OP-ED CONTRIBUTOR

There’s No Good Decision in the Next Big Data Privacy Case

People in line outside the Supreme Court last week. Drew Angerer/Getty Images

By Jennifer Daskal Oct. 18, 2017

In 2013, United States agents served a warrant on Microsoft seeking the emails of a suspect in a drug case. Microsoft balked at the request, saying that the data was stored on a server in Ireland and out of the reach of United States law enforcement. To access the data, the United States would need to make a request to the Irish government through diplomatic channels — a slow and burdensome process. The government fought back, arguing that the Washington State-based company could access the emails from the United States, without ever stepping foot in Ireland, and was required to comply.

Monday, the Supreme Court agreed to hear the case this term. (https://www.nytimes.com/2017/10/16/business/justices-technology-data.html) Its decision — which will come after two lower courts sided with the government and the Second Circuit reversed — will determine the extent to which United
States law enforcement can access data held abroad. Microsoft will argue that the data is outside domestic law enforcement’s direct reach. The government will make the case that its warrant authority covers data held anywhere, so long as it can be accessed by a company operating from within the United States.

Both of these positions have troubling implications. What is needed is a solution that falls between these two extremes. Because the courts can’t provide this, Congress needs to step in.

At issue in the case is the interpretation of a 30-year old statute, the Stored Communications Act. The Act was written before there even was a global internet, let alone anything that resembles the cloud. The statute governs when and how law enforcement can demand an internet service provider turn over data needed for a criminal investigation. But it is silent on the key issue presented by the case – whether and when United States warrants can reach data held outside the United States.

If the Supreme Court backs Microsoft, law enforcement access to data will be limited based on the arbitrary fact of where the data happens to be stored. Prosecutors will have to use diplomatic channels to seek enforcement of their warrants overseas.

This would require the data to be held in a relatively fixed location, and in a location known to the United States. It would put United States law enforcement investigations under the control of foreign governments, some of which have no interest in or capacity to cooperate with the United States. And it would preclude the United States from directly accessing the data of an American resident, even in the investigation of a local crime, and even if it has obtained a warrant, based simply on where the data is held.

Domestic law enforcement agencies are wrongly concerned. The ruling provides a blueprint for malicious actors to evade the reach of American law enforcement. It also incentivizes costly data localization mandates, pursuant to which companies are required to store data locally as a means of ensuring law enforcement access. This would undermine the growth potential of the internet and potentially price small start-ups out of the international market.

But a government win would have its own costs. It would broadcast to the world that United States law enforcement can access data held by a domestically based company anywhere. This could be deeply damaging to American tech companies already reeling from the economic fallout of the Snowden revelations — lost
revenue from foreign customers concerned about the scope of U.S. foreign intelligence. Rightly or wrongly, foreigners are wary about what they see as the broad reach of the American surveillance state. The unconstrained ability of domestic law enforcement to access data stored overseas threatens to push a potentially lucrative foreign customer base further away from United States-based providers, as the number of tech companies that have rallied to Microsoft’s defense highlights.

More critically, it would set a dangerous precedent, allowing governments to reach data across borders without regard to the sovereign interests of other states. It would make it that much harder for the United States to protect our own citizens and residents from the reach of foreign law enforcement asserting the same authority. It would, as a result, threaten privacy on a global scale.

There’s a middle ground. The two Second Circuit court judges who have urged Congress to step in to find a solution are right. Legislation already pending in Congress (https://www.congress.gov/bill/115th-congress/senate-bill/1671/text) is a good place to start. It would permit the United States to access, pursuant to a warrant, data needed for the investigation of criminal activity, regardless of where that data happens to be. But it also would require courts to take a second look if the data belongs to a foreign national outside the United States, when certain conditions are met. This takes into account foreign governments’ interests in protecting their own citizens’ and residents’ data. And it shifts the focus away from the location of data to the location and nationality of the target.

Such a shift makes sense. People have connections to the place that they live, not where their data happens to be stored. Such a system preserves democratic accountability. It focuses on a government’s sovereign interest over its people — as opposed to the 0s and 1s that flow through a digital platform in its territory.

Notably, even Microsoft has urged (https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/) this kind of legislative response. In asking the Supreme Court to leave the Second Circuit ruling intact, it focused on the need to give Congress room to act. Congress should heed this call.

How we resolve this issue will shape privacy, security, the economy and the very future of the internet for years to come. The Supreme Court’s decision to take the case is a clarion call for Congressional action.
Jennifer Daskal is an associate professor at American University Washington College of Law and was formerly counsel to the assistant attorney general for national security at the Department of Justice.


Sign up for the Opinion Today newsletter
Every weekday, get thought-provoking commentary from Op-Ed columnists, The Times editorial board and contributing writers from around the world.

SEE SAMPLE (HTTPS://WWW.NYTIMES.COM/NEWSLETTERS/SAMPLE/OPINION-TODAY)