We Don't Hire The NSA or Federal Prosecutors To Make U.S. Internet Policy (And That's a Good Thing)

Christopher Sprigman

Over the past 15 months, and thanks to the documents leaked by Edward Snowden, we've learned some of the details of a heretofore secret and incredibly wide-ranging U.S. government effort to spy on hundreds of millions of ordinary people, in the U.S. and across the globe. The NSA's various surveillance programs suck up billions of digital communications – telephone calls, emails, texts, chats, social media postings – and search through this content for information pertaining broadly to the foreign relations and national security interests of the U.S. government.

What Happens When The NSA Makes Internet Policy

There has been a debate in the U.S. about whether the NSA's warrantless, suspicionless mass surveillance programs are lawful. But there has been, at least in the minds of the American government, no debate about the legality of spying on foreigners. The private communications of ordinary citizens outside the U.S. are considered fair game. Under U.S. law, companies with a presence in the U.S. that store data for foreigners can be compelled to disclose that information without probable cause, court review, or post-collection safeguards so long as the government has a "foreign intelligence" purpose for the collection.

Not surprisingly, a lot of non-Americans don't particularly like the U.S. government's cavalier approach to their privacy. And they are pushing back. One facet of the pushback is economic, and it involves U.S. technology companies.

The American government's hunger for easy access to emails, chats and other Internet data is driving Internet users around the world away from American Internet product and service providers. These are some of America's most successful companies. And they're worried. Foreigners comprise nearly 70% of the users of Google's email service, gmail. Nearly 85% of Facebook users reside outside the U.S. And increasingly, foreigners are wary of keeping their data with U.S.-based technology companies. "We're hearing from customers, especially global enterprise customers, that they care more than ever about where their content is stored and how it is used and secured," John E. Frank, deputy general counsel at Microsoft, told *The New York Times* earlier this year.

Those consequences have already started to hit home, in ways that hurt U.S. companies and destroy U.S. jobs. Back in January, American technology giant IBM said that it would be spending more than a billion dollars to build 15 new data centers overseas. Salesforce.com announced similar plans back in May. And, in conversations with foreign customers, U.S. computer giant Microsoft, in its marketing to business customers, emphasizes that they can choose to store data in Microsoft facilities located outside the U.S. The decision of IBM, Microsoft and other U.S.-based tech companies to try keep their foreign users' data at facilities located outside the U.S. is motivated in part by the desire to reduce latency – that is, improving the speed and responsiveness of the service provided to foreign users by storing

data closer to the customer. But the move is also prompted at least in part, by foreign customers' concerns that storing their data inside the U.S. enables U.S. spying.

Concern over U.S. mass spying has been picked up and amplified by foreign governments, who are eager to capitalize on the privacy concerns of their citizens, while improving their own surveillance capabilities and advancing the competitive interests of the EU-based technology companies that compete with their dominant American counterparts.

In June, the German government cancelled a network infrastructure contract with Verizon, citing fears that sourcing network infrastructure from a U.S. company would facilitate NSA spying on German citizens. Brazil and the European Union, which had used American undersea cables for intercontinental communication, recently decided to build their own cables between Brazil and Portugal, and project planners shunned American technology companies in favor of Brazilian and Spanish firms. Brazil also announced plans to abandon Microsoft Outlook for its own email system that uses Brazilian data centers. Telenor, Norway's largest telecom provider, halted its plans to move its customers to a U.S.-based cloud provider. The *Wall Street Journal* recently reported that AT&T's desired acquisition of the European company Vodafone is in danger due to the company's seemingly willing cooperation with the NSA's data-collection programs. And last year, leading Internet infrastructure provider Cisco Systems reported a 12 percent slump in its sales in the developing world that the company suggested was connected to the NSA revelations.

The overall damage to U.S. tech companies and the U.S. economy is very difficult to quantify. But a study by the Forrester Research firm found that U.S. technology firms could lose $180 billion in overseas sales – or about 25% of total U.S. foreign trade in the provision of Internet services -- by 2016.

In sum, what Jennifer Granick and I predicted [LINK: http://www.theatlantic.com/technology/archive/2013/06/us-government-surveillance-bad-for-silicon-valley-bad-for-democracy-around-the-world/277335/?single_page=true] in the immediate aftermath of the Snowden revelations has come true -- the National Security Agency and its massive electronic spying programs have done significant damage to one of the most vibrant parts of the U.S. economy.

What Happens When Federal Prosecutors Make Internet Policy

Which makes it all the more dismaying that Preet Bharara, the U.S. Attorney in Manhattan and a government official who has no particular authority to make Internet policy, is taking a litigation position that will make an already bad situation potentially much worse.

As part of a law enforcement investigation involving suspects and wrongdoing that have not yet been disclosed, Bharara and his New York federal prosecutors applied for and received a U.S. search warrant under a law called the Stored Communications Act (SCA). The warrant commanded Microsoft to produce emails from the account of one of its presumably foreign webmail users.

The problem was that the emails are stored on a server at a Microsoft datacenter in Dublin, Ireland. It has been black letter law for a very long time that search warrants issued by a U.S. court are enforceable only in the U.S.

If a U.S. prosecutor wants to seize evidence located abroad, there is a way to do that. The U.S. has entered into a large number of Mutual Legal Assistance Treaties, including one with Ireland. Under the U.S./Ireland MLAT, which was updated in 2008 to provide streamlined evidence-gathering procedures, the U.S. prosecutor can make a request to an Irish court to order evidence seized and turned over. Those requests are evaluated according to standards and processes to which both participating countries pledge to adhere.

But Preet Bharara says that the MLAT process isn't quick enough for him. So he's trying to bend U.S. law to enforce his search warrant abroad – and so far he has been successful. Last Thursday, District Judge Loretta Preska ruled that Bharara could use a SCA search warrant to compel Microsoft to turn over the documents located in Dublin. In other words, the court said that foreigners who store data with any U.S.-based company can have their data seized, *even if it is stored abroad.*

Preska's ruling is not the final word; Microsoft has vowed to appeal. But if the district judge's ruling stands, foreigners will have another reason to think long and hard about storing data with any company that has offices inside the U.S., because the fact that the data is kept outside the U.S. will no longer stop the U.S. government from getting ahold of it. However much you favor U.S. law enforcement getting whatever it wants, you must recognize that, thanks to NSA overreach and the U.S. government's explicitly stated policy of not giving a whit about the privacy interests of non-Americans, a lot of foreigners don't see it that way. Which means that U.S. Internet companies will be facing an even bigger threat to their businesses.

Nor will the mischief stop there. Microsoft over 100 data centers in 40 countries, and many U.S. tech companies have a similar global reach. If the U.S. government position were adopted by foreign governments – a process which has already begun in the UK, and, if upheld, will eventually happen in many more jurisdictions – potentially scores of countries could demand the disclosure of data on U.S. citizens stored in the U.S., based on legal standards weaker than our U.S. courts apply or even on an illiberal government's whim.

The Stored Communications Act

How did this happen? An explanation must start with the Stored Communications Act (SCA), which Congress enacted in 1986. The SCA states that the government may use a warrant "issued using the procedures described in the Federal Rules of Criminal Procedure … " to obtain email from an electronic communication service provider. Nothing in the SCA explicitly contravenes the longstanding rule that search warrants issued by a U.S. court are good only within U.S. territory. And nothing in the SCA even implies that warrants issued under its authority are subject to rules different from those that govern warrants generally.

Instead, the SCA explicitly adopts the provisions governing the scope of warrants laid out in Rule 41 of the Federal Rules of Criminal Procedure. Rule 41 does not provide U.S. courts

with any general authority to issue warrants to seize property located outside the U.S. In fact, it's clear that Rule 41 rejects such a general power. The only part of the rule that expressly *allows* extraterritorial execution of warrants for seizure of property – which is defined to include "information" – is limited to U.S. territories, possessions or commonwealths, and U.S. embassies and consular posts. The specific provision of authority to execute search warrants in these very particular and limited places outside the U.S. means that there is no *general* authority to enforce warrants extraterritorially.

The implication of this is not terribly surprising. A warrant to search for and seize property at the U.S. embassy in Dublin is ok – as far as the law is concerned, the U.S. embassy should be treated as U.S. territory. But every other square inch of Dublin is off-limits to U.S. warrants. Searches and seizures, to be legal under both U.S. and Irish law, must be done with the cooperation of the Irish government.

So how did the government manage to convince Judge Preska to uphold the warrant? By arguing that SCA search warrants are not really search warrants, but instead a "hybrid" of warrant and subpoena. A search warrant is a legal process allowing the government to execute a search and seizure. It does not require the cooperation of the targeted person or firm. A subpoena, in contrast, is legal process commanding a particular person or company to produce property, including information, in their possession.

The SCA also provides the government authority to use subpoenas to order the production of information. But Congress limited that authority in two ways that the prosecutors don't particularly like. The SCA generally does not permit the production of email less than 180 days old via subpoena – those "fresher" communications, which Congress hypothesized would generally raise greater privacy interests, may in most cases be searched and seized only via warrant, which, unlike a subpoena, require a showing of probable cause. And under the SCA prosecutors are typically required to give notice to persons whose emails are seized via subpoena. And recently, a Federal appeals court held that the seizure of emails (whether older than 180 days or not) without a warrant was unconstitutional. Which means that the SCA's subpoena process is under a very dark cloud.

The government's argument -- which Judge Preska bought – is that because the SCA warrant, like a subpoena, is served on an individual or firm and not executed by a police officer or other government official, it should be usable, like a subpoena, to require production of any record within the possession of a person or firm properly subject to the court's jurisdiction. As Microsoft has offices in the U.S. and is therefore subject to the court's jurisdiction, and can access the information stored in Ireland, the government argued that the territorial limits that apply in general to search warrants should not apply in the SCA context.

That argument is extraordinarily weak – not least because of another provision of the SCA, added in 2002, which makes clear that a law enforcement officer does not have to be present when an SCA warrant is executed, and yet the process is still identified as a "search warrant" and it is still being "executed."

If you think about it for a moment, the statute's purpose in deputizing the technology firm to execute an SCA warrant wasn't meant to distinguish between warrants and subpoenas or

to create a new "hybrid" category of subpoena-ish warrants. It is, rather, an entirely practical response to the difficulty of executing warrants in the context of highly complex and carefully secured computer networks.

Having a law enforcement officer, even a very highly trained one, search for and seize emails would in many instances simply be impractical. It would take a lot of time—if not be impossible-- for an officer to understand how to access and query the service provider's network without messing everything up. Until he did, he'd have no capacity to execute the warrant himself or even to competently supervise a search done by an employee of the technology firm that had been served with the warrant.

The SCA adapts the mode of executing warrants to a particular technological environment. That does not transform a warrant into a subpoena, or into some sort of "hybrid" of the two – that is a category heretofore unknown and better left that way.

In sum, the statute itself forecloses the government's "hybrid" argument. The statute calls a warrant by its name, and Congress legislated knowing precisely what a warrant is and what the territorial limitations were. Any adjustments that the statute makes to the warrant procedures are driven by practicality and have no bearing on the longstanding rules barring extraterritorial execution of warrants. And in the absence of any statutory provision explicitly providing (or even implying) otherwise, the SCA warrant is, like any other warrant, subject to the traditional territorial constraints.

There is another government argument that's worth taking a moment to consider. The government asserts that even if SCA search warrants cannot be executed outside U.S. territory, it can still get Microsoft documents located in Dublin. That's because, according to the government, the actual search and seizure takes place in the U.S., when a U.S.-based Microsoft employee queries the Dublin database, prints out or saves to a hard drive documents retrieved from that database, and hands them to the government.

Yet is it well-established that searches occur where the content is stored. Indeed, the government has relied on this exact reasoning in other cases where it's argued (successfully) that FBI agents searching content stored on a computer located overseas are not engaging in a search conducted in the U.S., which would require a warrant.

What about the seizure of the emails? That too is regulated by the warrant – so does the government have a decent argument that the seizure of emails on a Dublin server takes place when a Microsoft employee delivers those emails to a government agent in Redmond? When the search turns up relevant emails, copies of those emails are then made on the Dublin server at the government's command. The Federal Court of Appeals in New York, which will hear the government's arguments in this case, has previously held that copying electronic files constitutes a seizure, even before an agent receives the data or is able to search through it.

It's always possible that the appeals court could reverse course by distinguishing the Microsoft search on its facts. But it seems likely that at very least the seizure of the Dublin emails would take place in Dublin. Which means that if the government wants to get emails

from Microsoft's Dublin facility, they most likely will be obliged to ring up their Irish counterparts and start talking.

The Deeper Issues for U.S. Internet Policy

Whatever the appeals court does, there are deeper policy issues presented by the Microsoft case that Congress and the Administration should address. If warrants issued by U.S. courts do not have extraterritorial effect and a similar rule is applied by foreign governments respecting data stored in U.S. facilities, then governments may increasingly require providers (including those based in the U.S.) to store data locally to ensure that local law enforcement will have access.

From a U.S. perspective, that would not be a good result either. U.S. firms enjoy dominant positions in the provision of many sorts of Internet services, and an outsized proportion of Internet infrastructure is located in the U.S. America's future prosperity would be best served by us keeping things that way.

The answer, to avoid both the misuse of SCA authority in the Microsoft case and the misguided "data sovereignty" reaction to territorial limits on warrants, would be for the U.S. government to work with its foreign counterparts to strengthen and streamline MLAT procedures. Indeed, that is already the stated policy of the U.S. government. In a speech on surveillance policy back in January, 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 this directive, the DOJ is leading an effort to update and improve the MLAT process, and to 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 U.S. evidentiary standards, a predicate for quick fulfillment of MLAT requests.

Improving the MLAT process will take time, money, and effort. But it's the right way to achieve our legitimate law enforcement goals. Bending existing law, creating a new "hybrid" species of search warrant, and causing further damage to U.S. Internet companies that are already under threat, is not.