Potential Changes in the Operation of U.S. Search Warrants to Obtain Extraterritorial Data

A Discussion of the Pending Changes to Rule 41 and of Microsoft v. Ireland

Discussion Paper

Octopus Conference 2015 Cooperation Against Cybercrime

Joseph J. Schwerha IV, M.S., J.D.

Associate Professor of Business Law & Technology

California University of Pennsylvania

There are two wholly separate avenues whereby the use of search warrants in the United States may significantly change transnational evidence gathering for criminal investigative purposes within the United States. Even though the Proposed Amendments to Federal Rule of Criminal Procedure 41 and the case of Microsoft v. Ireland are still mid-stream, their implications deserve some discussion. While completely separate, each poses significant possible changes on how Federal Law Enforcement authorities within the United States may access electronically stored information outside the physical boundaries of the United States, especially that which may be considered in the "cloud".

Potential Changes to Federal Rule of Criminal Procedure 41

By letter dated September 18, 2013, Acting Assistant Attorney General Mythili Raman submitted a letter to the Chair of the Advisory Committee on the Criminal Rules recommending changes in Federal Rule of Criminal Procedure 41 "relating to the territorial limits for searches of electronic storage media."[1]

The Department of Justice asserts it needs these modifications for three reasons:

> "1) to enable investigators to obtain warrants where the location of the computer to be searched is unknown, including where a suspect is using anonymization tools like Tor or other

[1] *See* letter, Mythili Raman to The Honorable Reena Raggi, dated September 18, 2013 accessed on June 3, 2015 here: http://justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf.

proxy services to mask his or her internet protocol ("IP") address and other identifying information;

2) to enable investigators to obtain warrants to search Internet-connected computers in many districts simultaneously when those computers are being used as part of "complex criminal schemes." As an example, DOJ describes crimes involving "the surreptitious infection of multiple computers with malicious software that makes them part of a 'botnet,'" where investigating and addressing the threat posed by the botnet may involve law enforcement action in many judicial districts simultaneously; and

3) to enable investigators who obtain a warrant to search a physical computer in a particular location to also use that same warrant to search information that is accessible from that computer but stored remotely in another district, such as information stored on cloud-based services (e.g., Dropbox or Amazon Cloud Drive) or web-based email (e.g., Gmail or Yahoo! Mail)."[2]

If the proposed amendments are adopted as actual changes to Rule 41, several have argued that there could be vast implications to transnational evidence gathering.

How are the Rules Changed?

The Federal Rules of Criminal Procedure are changed in a very different way than changing an actual statute. A statutory amendment in the United States starts as a bill.[3] A bill is just a proposed statutory amendment. It must then pass in both the House of Representatives and the Senate.[4] Afterwards, the President of the United States signs it and it becomes a statute.[5]

The Rules change in a very different fashion. The Federal Rules of Practice and Procedure control the process of "trials, appeals and cases under Title 11 of the United States Code."[6] This procedure was originally mandated through congressional action by and through

[2] *See* ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media, American Civil Liberties Union, p. 1 (April 4, 2014), http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0016, citing Advisory Committee Materials 172–73, 261 (last visited on June 3, 2015).
[3] For the purposes of this discussion, we will assume that we are talking about a Federal statutory amendment. Each state has a its own, very similar procedure.
[4] Once again, we are assuming this is a piece of Federal legislation.
[5] We are using the term statute to be synonymous with the term law. There are several variations of that procedure.
[6] United States Courts Website, How the Rule Making Process Works, http://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works (last visited on June 3, 2015).

the Rules Enabling Act of 1934.[7] That act authorized the United States Supreme Court to establish the Rules and any changes thereto, which have the effect of a law.[8] They delegated this process to the committees of the Judicial Conference, which is the primary policy body of the U.S. Courts.[9] Changes to the Rules of Criminal Procedure are further delegated to the Judicial Conference's Committee on Rules of Practice and Procedure ("Standing Committee") and its advisory committee on the Criminal Rules.[10] Any proposed change is reviewed by the appropriate advisory committee, which then recommends it to the Standing Committee.[11] It reviews it, and then recommends any changes to the Judicial Conference, which then recommends it, if appropriate, to the United States Supreme Court.[12] That court reviews the proposal, and if satisfied, promulgates the amended rules by order.[13] Any Rule adoption made by May 1 of that year may be put into effect no earlier than December of that same year.[14] During this time, Congress will review same, should they desire.

What is the Status of the Rule Change Proposal?

On August 15, 2014, the public comment period opened for the current proposed rule changes. That period ended on February 17, 2015. On March 16, 2015, the Judicial Conference Advisory Committee on Criminal Rules voted 11-1 to amend Rule 41 of the Federal Rules. The Standing Committee approved the proposed amendments and they are now in the hands of the Judicial Conference. If approved, they will go to the United States Supreme Court.

What is Proposed?

According to the proposed changes publicized for comment, the following changes are proposed. There are two main proposals.

[7] *See* 28 U.S.C. § 2071-2077.
[8] United States Courts Website, How the Rule Making Process Works, http://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works (last visited on June 3, 2015).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

Rule 41 (b)(6) Added

The first part is the proposed addition of a new section to Fed. R. Crim. P. 41. Under the new Fed. R. Crim. P. 41 (b) (6), "[a]t the request of a federal law enforcement officer or an attorney for the government", the following would be added:

> "(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."[15]

According to the Committee Note, "[t]he amendment provides two specific circumstances a magistrate judge in a district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information is or may be located outside the district."[16] The first option, which is located under subparagraph (b)(6)(A), applies "when the district in which the media or information is located is not known because of the use of technology such as anonymizing software."[17] The second option, which is located under (b)(6)(B), "allows a warrant to use remote access within or outside the district in an investigation of a violation of 18 U.S.C. § 1030(a)(5) if the media to be searched are protected computers that have been damaged without authorization, and they are located in many districts."[18] The Note specifically refers to "creation and control of 'botnets'" as a covered circumstance.[19] Likewise, the Note states that the Amendment does not address the Constitutional questions, such as specificity of the warrant.[20] The Note does not address whether the search could actually occur outside of the investigator's country.

Rule 41 (f)(1)(C) Modified

---

[15] Fed. R. Crim. P. 41(b)(6), (Preliminary Draft 2014).
[16] Fed. R. Crim. P. 41, advisory committee's note (Preliminary Draft 2014).
[17] *Id.*
[18] *Id.*
[19] *Id*.
[20] *Id*.

The second part of the proposed changes is a modification of the above-mentioned rule, which would add the following language:

> "For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person."[21]

As the Committee Note makes clear, this modification was made to make sure "reasonable efforts are made to provide notice" to the person whose information was taken or whose property was searched.[22]

Comments

Most of the comments appear to be negative. During the public comment period, there were numerous discussions of the Proposal's advantages and disadvantages. One of the Proposal's most outstanding critics has been Google.

Google

On February 15, 2015, Google submitted their comments to The Judicial Conference Advisory Committee on Criminal Rules. They were drafted by Richard Salgado, their Director of Law Enforcement and Information Security.[23]

Google argues that the Proposed Amendment substantively expands the Government's search capabilities, which is a decision that must be left to Congress.[24] In support thereof, Google first submits that the Government should not be able to seize evidence outside of the United States via remote access to computers located abroad.[25] Simply put, Google says that this proposal would now change the substantive law which previously limited execution of searches only within the district where the issuing judge was physically located, with certain

[21] Fed. R. Crim. P. 41 (f)(1)(C) (Preliminary Draft 2014).
[22] *Id*.
[23] Mr. Salgado used to actually work for the Department of Justice in the Computer Crimes and Intellectual Property Section.
[24] Richard Salgado, Google Inc. Comments on the Proposed Amendment to the Federal Rules of Criminal Procedure 41, Google Inc. (2015), http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0029 (last visited on June 3, 2015).
[25] *Id* at pp. 1-2.

very limited exceptions.[26] While the Department of Justice argues that nothing in the Proposal specifically authorizes extraterritorial searches outside of the United States,[27] the problem is that the Proposal doesn't make clear that the new powers would only be exercised within the United States because it doesn't have a limit on searches beyond our borders.

The second reason Google offers that the Proposal should be left to Congress is that the Proposal violates the Enabling Act. Under this theory, Google argues that the Proposal may not go forward because it is altering a substantive right, thereby taking it outside the purview of the Standing Committee. Google adds that when similar questions had come up in the past, it was Congress, not the Rules Committees who considered those amendments. Google offers the following as examples: the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. § 2518, The Stored Communications Act, 18 U.S.C. §§ 2701 et seq., as well as others.[28]

Google argues that the Proposal is too vague because it fails to specify how searches may be conducted and what may be searched.[29] Of particular concern is the possibility of the Government using Network Investigative Techniques ("NITs"). Use of a NIT presents many concerns that were held by more than just Google, including the "creation of vulnerabilities in the target device thereby increasing the target's risk of exposure to compromise by other parties, actual damage to the target device, the creation of a market for zero-day exploits, and unintended targets' exposure to malware."[30]

In addition to not limiting how a search can be conducted, the Proposal also fails to limit precisely what may be searched once it is accessed. In particular, the Amendment fails to define "concealed through technical means" and would, apparently, include many legitimate uses of encryption. Google argues that the proposed amendment would actually allow searches of wholly legitimate users' computers solely because they used encryption in their everyday business practices.[31] Likewise, Google urges that the term "media" is not defined and

---

[26] *See* Fed. R. Crim. P. 41(b)(2)-(5).
[27] *Id* at p. 2.
[28] *Id* at p. 5
[29] *Id* at p. 6.
[30] *Id* at p. 7.
[31] *See Id* at p. 7, note 22, specifically citing: "A number of news outlets have reported that Attorney General Eric Holder has authorized the National Security Agency to collect and indefinitely retain encrypted data, regardless of its U.S. or foreign origin, " for a period sufficient to allow thorough exploitation" of that data. Andy Greenberg, Leaked NSA Doc Says It Can Collect And Keep Your Enc1ypted Data As Long As It Takes To Crack It, Forbes (June 20, 2013, 6:21 PM), http://www. forbes.com/s i tes/andvgreenberg/20 13/06/20/1 eaked-nsa-doc-says-it -can-co II ect -and-keep-your-encrypted-d ata-as-long-as-it-takes-to-crack-it/; see also Declan McCullagh, NSA 'secret backdoor' paved way to U.S. phone, e-mail snooping, CNET (Aug. 9, 2013, 11:16 AM), http://www.cnet.com/news/nsa-secret-backdoor-paved-way-to-u-s-phone-e-mail-snooping/. The government therefore considers the mere use of encryption as a red flag that raises the suspicion of criminal misconduct. Law enforcement's suspicion of perfectly lawful activity indicates that the amendment as drafted may be fertile grounds for abuse."

thereby adoption of the proposed amendments could lead to searching whatever is accessible through the device being searched, be it in the cloud, in a cell phone, or wherever you can imagine.

The third major argument Google raises is that the Amendments raise serious constitutional concerns. They cite four reasons: 1. The proposed amendments will cause confusion with how the particularity requirement of the Fourth Amendment should be interpreted. ; 2. The use of NITs may constitute an unreasonable search and seizure due to "their destructive and unpredictable nature."; 3. The types of searches authorized may circumvent the "super warrant" requirements of Title III.; and 4. It would weaken the notice requirement of Rule 41.[32]

The last central argument Google makes is that the Proposal "would authorize searches of millions of computers."[33] This refers to the "an investigation of a violation of 18 U.S.C. § 1030(a)(5)." Google cites the Committee Note and the Federal Bureau of Investigation to conclude that searches allowed by such provision could amount to millions of computers under a single search warrant, if not even one third of all computers, if a virus were to be investigated.[34] Google argues that allowing searches of such magnitude and privacy implications would be best considered by Congress.[35]

There are many detractors from the Proposed Amendments, including the American Civil Liberties Union, National Association of Criminal Defense Lawyers and the Pennsylvania Bar Association. While they may cite slightly different arguments, the comments of Google nicely illustrate the major arguments against implementation of the Proposed Amendments.

Position of the Department of Justice

The United States Department of Justice, of course, disagrees with the detractors to the Proposed Amendments. It argues that the Rules Committee is, in fact, the appropriate body to consider these changes. Assuming rightly or wrongly that the "proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current" law, the DOJ frames the issue as one merely of venue. They claim the amendments merely dictate where a request for a warrant may be made, not

[32] *Id* at pp. 9-10.
[33] *Id* at p. 13.
[34] *Id* at pp. 13-14.
[35] *Id.*

whether remote searches and the like are actually legal.[36] Second, the DOJ asserts that the Committee is the right place to make this argument because it has addressed such amendments in the recent past. Third, Congress does not have to approve new investigative techniques before they are used.[37] Fourth, the Rules Committee has told the DOJ in the past that the DOJ should address their problems through the Rules Committee versus Congress.[38]

The DOJ argues that the Proposal is not vague. Without going through each term, the DOJ merely believes that there are established definitions for each of the terms or phrases that are complained of. More specifically, it argues that search warrant authorizations have never specified exactly how the search was to be conducted.[39]

The DOJ goes on to argue that the botnet amendment was very appropriate. It dismisses Google's arguments about scope and the idea of millions of computers could be investigated at once by saying the scope of crime is dictated by the criminal and that there is such thing as a crime that is too big to investigate.[40]

Status

As of right now, as I stated earlier, the Proposed Amendments are being considered by the Judicial Conference. If approved, then they would be transmitted to the United States Supreme Court for consideration and possible adoption.

Microsoft v. Ireland

Just after the United States Department of Justice requested changes to Federal Rule of Criminal Procedure 41, it served a warrant upon Microsoft Corporation. Microsoft refused to completely respond because doing so would require it to provide data from one of Microsoft's data centers in Ireland. That action has ultimately raised great discussion of the extraterritorial effect of warrants served by U.S. DOJ officials upon domestic corporations under the Stored Communications Act. *At its heart is the question of whether such a warrant can legally compel a U.S. company to reach out across national boundaries to retrieve data under its control even if such transfer arguably is illegal under the law of the country from where the data was retrieved.*

[36] *See* David Bitkower, Additional Response to Comments Concerning Proposed Amendment to Rule 41 (February 20, 2015)
[37] *Id* at p. 2.
[38] *Id* at p. 3.
[39] *Id* at pp. 3-4.
[40] *Id.*

The following is a brief discussion of the respective interested parties' positions. Presently, the case is before the Second Circuit Court of Appeals.

Microsoft's Argument to Magistrate

Microsoft was presented with a warrant that required production of electronically stored information from a specific account ("account").[41] According to Microsoft, the account is located in an Ireland datacenter. Therefore, releasing the information would allow the government to conduct and extraterritorial search and seizure. Without express congressional intent, statutes are presumed to have no extraterritorial effect.[42] Microsoft can access the data remotely here in the U.S., but asserts the search takes place where the data is located. Essentially, the government would be conducting an extraterritorial search through Microsoft, as they would be gathering the data. Based on the text of the statute and longstanding history, this type of search is not allowed. Ireland is an MLAT member and that process would have been more appropriate to obtain the necessary data.[43]

Government's Argument to Magistrate

The DOJ argued that Microsoft's reasoning is flawed, because the text of the SCA does not provide a safe harbor for information stored overseas. The SCA confers broad authority on courts to issue 2703(d) orders and SCA warrants where the court has jurisdiction over the offense being investigated.[44] Under the SCA, they urged, location of records is irrelevant. Any court that has jurisdiction over the offense being investigated is authorized to issue an SCA warrant. The appropriate test for the production of documents is control, not location.[45] Legislative history shows that this requirement has been strictly enforced even when it violates the laws of another country.[46] Basing production on location would directly contradict longstanding precedent and would prevent the government from obtaining otherwise responsive data.

---

[41] Microsoft's Memorandum in Support of its Motion to Vacate the Warrant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).
[42] *Id.*
[43] *Id.*
[44] Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).
[45] *Id.*
[46] *Id.*

They went on to say that under section 2703, the use of the term "warrant" is intended to adopt the probable cause standard, not to limit the geographic scope. The SCA was amended in 2001 to eliminate the reliance on the location of data as a necessary basis for obtaining an SCA warrant. SCA warrants are different in that they are not directed at physical property and do not require a law enforcement officer to be present.[47] Instead the warrant requires Microsoft to review their records and produce the relevant material.[48] Microsoft's employees do not have to go to Ireland to receive the requested data. The data can be accessed here in the United States without the involvement of foreign law enforcement.

Lastly, the DOJ contends that Microsoft's position would hinder the Government's ability to conduct criminal investigations.[49] The Government's ability to obtain data would be based on where the data is stored. With ever-changing technology, the data could be in the United States one day and in a foreign country the next. Also, Microsoft argues they store a person's data based on where they live, but they do not verify validity of that information. This would make it easier for people to avoid criminal sanction by simply stating they live in a foreign country.

Magistrate Opinion

The magistrate denied Microsoft's motion to vacate the search warrant,[50] concluding that SCA warrants are "hybrids" and only similar to a Rule 41 warrant in that it requires a showing of probable cause. The Judge reasoned that a SCA warrant is similar to a subpoena in execution. An SCA warrant is served on a provider and it is the provider's responsibility to produce the requested information. Further, the Judge held that there was no extraterritorial search because the search does not take place until law enforcement reviews the data in the U.S. The court further held the MLAT process is not proper[51] because the MLAT process can be slow and it is not available in all countries. Furthermore, member countries can deny a MLAT request. Based on the hybrid distinction, the Judge determined the relevant question is whether the data is in the provider's control. The data from the account was in Microsoft's control. Therefore, Microsoft was required to produce the requested information.[52]

---

[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014)
[51] *Id.*
[52] *Id.*

Microsoft's Argument to Federal District Court

Microsoft's asserted that if extraterritorial effect is not expressly stated in § 2703(a), it is presumed that the statute will only apply within U. S. territory,[53] adding that the Electronic Communications Privacy Act warrant provision does address conducting law enforcement search and seizures abroad. Therefore, the statute should only apply in U.S. territory.

Microsoft goes onto argue that although Microsoft is the one executing the warrant, it is still a law enforcement tool.[54] Therefore, a seizure is still taking place on foreign soil. Next, Microsoft urges that the district court erred in relying on the rule that states, "the test for production of documents is control, not location".[55] Instead that rule applies to subpoenas for company business records rather than warrants for customer property. In the Government's argument to the magistrate, they analogize a § 2703(a) warrant to a subpoena and argue the only similarity to a warrant is the standard of probable cause.[56] Microsoft disagrees on the basis that the Rule has never been applied to require a caretaker to import a customer's records from abroad.[57] Furthermore, they restate their argument in regards to the use of the term warrant.

Lastly, Microsoft argues the district court should not be concerned criminal investigations will be hampered if § 2703(a)'s application is limited to U.S. territory.[58] Other tools, such as the MLAT are available for the government to obtain necessary electronic data. Affirming the district court's decision would give the U.S. a unilateral authority to seize emails from foreign soil. This unilateral authority contradicts treaties already in place and foreign countries will want to assert the same authority.

Government's Argument to Federal District Court

[53] Brief for the Appellant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).
[54] *Id*.
[55] *Id*.
[56] *Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014)*
[57] *Id.*
[58] *Id*.

The Government focused on Microsoft's control of the requested data rather than the data's location. As long as the data was in Microsoft's control, where they choose to store it has no relevance for production.[59] The DOJ urged that there is nothing in the text or legislative history that limits the scope of the warrant based on the location of the data. In fact, the DOJ argues that the scope of the SCA warrant is broad, allowing a Judge to issue an SCA warrant when it has jurisdiction over (1) the offense under investigation, (2) the physical location of the service provider, or (3) the storage site of the relevant records.[60] Microsoft is a company located within the United States. Therefore, the Court had a right to compel production of the data.

The DOJ disputed that the SCA warrant is a physical search is and they argue that they have not requested one. The text of the statute requires Microsoft to produce wire communication under § 2703 and allows review of that data by law enforcement. Microsoft will simply access the data from the U.S. and provide it to the government.[61] The production of the documents does not require the assistance of law enforcement nor will law enforcement be present. Therefore, the government is not conducting a search and Microsoft is wrong to characterize it as such.[62]

The Government agreed with Judge Francis in that an SCA warrant is a hybrid. The SCA warrant is obtained like a search warrant and executed like a subpoena. The Judge clarified that Congress intended for SCA warrants to operate as a form of compulsory process, functionally similar to subpoenas. Thus, the SCA specifically uses the language of compulsory process in describing how electronic communications may be obtained by warrant, providing that the Government may use a warrant to "require the disclosure" of communications "by a provider."[63]

Lastly, the Government contends that the production of records for a Federal criminal investigation historically had not been limited because the documents are located abroad. A requirement like this would hinder the effectiveness of the Government to conduct criminal investigations. It would also allow persons to avoid criminal prosecution by electing to have their documents stored abroad. There is no argument to be made that this is what congress

---

[59] *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, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).*
[60] *Id.*
[61] *Id.*
[62] My recollection of how this law developed is different. As a prosecutor, I used similar orders under state law and warrants to obtain data. It was responded to by companies and not by direct search in part because the law enforcement officers likely could not obtain the data they wanted in reality and did not desire to travel to the data centers to work with them to obtain a response. This may not have been the experience everywhere, however.
[63] *Id at 8.*

wanted. Microsoft cannot argue particularity, because it failed to raise it at the magistrate level. Even if the argument is allowed, the particularity requirement under the Fourth Amendment is satisfied. The warrant requested production of emails from a specific user account.

Amici in Support of Microsoft

Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) argued that the magistrate erred in determining no Fourth Amendment event occurs until the data received is reviewed in the U.S.[64] According to EFF a Fourth Amendment seizure occurs when the data is collected abroad.[65] Then, a Fourth Amendment search occurs in the U.S. once the government reviews the data. EFF also argued that the use of the term "warrant" in the SCA implies it should have the traditional attributes of a Rule 41 warrant. Therefore, the warrant would not apply outside U.S. territory. Lastly, EFF argues that the foreign seizure in question would fail a reasonableness standard[66] because it does not comply with Irish Law.

Verizon

Verizon asserts the text of the SCA and its legislative intent does not provide for extraterritorial effect.[67] Verizon's argument is based on a longstanding history that unless expressly stated, a statute will only apply within the territorial jurisdiction of the United States. Allowing U.S. search warrants to obtain data stored abroad will interfere with sovereign authority of other nations and could potentially conflict with foreign data protection laws.

Verizon also argues the Magistrate's ruling will negatively impact American businesses.[68] The Magistrate's ruling would grant government agencies access to foreign data that they previously were not privy to. The expanded access to foreign data would cause foreign companies to move their businesses to areas that are not associated with the United States.[69]

---

[64] *Brief Amicus Curiae of Electronic Frontier Foundation in Support of Microsoft Corporation, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).*
[65] *Id.*
[66] *Id.*
[67] *Memorandum of Law in Support of Verizon's Communications Inc.'s Motion to Participate as Amicus Curiae and Microsoft Inc.'s Motion to Vacate Search Warrant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).*
[68] *Id.*
[69] *Id*.

Lastly, Verizon contends that allowing access to foreign data may interrupt agreements that are already in place.[70] Ireland is a member of the MLAT and Verizon believes the MLAT is the appropriate avenue in obtaining information from treaty members.

Apple and Cisco

Apple and Cisco argue the MLAT should have been utilized, as Ireland is a member. By failing to use MLAT, the United States is encouraging other nations to disregard treaties currently in place.[71] Secondly, Apple and Cisco argue the Magistrate failed to give adequate consideration to international law. Specifically, the court did not address possible violations of foreign laws and the impact that could have on service providers. Lastly, Apple and Cisco argue the Electronic Communications Privacy Act does provide a basis to forego a comity analysis. The Court should have considered the laws and interests of foreign states in making its ruling.

AT&T

Similar to Verizon, AT&T argues a statue will only apply within U.S. territory unless there is clear congressional intent to the contrary.[72] AT&T further argues the use of the word "warrant" in the SCA does not authorize compelled disclosure of information that lacks a substantial nexus to the United States.[73] The word "warrant" is taken from the Fourth Amendment. Therefore, it was the intent of congress to provide Fourth Amendment protection for computer networks.

Next, AT&T argues the court erred in failing to determine whether the warrant would violate any laws of Ireland.[74] The court focused solely on Microsoft being a U.S. company. Instead, the court should have conducted a comity analysis. If it is found that SCA should apply extraterritorially, it should be limited to a case-by-case analysis. If the court fails to do this, it may cause issues with treaties that are currently in place. Specifically, foreign countries may ignore MLAT. If the U.S. ignores MLAT and obtains foreign data by other means, such as here, treaty members may do the same.

---

[70] *Id*.
[71] Memorandum of Law in Support of Motion by Apple Inc. and Cisco Systems, Inc. to Participate as Amicus Curiae and Microsoft Inc.'s Motion to Vacate Search Warrant, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).
[72] Memorandum of Law Amicus Curiae AT &T Corp. in Support of Microsoft Corporation, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).
[73] *Id*.
[74] *Id*.

Commentators

Marc Zwillinger

Mr. Zwillinger argues that the ruling should not offend the senses in that it is very narrow. It focuses on U.S. entities that have possession and control of foreign records that are easily accessible from the U.S.[75] The opinion does not address foreign subsidiaries or affiliate companies' possession of data that is stored abroad.[76]

Orin Kerr

Professor Kerr does not believe Microsoft's argument under the Fourth Amendment is valid if the account holder is not a U.S. person.[77] Only U.S. persons have a right to Fourth Amendment protection and the holder of the account in question is likely a foreigner. Microsoft claims that data is stored based on where the account holder lives. Therefore, it is likely that the account holder is a resident of Ireland. If this is true, the account holder only has statutory rights to privacy.

Kerr argues that ordering Microsoft to copy these emails and give them to the Government constitutes a Fourth Amendment seizure.[78] Once the government looks through the files, a search has taken place. Because the Fourth Amendment seizure would take place outside the United States, a reasonableness standard would apply. This is the comity analysis mention by other parties to the matter. Even if Microsoft is successful, the DOJ will likely be able to obtain foreign emails through a U.S. subpoena.[79] Again, the Government would have to look at multiple factors instead of simply obtaining the data under the SCA.

Kate Westmoreland

The question Ms. Westmoreland wants answered is, what criteria should jurisdiction for user data be based on? The four options she considers are data location, user location,

---

[75] *Marc Zwillinger, Microsoft Ordered to Produce User Data Stored in Ireland: Plans to Appeal (2014), http://blog.zwillgen.com/2014/04/30/microsoft-ordered-produce-user-data-stored-ireland-plans-appeal/ (last visited on June 3, 2015)*.
[76] *Id*.
[77] *Orin Kerr, What legal protections apply to e-mail stored outside the U.S. (2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/ (last visited on June 3, 2015)*
[78] *Id*.
[79] *Id*.

company location, and terms of service.[80] Currently Microsoft is advocating for jurisdiction based on data location. Data is often stored in multiple jurisdictions and moves throughout different jurisdictions, so this may not be the best idea. Companies such as Google, Twitter, and Facebook have adopted jurisdiction based on headquarters. This allows for some consistency when legal issues arise. Ultimately, Ms. Westmorland believes the laws governing data should be based on location of the person rather than location of the data. If multiple states assert jurisdiction, a separate analysis can be conducted.

The European Parliament Perspective

A member of the European Parliament filed an amicus brief criticizing the Department of Justice's position.[81] Jan Philipp Albrecht is a member of the European Parliament from Germany, who serves as the vice-chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, among his other responsibilities.[82]

Mr. Albrecht argues that by allowing the Department of Justice to proceed to collect the requested information from Ireland through a warrant issued to Microsoft in America, the Department of Justice is improperly bypassing the entire legislative framework currently in place to handle such a need. Further, such action will adversely impact the ability for the exchange of data between the United States and the EU member states in the future.[83] Importantly, Mr. Albrecht emphasizes the large difference in how personal data is handled in the United States versus how it is handled in Europe, even stating how executive branches in each entity have acknowledged those differences all the way back in 2003 during the conclusion of the U.S. – EU Agreement on Mutual Legal Assistance.[84] He expresses the opinion that because the data at issue in this case is located in Ireland, that the data subject must benefit from regulatory protections in place for EU citizens.[85]

Mr. Albrecht directly addresses one of the important arguments in the Case. The Department of Justice has argued that it is uncertain whether it is even illegal for Microsoft to

---

[80] Kate Westmoreland, Jurisdiction over user data-what is the ideal solution to a very real world problem? (2014), http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem (last visited on June 4, 2015)

[81] Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014) accessed on June 5, 2015 at http://digitalconstitution.com/wp-content/uploads/2014/12/albrecht-microsoft-ireland-amicus-brief1.pdf.

[82] *Id* at p. 3.

[83] *Id* at pp. 3-4.

[84] *Id* at p 5.

[85] *Id* at p. 8.

retrieve the requested data from Ireland.[86] Mr. Albrecht, however, expresses his opinion that it most certainly is illegal in the eyes of the European Parliament, as follows:

> "One of the protections is that the data will not be transferred to a country outside the EU unless the recipient has in place safeguards to ensure that the data will receive equivalent protection to that which it is afforded in the EU.13 Under these provisions the transfer by Microsoft of the content of the email account from Ireland to the United States is not permitted by EU law. However, the criminal law exceptions in the European directives, including as covered by the EU MLAT procedures, would permit Irish law enforcement authorities to obtain the information, but do not permit Microsoft to send the data to the U.S. to be handed to the U.S. Attorney there."

Mr. Albrecht adds that even if the warrant at issue could be applied to legally request the electronically stored information in Ireland, that such a position would give rise to a conflict of jurisdiction.[87] Finally, he asserts that the "refusal of the U.S. Attorney to recognize that the email account at issue is located in a foreign jurisdiction and subject to foreign data protection rules is not only offensive to the sensitivities of European citizens but also reinforces the already strong sentiment of many EU citizens that their data is not "safe" when they use IT services offered by U.S. Corporations."[88]

The Irish Perspective

On December 15, 2014, Digital Rights Ireland Limited, Liberty and The Open Rights Group filed their Brief of Amici Curiae in support of Microsoft's position.[89] They present several points.

The initial argument is that data privacy is a human right under Irish law; but, it cannot be used to subjugate criminal investigations.[90] They point out that Article 2 of the EU Data Protection Directive provides that "the protections do not apply to data processed in the course of 'the activities of the State in areas of criminal law.'"[91]

They then argue that MLATs should be used instead of judicial directive because those treaties were specifically negotiated to account for such circumstances. In 2006, long after the

---

[86] *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, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d. No. 13 Mag. 2814, 2014 WL 1661004, (S.D.N.Y. Apr. 25, 2014).*
[87] Brief of Amicus Curiae Jan Philipp Albrecht, at p. 9.
[88] *Id* at p. 11.
[89] *See* Brief of Amici Curiae Digital Rights Ireland Limited, Liberty and The Open Rights Group, No 14-2985-cv (2nd Cir. 2014).
[90] *Id* at p. 8.
[91] *Id, quoting,* Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) at p. 38.

Electronic Communication Privacy Act of 1986 was enacted, the United States overhauled MLATs with twenty five member states.[92] This action took into account the arguments that the Department of Justice is now making and specifically was agreed to as the method to obtain evidence from Ireland in criminal investigations, without any modifications to United States law. Not going through this procedure is ignoring the United States' own Federal law and goes directly against what the Executive Branch had previously put forth during the course of executing the MLATs.[93]

Conclusion

The way in which criminals have operated in geographical locations very remote from their targeted locations has given rise to many problems for law enforcement, as well as for privacy advocates. The recent developments in how search warrants may be used in U.S. Federal law enforcement investigations raise several implications. While not new to the discussion on how electronic evidence is to be obtained, the fact that the Proposed Amendments and the case of Microsoft v. Ireland may be so close to completion means that substantial changes could be imminent. The scope of this discussion paper does not allow meaningful discourse on all of the possible repercussions from the above-referenced actions. However, it is surely an appropriate topic for discussion.

[92] *Id* at 15.
[93] *Id* at pp. 20-25.