The New York Times | http://nyti.ms/1IvRKM7

The Opinion Pages | OP-ED CONTRIBUTOR

Dark Clouds Over the Internet

By ANDREW KEANE WOODS NOV. 30, 2015

LEXINGTON, Ky. — The Internet is routinely described as borderless, and that is often how it feels. Tweet a photo or post a comment, and it is instantly viewable in nearly every country in the world. But a global Internet unbounded by territorial limits is pure fantasy.

Down where the cables lie and the servers spin, territory still matters.

Take user data. While 90 percent of the Internet's users are outside the United States, the web is dominated by American firms. As a result, a great deal of non-American data is held on American servers. This was tolerable when trust in the United States was high. But after Edward J. Snowden peeled back the curtain on the National Security Agency's Internet surveillance efforts, that trust withered.

In response, other nations are increasingly exercising their territorial control over the Internet, often in ways that mimic America's worst practices.

Earlier this month, the British Home Secretary introduced a bill known as the Snoopers' Charter that would broadly expand the government's ability to collect user data — from authorizing the police to hack into phones and computers, to mandating that Internet companies decrypt encrypted communications. The bill goes too far and privacy advocates are right to oppose it.

But governments do have legitimate reasons to seek user data beyond their territorial reach, and privacy advocates ignore that need at their peril.

Ask a police officer anywhere outside of the United States and he'll tell you that evidence for routine crimes — murder, theft, burglary — is very often stored in the cloud, typically in another jurisdiction. Last year alone, British law enforcement agents made nearly 54,000 requests for data from just five American firms: Facebook, Google, Microsoft, Twitter and Yahoo.

These requests often go nowhere because America's 1986 Electronic Communications Privacy Act only allows technology firms to release American-held data in response to orders from an American judge. So if a British cop is investigating a murder in London, and he has good reason to believe that Google or Facebook has evidence about the crime, he must satisfy an American judge using an American constitutional standard to obtain the evidence. This cross-border process is notoriously slow. Requests take an average of 10 months — an eon in a criminal investigation — and many languish for years.

Exasperation with this process was a key motivation behind the Snoopers' Charter, and Britain is hardly alone.

Because American law has made it nearly impossible to obtain digital evidence through legitimate channels, foreign police are turning to illegitimate ones. I recently attended a conference for purveyors of surveillance software — an event unofficially known as the "Wiretappers' Ball." I asked one vendor if he was aware of law enforcement's frustrations with American tech firms. The salesman grinned and told me that police departments now buy his malware precisely because they're tired of waiting for evidence through established diplomatic channels. This is alarming: Making it harder for the police to get criminal evidence lawfully may actually incentivize them to seek that data by snooping.

To surveil the Internet, it helps to have control over the physical nodes in the network. Indeed, wherever our data passes through cables or servers that are bolted to a particular country's territory, it is vulnerable to that government's control. Just last week, The Times revealed that the American military is concerned about Russian ships "aggressively" conducting military exercises near undersea fiber cables, an irony that wasn't lost on those aware of the N.S.A.'s own efforts at tapping the Internet backbone.

Territorial control over the Internet matters so much that when countries don't have access to any physical infrastructure within their borders, they often

mandate it by fiat. A number of nations have passed data localization bills, which require foreign Internet companies to store some of their users' data on local servers. Politically, this plays very well — "Keep Brazilian data out of the N.S.A.'s hands!" — but it doesn't necessarily keep users' data safe.

The threat of data localization was initially considered mere saber rattling, but no more. Last month, the European Court of Justice invalidated a 15-year-old Safe Harbor framework that enabled American technology firms to move data between Europe and America to optimize their services. Without such a framework, radical restructuring of many companies' networks may be required. Indeed, within weeks of the court's decision, Microsoft announced that much of its European customer data will be held in Germany by Deutsche Telekom. This is good news for the N.S.A. and German intelligence agencies — and a subsidy for the German cloud storage industry — but it is bad for user privacy and a dangerous precedent for the future of the cloud.

If the global Internet is going to be warped to suit governments' interests, we must ensure that it isn't broken up into cantonized national networks with less privacy, less efficiency, less commerce and less speech. That means making it easier for foreign governments to get data when that access is justified and harder when it is not.

International agreements are one solution, and America and Britain are rumored to be negotiating such a deal. In the meantime, American technology companies should be free to comply directly with foreign government requests for data, as long as that access is warranted and meets international standards of due process and human rights. If America fails to allow such access, it will happen anyway in a brute and extralegal manner — and the result will be a less secure, less efficient Internet.

Andrew Keane Woods is an assistant professor of law at the University of Kentucky.

A version of this op-ed appears in print on December 1, 2015, on page A27 of the New York edition with the headline: For Digital Privacy, Borders Still Matter.