The New York Times
NYTIMES.COM
"All the News That's Fit to Print" Monday, February 26, 2018 Reprinted With Permission

Opinion

Can the United States Search Data Overseas?

By CRAIG A. NEWMAN

Should the United States government be able to conduct a search of your emails if they are stored on a server in another country, or does the government's right to examine digital evidence stop at the border?

That is a central question in United States v. Microsoft, a case scheduled to be argued on Tuesday before the Supreme Court.

Both sides in the case have legitimate concerns. If the court sides with Microsoft and declines to allow searches for data stored in another country, the government will be hampered in investigating crimes like terrorism, child pornography and fraud.

If the court sides with the government and rules that it may demand data stored overseas by American companies, those companies will find it much harder to do business abroad. This is because many foreigners fear that United States warrants authorizing such searches will disregard privacy protections afforded by their country. The government of Germany, a country with stringent privacy laws, has already indicated it will not use any American company for its data services if the court decides to allow searches.

For the United States technology industry, the stakes are high. Last year, the worldwide public cloud services market was estimated to be a $246.8 billion business. Most of the leading companies in this sector are American: Amazon, Microsoft, Google, Oracle, IBM. If other countries were to follow Germany's lead, the economic consequences could be severe.

While a clarifying decision is needed in this particular case, nothing that the Supreme Court rules will solve the fundamental problem: The Stored Communications Act, a 1986 law that governs the storage and disclosure of electronic communications by third parties, is outdated. Congress needs to act to ensure that technology companies can flourish overseas while law enforcement has the right tools to gather evidence worldwide.

The Supreme Court case goes back to 2013, when federal agents served a warrant on Microsoft, seeking email communications belonging to a drug trafficking suspect. Microsoft handed over the suspect's account information and address book, which sat on its servers in the United States, but refused to turn over any email content, which was stored at a data center in Ireland.

Microsoft argued that the email content was outside the reach of United States law enforcement. The government countered that because Microsoft could retrieve the data in Ireland with a click of a mouse, without leaving its headquarters in Redmond, Wash., the email content was within its reach.

Two lower courts agreed with the government. But in July 2016, the United States Court of Appeals for the Second Circuit in New York reversed the lower courts and determined that the information stored in Ireland was beyond the reach of a United States warrant.

At the center of this case is the Stored Communications Act, which was written when there was no modern global internet or cloud storage. It provides Fourth Amendment safeguards to prevent unreasonable searches of electronically stored communications — but says nothing about data held abroad.

The Court of Appeals concluded that the Stored Communications Act was not intended by Congress to allow searches outside the country. The ruling followed the well-established principle that American courts generally do not apply United States law beyond its borders unless Congress intended so.

But at least four federal courts have since refused to follow the ruling, mostly for practical, technology-driven reasons. The cases before those courts involved Google and Yahoo, which store data "dynamically" — breaking data into many small pieces and constantly shuttling it among storage centers in various countries to optimize performance and network efficiency. The text of an email might reside in Bulgaria, but the attachment in Spain.

Does it make any sense to think of this email as located in a specific country overseas? As a United States District Court judge, Juan R. Sánchez, wrote in an opinion that rejected the Second Circuit's ruling, "no one knows which country to ask" for the data.

Because Microsoft still frequently uses local-based storage, the Supreme Court case, though important, is of limited significance. The court has an opportunity to clarify the scope of the Stored Communications Act with respect to data stored "statically" outside the United States. (When signing up for service, a Microsoft user indicates his or her country of residence and Microsoft usually stores the user's data in a nearby data center.) But the case does not address the more general question of the legal standards that govern information that crosses borders — and in particular, data stored "dynamically."

Only Congress can address that larger question, by writing an urgently needed new law. (Even the Second Circuit appealed to Congress to step in.) The International Communications Privacy Act, introduced last term in Congress, is a good place to start. It provides a framework by which United States law enforcement can obtain communications of both United States and foreign citizens, consistent with the privacy protections afforded by international law.

The guiding principle should be that the reach of any new law is defined by the citizenship and geographical location of the individual whose data the government seeks, rather the physical location of the data. This would allow for the right balance between global privacy rights and the needs of United States law enforcement.

No matter how the Microsoft case is decided, if Congress fails to act, we will continue to have a legal system that inadequately governs the vast stores of electronic data that move seamlessly across international borders.