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

NEITHER WARRANTS NOR SUBPOENAS SHOULD REACH DATA STORED OUTSIDE THE US

7/30/14

Microsoft's challenge to a warrant issued by a US court seeking to compel the company to disclose customer email stored at a data center in Ireland raises a question of growing importance: What rules should apply when one country demands from service providers with a physical presence on its territory access to communications stored in another country? Developments in the US and globally – including the Snowden leaks and the growing assertiveness of other countries for both data localization and transborder authority – heighten the urgency of the issue.

In the era when companies offer their services to customers around the globe and store data on dispersed networks linked though global communications networks, two or more governments are likely to have legitimate interests in the same piece of data. In the law enforcement context, the best way to accommodate the interests of both governments is through the process established under Mutual Legal Assistance Treaties (MLATs). In the Microsoft case, the US government is seeking to avoid the MLAT process. It is arguing that a warrant issued in the US can compel Microsoft to copy and disclose data stored in Ireland.

The US government position contravenes the longstanding principle that warrants issued by US courts are generally not enforceable outside the US. It also conflicts with the concept of comity, which US courts have long recognized requires them to give due regard — and, where appropriate, deference — to the laws and legal system of a foreign country. Applying the US government's position on a globally reciprocal basis would yield chaos, with governments serving demands on local representatives of global companies seeking disclosure of data stored elsewhere and covered by the laws of the country where it is stored. That would be especially burdensome to US companies, which currently store, in the US and elsewhere, a disproportionate share of the world's data. It would also harm US citizens, as foreign governments could demand from local representatives of US companies the communications of Americans under standards weaker than those that apply in the US.

Finally, the case brings to the fore a critical issue that so far has been largely overlooked in discussions about government access: The emails that Microsoft stores on behalf of its customers are not Microsoft's "business records," and they should not be subject to the disclosure rules applicable to business records.

I. Background

On April 25, 2014, a magistrate judge in the Southern District of New York ruled that Microsoft must turn over email content stored on a server in Ireland pursuant to a search warrant issued under the Stored Communications Act (SCA). Microsoft has challenged the magistrate's order. Technology companies AT&T, Verizon, Apple, and Cisco have filed "friend of the court" briefs supporting Microsoft. So has the Electronic Frontier Foundation. The government argues that the warrant properly requires Microsoft to disclose data under its control regardless of where Microsoft has chosen to store the data. CDT has prepared a backgrounder on the case that summarizes key legal documents and commentary related to the case.

A few factors seem relevant: The case involves a criminal investigation being conducted in New York. It is generally assumed that the person who owns the account at issue is not a US resident or a US citizen; in any case, the government has not asserted that he is. Microsoft employees in the US have the ability to access and copy the data from the Irish servers. The government does not claim that the account holder intentionally sought to evade US process or that Microsoft created a data center in Ireland to evade the reach of US government agents.

II. Fundamentals of Extraterritoriality

With only a few exceptions not relevant here (and discussed in greater depth below), a search warrant issued by a US court has no effect outside the territory of the US. Referring to searches of non-citizens' homes in foreign jurisdictions, Justice Stevens said, "American magistrates have no power to authorize such searches." United States v. Verdugo-Urquidez, 494 U.S. 259, 279 (1990) (Stevens, J., concurring). The same is true of seizures of property (including information): Rule 41 of the Federal Rules of Criminal Procedure explicitly describes the authority of federal magistrates to issue warrants for searches and seizures and clearly does not include any general authority to issue warrants to seize property that is located outside the US. The fact that Rule 41(b)(5) *does* expressly allow warrants for seizure of property in US territories, possessions or commonwealths, and in US embassies and consular posts, reinforces the conclusion that there is no general authority to issue warrants for seizures abroad.

Likewise, the Stored Communications Act has no extraterritorial effect. "When a statute gives no clear indication of an extraterritorial application, it has none."

Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010). In the SCA itself, there is no indication of extraterritorial application, and the magistrate judge in this case recognized that. Extraterritorial application would have absurd results, prohibiting, for example, US companies that offer services abroad from ever complying with the demands of foreign governments for disclosure of communications content, even when the data is created and stored entirely outside the US by persons having no connection with the US. (Compare the prohibitions of Section 2702(a) with the definition of governmental entity in Section 2711(4).)

In the Microsoft case, the US government attempts to avoid the territorial limits on warrants by arguing that the search or seizure occurs inside the US, either in Washington state, when the Microsoft employee accesses and copies data stored in Ireland, or in New York City, where US government investigators will review the email. Alternatively, the government argues that there is no search or seizure at all, but only a "compelled disclosure."

III. Where Does the Search or Seizure Occur?

The government's argument that the search or seizure would occur only in the US is rebutted by cases holding that a seizure occurs when and where data is copied. The Second Circuit has found that the act of copying electronic files constitutes a seizure, even before an agent searches through the data. United States v. Ganias, 12-240-CR, 2014 WL 2722618 (2d Cir. June 17, 2014). See also United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (referring to the copying of electronic files as a seizure); United States v. Bach, 310 F.3d 1063, 1067 (8th Cir. 2002) (characterizing Yahoo!'s copying of subscriber's email content as "items 'seized'[,] located on Yahoo!'s property").

Other courts have held that a search or seizure of computer data occurs where the computer is located. United States v. Gorskhov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) (search of computer occurs where the computer is, not where the person conducting the search is sitting). As Magistrate Judge Smith has noted, "digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location." In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 757 (S.D. Tex. 2013). The court, just as a search "takes place, not in the airy nothing of cyberspace, but in a physical space with a local habitation," so also a seizure takes place in a physical location, and that is where the data resides.

IV. What is the Reach of an SCA Warrant?

The SCA states that the government may use a warrant "issued using the procedures described in the Federal Rules of Criminal Procedure … by a court of

competent jurisdiction" to obtain email from an electronic communication service provider. The SCA is silent however, on the reach of a warrant. Instead, one must look to the Federal Rules of Criminal Procedure and specifically to Rule 41, which governs search and seizure.

Rule 41 is very explicit: Property is defined to include information, Rule 41(a)(2)(A), and magistrates have authority to issue warrants for seizure of property only under four circumstances described in Rule 41(b):

(1) property located within the district where the warrant is issued;
(2) property that is located within the district when the warrant is issued but that might move outside the district before the warrant is executed;
(3) in an investigation of domestic terrorism or international terrorism, property located outside the district of the issuing court;

(5) property located outside the jurisdiction of any state or district but within a US territory, possession or commonwealth or within the premises of a US diplomatic or consular mission or a residence or appurtenant land owned or leased by the US government and used by US personnel assigned to a US embassy or consulate.

It is a separate question whether (b)(3) would authorize warrants for searches outside the territory of the US, but the government has not argued in the Microsoft case that (b)(3) supports its warrant. Instead, the Justice Department ignores the provisions of Rule 41 and relies on the provisions of the SCA which state that a warrant may be issued by a "court of competent jurisdiction." In doing so, the government confuses jurisdiction over a case with the reach of a governmental authority.

The SCA defines "court of competent jurisdiction" to include a court that has jurisdiction over the offense being investigated as well as a court that is in a district in which the service provider is located or in which the wire or electronic communications, records, or other information are stored. In the Microsoft case, the US district court for the Southern District of New York is a court of competent jurisdiction because it apparently has jurisdiction over the offense being investigated.

However, as the Supreme Court in *Morrison* made clear, the question of jurisdiction of a court is different from the question of what is the authority of the court to regulate conduct. 561 U.S. at 254. A court of jurisdiction can only issue warrants with the scope authorized in Rule 41; and Rule 41 says that warrants, with exceptions not applicable here, can only be issued for property (including information) that is located within the US.

V. A Search By Any Other Name

The government attempts to evade the territorial limitations placed on search warrants by arguing that an SCA warrant is actually part search warrant and part subpoena. The magistrate judge relied on this approach in asserting that an SCA warrant is "obtained like a search warrant" but "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 e-mail account in question." That much is undoubtedly true. But it still doesn't make an SCA warrant into a subpoena.

To the contrary, a search or seizure undertaken by a third party acting on behalf of the government still constitutes a search or seizure, even if the government never sets foot on private property. United States v. Jacobsen, 466 U.S. 109 (1984); Cassidy v. Chertoff, 471 F.3d 67, 74 (2d Cir. 2006). As the Sixth Circuit stated in Warshak, "It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search." 631 F.3d 266, 286 (6th Cir. 2010).

The reasons for allowing SCA warrants to be served electronically and executed without the presence of a government official is that it would be both ineffectual and disruptive to have a law enforcement officer present: Ineffectual because the officer would almost certainly not understand the network of the service provider and would have no ability to execute the warrant himself or to even know, looking over the shoulder of the service provider employee, whether the search and seizure was being conducted correctly and completely. Following the Bach decision, 310 F.3d 1063 (8th Cir. 2002), the SCA was amended to add section 2703(g) to make it clear that an officer did not have to be present when an SCA warrant is executed, but 2703(g) also makes it clear that the process being enforced is still a "search warrant" and it is still being "executed."

VI. Compelled Disclosures – "Possession, Custody, or Control"

The government points out that a subpoena generally requires the entity on which it is served to assemble all responsive material in its "possession, custody or control." Relying on what is sometimes known as the Bank of Nova Scotia (740 F.2d 817, (11th Cir. 1984)) doctrine, the government argues that a subpoena can compel Microsoft to reach into its overseas databases, which it controls, and assemble any responsive documents and turn them over to the government. Microsoft maintains over 100 such data centers in 40 countries, according to its brief. The government argues that, if it can require worldwide discovery and disclosure with a subpoena, it should also be able to do so with the higher authority of a warrant. In essence, by arguing that an SCA warrant has the attributes of a subpoena, the Government wants to have its cake and eat it too: it seeks to exercise all of the authority that comes with a warrant, such as access to information without notice to the target,

without the limitations, including the geographic limitations on warrants set forth in Rule 41.

However, search warrants and subpoenas are fundamentally different. In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 854 (9th Cir. 1991) ("subpoenas are not search warrants"); In re Grand Jury Proceedings, 115 F.3d 1240, 1244 (5th Cir. 1997) ("the instruments are different in nature"). Most crucially, as Microsoft explains in its reply brief, subpoenas are limited to compelling disclosure of the *business records* of the entity on which they are served and cannot be used to compel a third party service provider to disclose communications or other property stored on behalf of a customer.

In other words, Microsoft points out, the rule long applied to physical property should also apply to information. FedEx has possession, custody or control of millions of packages every day, but the US government cannot force FedEx to turn over any of those packages with a subpoena. In order to seize a package in the US, the government needs a warrant. See, e.g. United States v. Jacobsen, 466 U.S. at 114 ("the Fourth Amendment requires that [government agents] obtain a warrant before examining the contents of . . . a package.") (And even with a warrant, the government has no power to force FedEx to turn over packages that are outside the US.) Likewise, Marriott has in its custody thousands of pieces of luggage, stored temporarily at hotels in the US and abroad. Again, the US government cannot use a subpoena to force Marriott to turn over luggage held by Marriott, in the US or abroad.

The only reason why the government believes it can use a subpoena to force a service provider to disclose communications stored by the provider is because the SCA includes an outdated provision treating them sometimes as business records, saying that subpoenas can be used to compel third-party service providers to disclose older email and documents in storage with a remote computing service. However, the Sixth Circuit has held this provision of the SCA unconstitutional and has firmly rejected the argument that stored email is a business record that can be compelled with a subpoena. Warshak, 631 F.3d. at 288.

VII. Subpoenas Should Not Be Sufficient to Reach Stored Content

This brings us, finally, to a buried issue in the case, which might seem obvious to a non-lawyer but which came to the fore only in Microsoft's reply brief: Stored emails are not the "business records" of the service provider. They are much more like the property of the subscriber or customer. Consequently, the government cannot compel a service provider to disclose stored communications with a subpoena any more than the government can compel Marriott to disclose stored luggage with a subpoena. In this regard, we have to disagree with the leading scholarly interpreter of the SCA, Orin Kerr, who warns that, if this warrant is quashed, the government could use a subpoena to compel Microsoft to turn over the email it stores in Ireland. We believe the time has come to fully repudiate the notion that email stored by a third-party service provider is that entity's "business records." In the digital world,

such content is much more akin to the property of the subscriber, like the stored luggage, capable of being obtained by the government only with a warrant and subject to the limits of warrants.

This, we believe, is the full implication of the Sixth Circuit's ruling in Warshak, which expressly concluded that "the ISP's 'control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy.'" 631 F.3d. at 287. Instead, as the Sixth Circuit recognized, stored email should be treated the same way that physical packages have been treated, where the courts have held that "mere surrender of custody to a carrier" did not mean that the government could compel disclosure without a warrant. Corngold v. United States, 367 F.2d 1, 7 (9th Cir. 1966). While Warshak was constitutionally based, it points to a broader conclusion even with respect to non-citizens outside the US who have no Fourth Amendment rights: that the kind of control a service provider exercises over content stored on behalf of its users is not the same as the kind of control that supports use of a subpoena to compel worldwide scouring of databases for business records.

VIII. Implications

The ramifications of the US government's approach in this case are deeply troubling. After the Snowden leaks, US businesses began to experience measurable losses of business as customers outside the US feared that use of services offered by a US-based company would expose their data to the US government regardless of where the data was stored. Just recently, Germany's Interior Ministry announced it was terminating a contract with Verizon Germany because of concerns the company may be obligated to turn over data to the US government. If the US government's position prevails, these concerns will be amplified and the damage to US companies will increase.

Reciprocal application of the rule that the US government seeks would mean that foreign governments, at least wherever a US-based company has established a physical presence, could demand access to communications content stored on U.S. servers, pertaining both to US citizens or residents and non-residents. Microsoft, for example, has a physical presence in 100 countries. If the US government position were applied globally, every one of those 100 countries could demand the disclosure of data on US citizens stored in the US, on standards weaker than those applicable in the US.

This is not a fanciful fear: Earlier this month, the United Kingdom adopted legislation that explicitly gives extraterritorial effect to "warrants" for communications content that are issued by a UK minister (not by a judge), based on a standard far more relaxed than probable cause. Privacy NGOs in the UK point out that under this legislation, a UK Secretary of State could serve Google in California with a warrant for "external communications" "requiring it to intercept all communications between subscribers in two specified countries or, for example, all communications leaving or

entering the UK." Other countries could be expected to follow.

We are not unmindful of the negative policy outcomes that a Microsoft victory could propel. If warrants issued by US courts do not have extraterritorial effect and a similar rule is applied world wide on a reciprocal basis, governments may increasingly require providers (including those based in the US) to store data locally to ensure access by local officials.

A Microsoft victory might also spur the US Justice Department to more vigorously resist reform proposals for the Electronic Communications Privacy Act that would impose a warrant requirement for stored content. The DOJ might argue that the statute ought not to preclude subpoena access to content stored abroad.

IX. Returning to – and Strengthening – the MLAT Process

Compared to the chaos of data localization and extraterritorial warrants, there is a far better way to reconcile the competing interests of privacy, international comity and the efficacy of criminal investigations. Mutual Legal Assistance Treaties, or MLATs, are specifically designed to address this situation. MLATs permit the government seeking data for its investigation to request the assistance of the government of the country in which the data is located – and they bind that second government to cooperate.

Indeed, the Justice Department position in the Microsoft Ireland case is at odds with the stated policy of the US government to strengthen the MLAT process and especially to address the delays that have often frustrated investigators. In his January speech on surveillance, President Obama specially stated that he "will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism." Pursuant to the President's commitment, the Department of Justice is leading an interagency effort to update, improve, and accelerate the handling of requests from foreign governments for evidence requested pursuant to MLATs. The DOJ is requesting an additional $24 million in its new budget to hire additional personnel to process MLAT requests and to support training efforts for foreign partners to ensure they can meet US evidentiary standards, which will enable the department to respond to their requests more quickly.

If the US expects foreign partners to go through the MLAT process for data stored in the US, it should follow the same process for data stored abroad.