Why the government cannot use a search warrant to get e-mail located outside the U.S. — unless Congress changes the law.

By Michael Vatis[1]

Orin Kerr has written two interesting posts about some of the legal issues raised by a case in which Microsoft has moved to vacate a U.S. search warrant for a subscriber's e-mails that are located in Ireland. Microsoft's central argument is that a U.S. warrant cannot be used to obtain e-mails located abroad because warrants have no extraterritorial reach. Steptoe filed an amicus brief in the case on behalf of Verizon Communications Inc., so I thought it would be helpful to provide our perspective on the legal issues. (I won't discuss here the profound business and policy implications of the government's position. For that, see the Verizon brief.)

While we disagree with Orin on some of his subsidiary points (as discussed below), we very much agree with the central thrust of his first post: "[T]he Stored Communications Act just wasn't drafted with the problem of territoriality in mind. It assumed a U.S. Internet with U.S. servers and U.S. users."

This recognition that Congress wasn't thinking about extraterritoriality when it passed the SCA is the crux of the Microsoft case. There is a well established doctrine called the "presumption against extraterritoriality," which holds that "legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 248 (2010). Thus, a statute is presumed not to have extraterritorial application unless Congress has "clearly expressed" its "affirmative intention...to give [the] statute extraterritorial effect." *Id*. Orin's acknowledgment that the SCA does not address the extraterritoriality issue should be the end of the story. As the Supreme Court said in *Morrison*: "When a statute gives no indication of an extraterritorial application, it has none." *Id*.

Orin doesn't discuss the presumption against extraterritoriality. But it is at the core of the Microsoft case.

The government has sought to sidestep the presumption against extraterritoriality by arguing that the statute would not actually be applying outside the United States in this case, even though the e-mails it seeks are in Ireland, because the warrant was served on Microsoft in the United States and because the e-mails wouldn't actually be seized or searched until they were in the government's hands in the United States. The government cites no cases supporting this novel argument. Regardless, the government ignores two key facts—Microsoft's computers would be searched when Microsoft—acting at the behest, and as an agent, of the government—looks for the responsive e-mails in Ireland. Moreover, those e-mails would be seized in Ireland when they are copied. On this point, Orin agrees that "the seizure would be occurring outside

[1] Michael Vatis is a partner in the New York office of Steptoe & Johnson, LLP, where he practices appellate litigation and counsels clients on data privacy, cybersecurity, and law enforcement issues. He was formerly an Associate Deputy Attorney General at the U.S. Department of Justice and Director of the National Infrastructure Protection Center at the FBI.

the United States." As a result, it seems undeniable that at least a seizure would be occurring in Ireland, meaning that the search warrant would indeed be applying extraterritorially.

Orin raises an argument different from the government's, asserting that "recent amendments to [Federal] Rule [of Criminal Procedure] 41…expressly allow extraterritorial warrants." But these amendments permit (in certain limited circumstances, such as terrorism investigations) only searches of property outside of the issuing court's *district*. They say nothing about searches or seizures of property located outside of the *country*. Not surprisingly, then, courts have uniformly held that Rule 41 does not authorize searches or seizures outside of the territory of the United States. *See, e.g., U.S. v. Odeh*, 552 F.3d 157, 169 (2d Cir. 2008). Moreover, the Supreme Court rejected a proposed amendment to Rule 41 that would have allowed warrants for searches and seizures of property located outside the United States. *See* Fed. R. Crim. Proc. 41, Notes of Advisory Committee on Rules—1990 Amendment. Not surprisingly, then, the U.S. government has not advanced the argument that Rule 41 authorizes a search warrant for e-mails (or other property) located outside the United States.

There is one narrow exception—Rule 41 authorizes warrants for searches conducted in United States territories, diplomatic missions, and residences owned by the U.S. and used by diplomatic personal outside the U.S. But this is not what Orin seems to be talking about, and it is not what the Microsoft case is about. Moreover, this exception shows that Congress knows how to make a warrant apply outside of the U.S. when it wants to, which just underscores that it did not do so for any other circumstances in Rule 41.

Thus, neither the SCA nor Rule 41 authorizes warrants for searches or seizures of e-mails (or anything else) outside of the United States. The presumption of extraterritoriality therefore comes into play, and Microsoft wins. Case closed.

A second, two-hundred-and-ten-year old doctrine holds that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains." *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804). The Supreme Court has repeatedly re-affirmed this principle, stating that U.S. laws should be interpreted "to avoid unreasonable interference with the sovereign authority of other nations." *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164 (2004). Orin doesn't discuss this *Charming Betsy* doctrine, but it provides another, independent reason that the SCA should not be construed as authorizing warrants for e-mails located abroad. For if it were construed in this manner, it could easily lead to conflicts with the laws of the nations where the e-mails are stored.

That is clearly the case here. For example, EU officials such as Viviane Reding, the Vice-President of the European Commission, have stated that if Microsoft disclosed the e-mails in Ireland, it would run afoul of the EU Data Protection Directive. It would also run counter to the Mutual Legal Assistance Treaty (MLAT) between the U.S. and Ireland, which presupposes that the U.S. will request assistance from the Irish government when it wants to get its hands on evidence located in Ireland.

So the case for Microsoft seems pretty clear. Orin goes on to argue that if Microsoft wins, the government could just turn around and use a subpoena to get the same data, which

might result in less privacy protection for e-mails than a probable-cause based warrant. There are two problems with this argument.

First, it strikes me as doubtful that the government would actually try to use a subpoena to obtain the *content* of e-mails located abroad. After all, the Justice Department has now given up using anything but warrants to get communications content in general, following the decisions of the Sixth Circuit (in *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010)) and other courts holding that the Fourth Amendment requires the government to use a warrant to get any communications content. The Attorney General and other Justice Department officials have also said the Department favors amending ECPA to require a warrant to obtain any communications content as part of a criminal investigation. Thus, even if the Fourth Amendment's warrant requirement doesn't apply to property located outside the U.S., it seems doubtful to me that the government would try to use a subpoena to obtain e-mail content because of the privacy ramifications (Fourth Amendment aside). Moreover, using a subpoena, based on a mere relevance standard, would only worsen the international uproar caused by the government's attempt to unilaterally obtain communications stored abroad. And it would be sure to generate intense opposition from U.S. communications and cloud service providers.

Second, it is not at all clear that the government could use a subpoena to obtain the content of e-mails that are in electronic storage for less than 180 days old. (The SCA allows certain other communications content to be obtained with a subpoena, but those are not at issue in this colloquy, so let's set them aside.) Orin asserts that if the court agrees that the SCA doesn't authorize an extraterritorial warrant, then the SCA's legal protections—in particular, the statutory requirement to use a warrant to get e-mail content—"necessarily…don't apply," either. I don't think that's right. Neither Rule 41 nor the SCA expressly authorizes warrants to be used to get data abroad, so the presumption against extraterritoriality and the *Charming Betsy* doctrine kick in. But Section 2702 of the SCA does expressly say that an electronic communications service provider may not knowingly divulge communications content except as authorized by Section 2703 (and a few other provisions), and Section 2703 requires the government to get a warrant. Section 2702 may not apply to communications providers located outside the United States. But it clearly does apply to providers inside the United States. So the SCA legally prohibits Microsoft from divulging any communications content to the government without a warrant.

Moreover, the cases in which the government has been able to get information stored abroad by serving a company in the United States all involve the business records of that company or an affiliate under that company's control. I'm not aware of any case in which a court has permitted the government to use a subpoena to a U.S. company to obtain property belonging to someone else or the content of another person's communications. Thus, as Microsoft suggests in its reply brief, the government might be able to use a subpoena to a U.S. bank to obtain the business records of the bank's subsidiary in Switzerland, but it could not use it to obtain the contents of a customer's safe deposit box there. It might be able to use a subpoena to a U.S. hotel company to get the records in France concerning one of the company's properties in Paris, but it could not use one to obtain the belongings of a hotel guest from his room in that Paris hotel. Similarly, the government might be able to use a subpoena to obtain an e-mail provider's own business records stored in Dublin (if those records are under the U.S. provider's

custody, possession, or control and the balancing test set out in the Restatement (Second) of Foreign Relations Law of the United States weighs in favor of the government). But I don't know of any authority that holds that a subpoena can be used to obtain the *content* of a subscriber's e-mails stored abroad.

Does this smack of the providers' wanting to have it both ways--that is, the SCA doesn't authorize warrants to obtain the content of e-mails abroad, but it forbids providers from disclosing e-mails in response to a subpoena, regardless of where the e-mails are located? It may seem that way. But all it really means is that Congress hasn't addressed the extraterritoriality issue in the SCA. This leads us back to the point Orin and I agree on: if Congress wants search warrants to apply to data stored abroad, despite the negative impact that would have on the business of American e-mail and cloud providers and on the United States' relationship with other countries, and despite the fact that the government can usually get the information it wants through assistance from foreign law enforcement, it needs to amend the statute to say so expressly. Balancing the negative effects on business and foreign relations against the needs of law enforcement is a quintessential policy decision that should be made by Congress, not by a prosecutor or judge in the Southern District of New York.