this case were decided in favor of the US government. At present, Microsoft insists, rightly, that any government must obtain valid search warrants issued in the jurisdiction in which data resides before they can be forced to share data on their customers with foreign governments. If this case were decided in favor of the US and against Microsoft, this would establish a precedent that would enable place any Microsoft customer at risk of unreasonable search and seizure of their data by the US, without the legal protections offered by their home jurisdiction.

The interests of US corporations would also be harmed if this case were decided in favor of the US government. At present, US corporations insist, rightly, that foreign governments must obtain valid search warrants issued in the jurisdiction in which data resides before they can be forced to share data on their customers with foreign governments. If this case were decided in favor of the US and against Microsoft, this would establish a precedent that would enable the US to obtain data belonging to any customer of a US data services company, regardless of the customer's home jurisdiction, and regardless of where in the world the data resided. Customers would rationally seek and find alternative service providers, damaging or even destroying one of the US's most innovative international market for services. Not surprisingly, a large number of technology and media companies have submitted *amicus curiae* briefs in support of Microsoft's position [23].

Even the interests of the US Government would be harmed by a decision against Microsoft. Voluntary data sharing and cooperation among government agencies is increasingly important, and the US is increasingly arguing for the rule of law and for coordination of activities among intelligence services and cooperation in the global fight against terrorism. If the US wants other countries to respect laws and common practices around the world, it must do so itself. If the US wants other countries to share data and intelligence information with it, it must respect data privacy laws of the nations with which it is cooperating.

6. The US government should withdraw this case rather than risk losing it

We argued in advance of the Second Circuit Court's ruling that the case was weak, and that the US was likely to lose it. This was indeed shown to be correct. This remains true now. The case remains weak, and the US remains likely to lose should it seek to pursue the case further by appealing to the US Supreme Court.

Moreover, it is easy to imagine future situations in which the Department of Justice truly might need to force a corporation to perform a search abroad, for example in a case involving data resident in a country with which the US did not have an MLAT in place. Losing this case would set a damaging precedent that would make it more difficult for the US to argue successfully for extraterritoriality in the future. Not only is the government risking setting a damaging precedent, it is doing so with a weak case, and with case that it does not need to pursue; the Irish Government has repeatedly offered to cooperate.

7. What we recommend as policy

There is a small set of actions that could easily be taken by all technology services companies and email providers. These actions would ensure that the outcome of a case would not be determined by delay caused by properly pursuing appropriate venues, simply by preserving potentially relevant evidence while warrants were pursued. Thus, no country would ever need to argue that in the absence of rapid search, including search of questionable legality, necessary email evidence would be lost forever. While this would not alter the need for speed in counter-terrorism operations, it would essentially nullify the arguments used by the Department of Justice in this case. The Congress should pass legislation that would make these actions mandatory for all service providers operating in the United States.

First, all email service providers around the world should be required to maintain backups of all email correspondence as soon as they receive a suitable official notification of an investigation anywhere in the world for which this email is material evidence and an official request for assistance in obtaining a valid search warrant. We are aware that backups are usually available, but this ensures that any email that was available at the time of notification would always remain available at the time the service provider received a valid warrant. This does *not* require the service providers to respond to a warrant from a foreign jurisdiction. It *does* require the service provider to maintain and protect archival data until such time as the case is resolved or the relevant jurisdiction where the data resides has issued a warrant. If such a valid warrant is issued,

then and only then is the company is required to provide the data covered by the warrant. An official request would be from a state, provincial, or national government, or from an organization such as Interpol. Rows (1) and (2) of table 1 below summarize the activities that would be required of all service providers providing email services within the United States, whether they are US-based corporations or not.

We note that it could easily be impossible to enforce this without international harmonization. A service provider operating out of the mythical Duchy of Grand Fenwick or the Republic of Illyria might seek to gain competitive advantage by persuading their governments not to require archiving of email accounts. We therefore believe that international harmonization would be critical here. Companies that were not required to archive email when notified of its relevance to litigation might enjoy a competitive advantage. Companies that could be forced to provide emails without a valid warrant would likewise be at a competitive disadvantage. While the US Congress cannot impose requirements or operating policies on companies when they provide email services outside the US, we believe that rows (3) through (5) represent policies that the US should seek to have implemented by trading partners around the world.

We believe that all governments should rely upon MLATs to obtain valid search warrants when they seeks data maintained by email service providers, regardless of the home country of the service provider and regardless of the location of the data requested.

However, no service provider offering services within the United States should be able to evade their legal obligations to respond to valid warrants relevant to US investigations by locating their servers off-shore. This would preclude both the obvious possibility of locating their servers in countries with which the US does not have MLATs, or the possibly more contrived alternative of constructing artificial islands not subject to any nation's laws and not responsive to any nation's MLAT. Indeed, we recommend that either of these actions should be interpreted under US law as a deliberate attempt to evade control over data when required for criminal cases. These off-shore legal evasions should be viewed as only slightly different from illegal off-shore money laundering and other illegal financial transactions. In these instances US courts should be permitted to search data *as if* it were maintained in the US, because its foreign location would have no other explanation except to avoid reasonable search. Obviously, the US can only impose these restrictions on companies operating in the United States and offering services within the US. However, for obvious reasons, the US should encourage international harmonization, so that all our trading partners impose comparable restrictions on service providers offering services within their borders. This is described in rows (6) and (7) in the table below.

Regrettably, obvious loopholes exist. Individuals with private email servers can agree amongst themselves to perform no archiving and retain no copies of messages. New email service providers can locate in unregulated markets and offer email services that retain no archives and thus are not subject to search, even if offering such service were to violate local laws and regulations. End-to-end encryption is emerging as a problem for law enforcement around the world. While most encryption is in principle subject to decryption with sufficient time and sufficient resources, most criminal investigations do not justify unlimited expenditure on decryption, and in the case of terrorist threats there is generally insufficient time for brute-force decryption.

Country Where Court Located	Country Where Data Stored	Relevant MLAT in Force	Warrant that is Required	Note
US	**US**	——	US (Country of Court and Data)	**(1)**
US	**Non-US**	**YES**	Country of Data via MLAT	**(2)**
US	**Non-US**	**NO**	US in the Absence of MLAT	**(3)**
Non-US	**Same Non-US**	——	Country of Court and Data	**(4)**
Non-US	**Different Non-US**	**YES**	Country of Data via MLAT	**(5)**
Non-US	**US**	**YES**	US	**(6)**
Non-US	**US**	**NO**	Country of Court in the Absence of MLAT	**(7)**

Table 1.—Recommended policies for the applicability of search warrants internationally.

8. Conclusions: Summary and Recommendations for Future Action

Our analysis supports the following assessment of the case:

- The US Government can already obtain the data it seeks; this litigation is unnecessary.
- The US Government's arguments are weak or even inapplicable in an online environment, and if the case is ultimately decided in the courts the US should lose.
- The US Government should withdraw this case rather than risk losing it and risk setting an unfortunate precedent.

The case is potentially harmful to the interests of US citizens, Microsoft and other US service providers, and even the US Government itself. If the US Government were to win this case, despite the weakness of its arguments, the interests of several groups would be adversely affected.

- US citizens using any data service provider anywhere in the world would be at risk of unreasonable search and seizure of their electronic communications as foreign governments use this case as a precedent to force cooperation with their own search warrants. US Citizens' protections would be limited to those of any country that wanted any data, rather than those available under US law.
- US Corporations including Microsoft would be at risk of losing credibility with their customers, since it would appear that the US Government could search their electronic records in foreign jurisdictions without complying with the laws of those jurisdictions.
- Even the US Government, at a time when voluntary data sharing and cooperation is increasingly important, and the US is increasingly arguing for the rule of law, may find its own long-term interests harmed if it were to appeal to the US Supreme Court and then to win this case on appeal.

For these reasons as well, the US Government should withdraw this case.

The US Congress should draft appropriate legislation that would require US corporations to maintain backup storage of critical electronic communications involved in litigation, but should not require them to turn over their records until they have received a valid search warrant for the jurisdiction in which the data resides. Moreover, existing mutual legal assistance treaties should be extended so that service providers in foreign jurisdictions obey harmonized codes.

9. References

[1] Baade, H.W., "The Eichmann Trial: Some Legal Aspects", *Duke Law Journal*, Vol. 1961 pp. 400-419, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1766&context=dlj.

[2] Calabresi, M. "CIA Chief: Pakistan Would Have Jeopardized bin Laden Operation", *Time,* May 03, 2011, http://swampland.time.com/2011/05/03/cia-chief-breaks-silence-u-s-ruled-out-involving-pakistan-in-bin-laden-raid-early-on/.

[3] Electronic Communications Privacy Act of 1986 (P.L. 99-508), https://www.justice.gov/jmd/electronic-communications-privacy-act-1986-pl-99-508.

[4] Ettling, M. "The Cloud's Biggest Threat Are Data Sovereignty Laws", *TechCrunch, December 26, 2015*, https://techcrunch.com/2015/12/26/the-clouds-biggest-threat-are-data-sovereignty-laws/.

[5] Gao, G. "What Americans think about NSA surveillance, national security and privacy", *Pew Research Center Fact Tank,* May 29, 2015, http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.

[6] Henning, P.J. "Microsoft Case Shows the Limits of a Data Privacy Law", *The New York Times,* July 18, 2016, http://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html.

[7] "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp." *Harvard Law Review,* January 12, 2015, http://harvardlawreview.org/2015/01/in-re-warrant-to-search-a-certain-email-account-controlled-maintained-by-microsoft-corp/.

[8] Lillington, K. "Government files supporting brief for Microsoft in US case: State granted extra time for rare filing by sovereign of Amicus brief ", *Irish Times*, December 23, 2014, http://www.irishtimes.com/business/technology/government-files-supporting-brief-for-microsoft-in-us-case-1.2047768.

[9] Lichtblau, E. and Benner, K. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", *New York Times,* February 17, 2016, http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[10] Mazzetti, M. and Schmidt, M.S., "Ex-Worker at C.I.A. Says He Leaked Data on Surveillance", *The New York Times,* June 9, 2013 , http://www.nytimes.com/2013/06/10/us/former-

cia-worker-says-he-leaked-surveillance-data.html.

[11] Microsoft v. United States, Brief for the United States of America Case 14-2985, Document 212, 03/09/2015, 1456279 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, available online at https://digitalconstitution.com/about-the-case/.

[12] Microsoft v. United States, Reply Brief for the Appellant, Case 14-2985, Document 222, 04/08/2015, 1480496 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, available online at https://digitalconstitution.com/about-the-case/.

[13] Microsoft v. United States, Decision of the Second Circuit Court of Appeals Case 14-2985, Document 286-1, 07/14/2016, 1815361 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, available online at https://digitalconstitution.com/about-the-case/.

[14] Nakashima, E. "Microsoft fights U.S. search warrant for customer e-mails held in overseas server", *The Washington Post,* June 10, 2014, https://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html.

[15] Palazzolo, J. "Microsoft Email Case Tests Power of Search Warrants", *The Wall Street Journal,* September 7, 2015, http://www.wsj.com/articles/microsoft-email-case-tests-power-of-search-warrant-1441660355.

[16] Rainie, L. and Madden, M. "Americans' Privacy Strategies Post-Snowden: Americans' Views on Government Surveillance Programs", *Pew Research Center Internet Science & Tech*, March 16, 2013 http://www.pewinternet.org/2015/03/16/americans-views-on-government-surveillance-programs/.

[17] Rainie, L. and Maniam, S. "Americans feel the tensions between privacy and security concerns", *Pew Research Center Fact Tank,* February 19, 2016.

[18] Savage, C. "Soldier Admits Providing Files to WikiLeaks" *The New York Times,* February 28, 2013, http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html.

[19] Scott, M. "Data Transfer Pact Between U.S. and Europe Is Ruled Invalid", *The New York Times*, October 6, 2105, http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0.

[20] Sengupta, S. "Updating an E-Mail Law From the Last Century, *The New York Times"*, April 24, 2013, http://www.nytimes.com/2013/04/25/technology/updating-an-e-mail-law-from-the-last-century.html.

[21] Smith, B. "Our search warrant case: An important decision for people everywhere", Posted July 14, 2016, http://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.00001wyvibh8cmei8pxv4492amk81.

[22] "Tech Companies Back Microsoft in Ireland Email Warrant Case", NBCNews, December, 15 2014, http://www.nbcnews.com/tech/tech-news/tech-companies-back-microsoft-ireland-email-warrant-case-n268901.

[23] Wingfield, N. "Tech and Media Companies Back Microsoft in Privacy Case", *The New York Times,* December 15, 2014, http://bits.blogs.nytimes.com/2014/12/15/tech-and-media-companies-back-microsoft-in-privacy-case/?_r=0.

[24] Wingfield, N. and Kang, C. "Microsoft Wins Appeal on Overseas Data Searches", *The New York Times,* Jul 14, 2016, http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html

[i] We gratefully acknowledge having received support from Microsoft in the past. However, Microsoft did not provide funding or support for this paper. The opinions expressed in this paper are our own and we are responsible

[ii] With apologies to Cole Porter, this is not the original wording of his song. It is not how the verse was originally sung by Sinatra, Fitzgerald, or any of the other greats who recorded it.