KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

MICROSOFT IRELAND CASE: BACKGROUNDER

CAN A U.S. WARRANT COMPEL A U.S. PROVIDER TO DISCLOSE DATA IT STORES ABROAD

July 17, 2014

The animating question in this case is whether a U.S. law enforcement agency can compel a U.S. provider of communications service to disclose the content of digital information the provider stores outside the U.S. The Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA) of 1986, does not explicitly address the issue. The SCA authorizes the Government to seek the contents of stored communications that are more than 180 days old, using a subpoena, a court order issued under 18 USC 2703(d), or a warrant. The Government takes the position that a subpoena can also compel disclosure of opened email no matter its age. However, Microsoft and most other large providers apply *U.S. v. Warshak,* 631 F.3d 266 (6th Cir. 2010) on a nationwide basis, and require warrants for all content. As a result, the stakes about resolution of this case are quite high: does a U.S. provider put content out of the reach of the U.S. government acting under the SCA by storing the data abroad?

Facts: On December 4, 2013, a magistrate in the Southern District of New York issued a warrant that directed Microsoft to produce content and non-content information about a user whose account is associated with its Dublin, Ireland datacenter. Microsoft's wholly-owned subsidiary, Microsoft Ireland Operations, Ltd., leases and operates the datacenter. Microsoft began storing email data there in September, 2010. Microsoft stores users' email information at datacenters around the world and assigns users to different datacenters according to proximity in order to increase communications quality and decrease network latency. When the user signs up for email service, he or she is prompted to enter a country code that Microsoft uses to decide where to locate the user's data. Microsoft maintains non-content metadata associated with the account in the U.S. The warrant was issued under 18 USC 2703(a), which requires the Government to use the warrant procedures described in Rule 41 of the Federal Rules of Criminal Procedure. Rule 41 is silent as to whether it has extraterritorial effect. Microsoft produced the non-content data stored in the U.S., but objected to producing the content information stored in the Ireland datacenter and on December 18, 2013, moved to vacate the warrant for that content. The magistrate judge rejected Microsoft's motion to vacate. Microsoft appealed to the District Court for the Southern District of New York.

The parties have briefed the case, and Microsoft enjoys amicus support from AT&T, Verizon, Cisco/Apple and the Electronic Frontier Foundation. The briefs

filed thus far, the Magistrate's opinion, and certain commentary on the case, are summarized below.

I. Arguments and Magistrate Opinion

A. Microsoft's Argument to the Magistrate

Microsoft argued to the magistrate that the warrant he had issued would require an extraterritorial search and seizure of data stored in its Ireland datacenter. According to Microsoft, a search of digital data occurs where the data is stored, not at the point from which the data is remotely accessed. Absent specific congressional authorization, statutes are presumed to have no extraterritorial effect. Since there is no authorization for extraterritorial application in Rule 41, the SCA, or elsewhere, the Government cannot execute a search and seizure in Ireland, and the Government cannot achieve this end indirectly by forcing Microsoft itself to produce the data, it argued. Microsoft pointed out that when the USA PATRIOT Act amended the SCA to permit judges to issue warrants for data outside the judge's district, it provided for "Nationwide Service of Search Warrants for Electronic Evidence" and not for worldwide service. It pointed out that in 1990, the Supreme Court expressly rejected a proposed amendment to Rule 41 that would have permitted issuance of warrants to search property outside the U.S. Microsoft conceded that a subpoena could compel it to produce responsive non-content outside the U.S. It said that the Government could compel disclosure of content stored in Ireland using the Ireland-U.S. Mutual Legal Assistance Treaty (MLAT). Microsoft did not argue that Irish law prohibits the disclosure of the content sought by the Government. However, it argued that considerations of international comity undercut the Government's policy arguments: when a subpoena calls for data stored outside the U.S., a motion to quash provides a mechanism for courts to consider comity matters; warrants do not provide such a mechanism.

B. The Government's Argument to the Magistrate

On February 14, the Government responded that U.S. service providers cannot avoid compliance with compulsory SCA process simply by storing data abroad. It argued that because the service provider itself, and not the storage location of the records, is the subject of the warrant, the issue is whether the content sought is in the service provider's custody or control, not whether it is in the U.S. The Government pointed out that the statute says the Government "may require the disclosure" by a service provider. It argued that the SCA is structured like an upside down pyramid, and that all information available with less rigorous legal process (such as a subpoena) is also available through more demanding process (such as a warrant). It argued that had Microsoft received a subpoena for opened email or email more than 180 days old, it would have to comply, citing the *Bank of Nova Scotia* (740 F.2d 817, (11th Cir. 1984)) line of cases compelling companies to produce subpoenaed documents located abroad even when such production would violate foreign law.

It argued that an "SCA Warrant" is different from a normal warrant because it functions like a subpoena in that it compels a service provider to gather and produce the data itself, as

opposed to authorizing entry into a physical premises in order to conduct a search and seizure. Consequently, the Government claimed, it is not subject to the typical substantive limitations of a warrant, just the procedural. The SCA explicitly incorporates only the *procedures* of Rule 41. Finally, the Government argued that to rule against it would undermine criminal investigations for several reasons. Whether records covered by a warrant are produced would depend on a provider's "arbitrary decision" to store documents abroad. Criminals could simply register their email using a non-U.S. country code and make their data inaccessible to law enforcement under the SCA. Mutual Legal Assistance Treaties (MLATs) and letters rogatory are too slow and cumbersome to be adequate alternatives, the Government claimed.

C. The Magistrate Opinion

The magistrate judge denied Microsoft's motion to vacate the search warrant. The magistrate first determined that the statutory language is ambiguous as to whether 2703(a) incorporates substantive warrant requirements of Rule 41, or just the procedural. Given the ambiguity, the magistrate looked to the SCA's structure and legislative history for guidance. The magistrate found that warrants issued under the SCA are "hybrids:" part warrant and part subpoena. An SCA warrants is obtained like a warrant (based on a showing of probable cause to a magistrate) and executed like a subpoena in that it is served on a provider that possesses information. As a result, the extraterritorial limits on warrants are not implicated and the relevant question is whether the data is in the provider's control. Moreover, the magistrate opined, a search does not even occur until the data is reviewed by law enforcement in the U.S., so there *is* no extraterritorial search. The concerns that motivate the presumption against extraterritorial application are not present: an SCA warrant does not involve deployment of US law enforcement personnel abroad. Finally, the magistrate gave weight to the practical considerations noted by the Government and emphasized that the MLAT process was "slow and laborious," and that countries retain discretion to turn down an MLAT request. The U.S. does not have MLATs with some countries, and servers could be located in server farms at sea, beyond any country's jurisdiction, so under Microsoft's reasoning, a provider could make information within its control completely unavailable to law enforcement.

D. Microsoft's Argument to the Federal District Court

"The Government cannot seek and a court cannot issue a warrant allowing federal agents to break down the doors of Microsoft's Dublin facility. Likewise, the Government cannot conscript Microsoft to do what it has no authority itself to do – i.e., execute a warranted search abroad."

Microsoft asserted that the Government takes the "extraordinary position" that it can access "private emails of any subscriber no matter where the data is located, and without the knowledge or consent of the subscriber or the relevant foreign government where the data is stored" by serving an SCA warrant on a U.S.-based service provider. This interpretation, Microsoft argued, blatantly rewrites the statue and reads the particularity requirement out of

the Fourth Amendment for digital data. Microsoft maintains over 100 data centers in 40 countries and the warrant purports to authorize a search of all of them. The Government reads a new "hybrid subpoena" into the SCA for datacenters, where a growing proportion of global information will be stored, ignoring the ordinary meaning of the term "warrant," Congressional intent, and critical distinctions between subpoenas and warrants.

A warrant, Microsoft pointed out, gives the Government the power to seize evidence without notice or an opportunity to challenge, but requires a specific description of the thing sought and the place – in the U.S. – to be searched. The search occurs where the data is located. A subpoena on the other hand, gives the Government the power to require a person to collect items in her possession, custody or control, regardless of location, and bring them to court, but gives the recipient an opportunity to move in advance to quash. *"Here, the Government wants to exploit the power of a warrant and the sweeping geographic scope of a subpoena, without having to comply with fundamental protections provided by either."* Even if permitted by ECPA, the magistrate's conclusion contravenes the 4th Amendment requirement of particularity (that the Government must articulate the location and things to be searched and seized specifically) by allowing a search of any stored data worldwide that is in Microsoft's control. Microsoft argues that this would lead to violations of international laws and treaties, of the territorial integrity of sovereign nations, circumvent the commitments made by the U.S. in MLAT agreements designed to facilitate cross-border criminal investigations, and "reduce the privacy protection of everyone on the planet." It pointed out that acts of Congress should be construed wherever possible to align with U.S. international obligations. The Government's position in this case, Microsoft argued, could encourage foreign governments to unilaterally seek data stored in the U.S. from providers that operate internationally, further erodes the trust in U.S technology companies' ability to protect the privacy of personal information located outside the U.S., and will ultimately erode the leadership of U.S. technology companies in the global market.

E. The Government's Argument to the Federal District Court

The Government argued, *"[t]he warrant properly requires Microsoft to disclose data under its control regardless of where Microsoft has chosen to store the data."* The text, structure and legislative history of the SCA do not limit the statute's scope based on the location of stored records. The key issue is Microsoft's control of the data, not its location. There is no extraterritorial application of the law because the law is being applied exclusively within the U.S. to a U.S. provider served within U.S. territory. Additionally, to bring to bear the presumption against extraterritoriality and potential conflicts with international law, Microsoft inappropriately analogized the SCA warrant to a physical search, where there is forced entry by law enforcement to a location, rather than acknowledging that Microsoft *itself* must produce the documents in its control, regardless of location. For Microsoft to challenge compulsory process on comity grounds, the Government pointed out, it must first establish that production of the records would violate the law of the state in which the documents are located, something Microsoft did not even assert below. In addition, argued the Government, there is nothing in international law that *requires* the use of an MLAT to obtain evidence located in a foreign country when there are other lawful means of obtaining it. An

MLAT is simply one mechanism.

Practically, the Government said, law enforcement's effectiveness would be significantly impeded by Microsoft's position since this information can be stored anywhere - even in areas not under any country's territorial jurisdiction – and can be relocated quickly. An MLAT request "typically takes months to process," if a treaty even exists between the U.S. and the foreign nation. A provider could, "for legitimate or illegitimate reasons," distribute the contents of a single user account across computers maintained in dozens of countries, making it practically impossible for the Government to collect the data through international channels. Microsoft's position means in practice, the Government claimed, that where a user's data is stored depends entirely on which country the user selects when signing up for the account; criminal users may well lie their way out of SCA coverage. According to the Government, foreign relations concerns raised by Microsoft should ultimately be left to the other two branches of government, and the impact on Microsoft's business is simply "beside the point." (p. 27). Lastly, the Fourth Amendment's particularity requirement is satisfied by the warrant's articulation of a particular, clearly identified user account. The Government is not typically in a position to know where the provider has located data. Moreover, Microsoft waived the particularity issue in failing to raise it to the magistrate judge.

II. Amici in Support of Microsoft

A. Electronic Frontier Foundation

EFF argued that the magistrate erred in finding that no Fourth Amendment event occurs until the government reviews the data in the U.S. Regardless of when the "search" of the data occurs, a Fourth Amendment "seizure" occurs abroad, when Microsoft copies the data in Ireland to fulfill the warrant. That is when a "meaningful interference with an individual's possessory interest" occurs. Accordingly, this warrant would be used to seize data abroad, and that data U.S. warrants cannot reach. EFF also argued that the magistrate erred failing to understand that Congress' use of the term "warrant" in the SCA signals its intent to require all of the attributes of a warrant, including the territorial limitations on warrants. Because the warrant requested all emails stored in the account, it also failed the particularity requirement of the Fourth Amendment. Finally, EFF contended that a foreign search or seizure that does not comply with Irish law and the MLAT process fails the Fourth Amendment's reasonableness requirement.

B. Verizon

Verizon had already taken the position that the U.S. government cannot compel a company in the U.S. to produce its customers' data stored in data centers abroad, whether it uses a warrant, subpoena, an order under Section 215 of the PATRIOT Act, or Section 702 of FISA. Verizon argued the SCA should not apply extraterritorially since the text does not show a clear intent to have extraterritorial effect and the legislative history shows a clear intent to regulate activities only within the territorial U.S. In addition, the law should be interpreted wherever possible to avoid unreasonable interference with the sovereign authority of other

nations. It cited a statement by the European Commission spokeswoman that the Commission's position is that the data shouldn't be transferred to U.S. authorities from Europe other than through "formal channels of co-operation," such as the MLAT process. Additionally, while the magistrate's position might facilitate criminal investigations, it would hurt American businesses to the tune of billions of dollars, and undermine U.S. relationships and agreements with foreign nations. Foreign relations law requires that officials in one state not exercise their functions in territory of another state without consent. Verizon, like EFF, also contended that the search occurs when the provider retrieves the data, not when law enforcement accesses it in the U.S., and the seizure takes place when the data is copied abroad by the service provider. The Government's position could result in "an international free-for-all," Verizon argued, with conflicts of law becoming the norm rather than the exception as other countries rush to impose on companies doing business abroad the obligations the U.S. Government is attempting to impose in this case.

C. Apple and Cisco

Apple and Cisco argued that the magistrate did not give adequate consideration to international law, comity, and reciprocity. The ruling could force service providers to violate the laws of foreign nations, given likely conflicts of law between the SCA and laws abroad. This puts the providers and their employees at significant risk of foreign sanctions. Moreover, the MLAT process, while not as simple as a warrant, it is not necessarily overly burdensome given the many FBI legal attaché offices abroad and the existence of numerous MLATs. Disregarding the MLAT process could encourage other nations to disregard the treaties, harming U.S. interests.

D. AT&T

AT&T argued that the magistrate's decision is troubling because it makes the provider's status as a U.S. entity the only factor relevant to whether U.S. authorities may use U.S. procedures to require disclosure of customer information. Instead, a court should consider whether the relationship between the customer and provider is centered abroad, the customer's ties to the U.S. and whether foreign law imposes different or additional data protections. AT&T contended that warrants for internationally stored data that can be "technical[ly] access[ed]" from the U.S. are unauthorized extraterritorial warrants absent "a substantial nexus" to the U.S. AT&T argued in the alternative that if the court does decide to apply the warrant provision extraterritorially, it should consider principles of international comity on a case-by-case basis and ordinarily require use of the MLAT process. Otherwise, given reciprocity, other nations could disregard the MLATs and seek data stored in the U.S. directly from the U.S. providers that have affiliates abroad. This would be detrimental to U.S. data privacy interests: the SCA contains numerous limitations to data demands, and due process and litigation rights that are not necessarily replicated abroad.

III. Commentators

A. Marc Zwillinger

Zwillinger argues the decision is narrow; it is limited to cases where the U.S.-based "entity has possession and control of foreign records which are reasonably accessible from the U.S." The decision did not address how an SCA warrant would apply to records stored abroad in a foreign subsidiary or affiliated company pursuant to an agreement that would prohibit the U.S. entity from accessing the records.

B. Orin Kerr

Kerr believes that Microsoft cannot successfully challenge the warrant on Fourth Amendment grounds and that its SCA challenge is a close call. The Fourth Amendment challenge, Kerr argues, is not yet ripe because we do not know whether the user whose data is sought has sufficient contacts with the U.S. to enjoy Fourth Amendment rights, and because how agents might search through the emails when they have been obtained has not been established. Even if the user has sufficient contacts to enjoy Fourth Amendment rights, when the seizure occurs outside the U.S. (as it does here, when the copy of the data stored in Ireland is made), the warrant requirement does not apply. The "reasonableness" prong of the Fourth Amendment applies, and is likely met because a magistrate already found probable cause.

With respect to the SCA challenge, Kerr believes that 18 USC 2703 is territorial, but that it is unclear what determines territoriality - the location of the data or the company – for a U.S. based provider with data stored abroad. Finally, even if Microsoft wins, the U.S. government would use subpoenas (not warrants) to seek the data U.S. providers store abroad, resulting in fewer privacy protections. If the SCA does not apply abroad, and the email sought is extraterritorial, the SCA's statutory warrant requirement will also not apply, and the government could just subpoena the emails stored on the foreign server. When the government subpoenas information stored abroad, courts called upon to enforce the subpoena must consider international norms of comity, and engage in complex balancing test the government would rather avoid by simply getting a warrant for the data. Kerr believes that the SCA needs to be amended to deal expressly with the extraterritoriality problem.

C. Kate Westmoreland

Westmoreland says that the case raises important issues: What criteria determine which laws apply to a user's data (where the data are stored? Where a company is headquartered? Wherever the terms of service specify?) When does a search or seizure of data occur? (When the company copies the data from the server? When it hands the data to the government? When a government official looks at the data?) She points out that Microsoft seems to be advocating jurisdiction on the basis or location of the data, which is consistent with its terms of service. They specify that different jurisdictions' laws apply

depending on where the user is located (which, she says, presumably has some correlation to data location). Google, Facebook and Twitter, she points out, have terms of service that say the laws of California, where their headquarters are located, always apply. This, she says, better enables them to provide services world wide, but turn down data requests from governments that seek data for nefarious purposes.

For more information, please contact Greg Nojeim, Director of CDT's Project on Freedom, Security and Technology, gnojeim@cdt.org, 202/637-9800. (END)