HTTPS://WWW.LAWFAREBLOG.COM/CLOUD-ACT-WELCOME-LEGISLATIVE-FIX-CROSS-BORDER-DATA-PROBLEMS

LAWFARE

(NOTE -- SIGNED INTO LAW FRIDAY MARCH 23, 2018) PART OF BUDGET LEGISLATION KEEPING GOVT OPEN.)

CROSS-BORDER DATA

The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems

By **Andrew Keane Woods**, **Peter Swire**
Tuesday, February 6, 2018, 5:49 PM

***Lawfare* readers are familiar with the perennial regulatory challenge of determining which country's law enforcement agents ought to be able to access internet data stored in the cloud. This is a considerable problem in two distinct contexts: (1) American law enforcement officers seeking access to data held abroad and (2) law enforcement officers around the world seeking access to data held by American firms. The Stored Communications Act (SCA) is problematic in both cases, because it does not specify whether it allows the American government to compel U.S. providers to produce content they have chosen to store abroad (the first problem), and it has been interpreted to prohibit American firms from complying with foreign government requests for user content (the second problem). The first issue has percolated through the U.S. courts for the last few years, and the Supreme Court is scheduled to hear oral argument in *United States v. Microsoft*, or the "Microsoft-Ireland" case, on Feb. 27. In that case, the court must decide whether a warrant issued under the SCA can compel Microsoft to produce emails that it stores in an Irish data center.**

On Tuesday, Sens. Orrin Hatch, Christopher Coons, Lindsey Graham and Sheldon Whitehouse announced a bill that could address both problems at once and even moot the Microsoft-Ireland case. If passed into law, the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 would accomplish two things: It would specify that an order under the SCA applies to all data that is in the "possession, custody, or control" of the provider, regardless of where that data is stored, and it would pave the way for executive agreements—such as the contemplated U.S.-U.K. agreement—to allow foreign governments to request content directly from American providers.

The Microsoft-Ireland Fix: U.S. Law Enforcement Access to Data Stored Abroad

The bill proposes amending the SCA by adding a section, 18 U.S.C. §2713:

> **A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to *preserve, backup, or disclose the contents of a wire or electronic communication* and any record or other information pertaining**

to a customer or subscriber within such provider's *possession, custody, or control,* regardless of whether such communication, record, or other information is located within or outside of the United States.' (Emphasis added.)

This provision reflects the Justice Department's position in the Microsoft Ireland case and would, if adopted, likely make that case moot. In other words, it codifies the so-called "Bank of Nova Scotia standard"—the standard, developed in *United States v. Bank of Nova Scotia* and a related line of cases, that allows for subpoenas to compel a bank to bring foreign-held records into the U.S. as long as those records are in the "possession, custody or control" of the bank. This will likely be decried as an exercise of extraterritorial jurisdiction, but it is entirely consistent with longstanding notions of state authority to legislate in areas that have domestic effects, or notions of jurisdiction that are grounded in both domestic and international law.

Moreover, a number of safeguards are built into the bill. The bill creates a mechanism whereby providers can apply for a motion to quash or modify legal process if the provider reasonably believes the subscriber is not a U.S. person and that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. It also requires a court to conduct a comity analysis in the event of such a motion to quash, which may alleviate foreign government concerns about sovereign interests. It is not clear why this comity provision is in the statute except as a symbolic gesture; courts were already free under the common law to conduct a comity analysis in thinking through whether to issue an order with extraterritorial impact. Its presence in the statute is perhaps a reminder that trust and mutual respect play an important role in these cross-border matters.

The idea is that if a provider is in the U.S., it should comply with the SCA, regardless of whether it chooses to offshore its data. The bill also provides a precedent for the reverse to be true: If an American provider is in a foreign market, in many instances (subject to comity principles) the provider ought to comply with local law, and law enforcement in that market ought to be able to compel the provider to respond to lawful requests.

Foreign Law Enforcement Requests to U.S. Providers (The U.S.-U.K. Agreement)

The other and perhaps more significant piece of the bill is that for certain nations the bill removes a number of blocking features—those provisions of American law that prevent American providers from complying with lawful foreign law enforcement requests, which are the sources of enormous frustration for American providers and foreign law enforcement alike. The bill amends multiple parts of the Electronic Communications Privacy Act (ECPA) related to stored records, wiretaps, and pen/trap access, to allow providers to permit disclosures to certain foreign governments—but only those that have struck executive agreements with the U.S. of the sort contemplated between the U.S. and U.K.

Those agreements are not available to every country—only to those that meet a stringent set of requirements. The president can strike such an agreement with a country only "if the Attorney General, with the concurrence of the Secretary of State," determines that:

(1) The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" (to be determined by reference to a laundry list of human rights and rule of law standards);

(2) The foreign government has adopted minimization procedures regarding information concerning US persons; and

(3) The agreement has protections to prevent the foreign government from targeting or collecting information about US persons or persons located in the US, and to prevent the US government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.

Foreign government orders issued under the agreement must relate only to serious crimes, including terrorism, and must meet a number of requirements. Orders must provide a "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;" they must be "subject to review or oversight by a court, judge, magistrate or other independent authority;" they cannot be used "to infringe freedom of speech;" and more.

This approach—with a stringent set of requirements—provides a way to address the globalization of criminal evidence that is similar to how nations addressed the globalization of travel in the 1980s. At that time, the U.S. created the "visa waiver program" so that countries with stringent standards would permit citizens of the other countries to enter without the need for a visa interview. Now that evidence for criminal cases so often is housed in other countries, this "ECPA waiver program" would allow streamlined access to criminal data for the countries that meet the strict standards.

A Very Good Start

This bill does not resolve the cross-border data problem, but it is good start. Privacy and human rights groups will argue that the bill offers insufficient protections for foreign-held data. If you compare the due process protections in this bill with those provided under the Fourth Amendment, it is likely less privacy-protective—meaning that foreign governments will get access to more information than they do currently. But that is not the right comparison. We are heading towards a world in which a growing number of foreign governments force providers to store data locally in order to comply with local orders, regardless of whatever strictures apply under U.S. law. As compared to that world, this bill—which might forestall or prevent localization efforts—offers privacy advocates quite a lot.

Perhaps a bigger concern is what happens if the bill passes and the president uses it to negotiate an agreement with the U.K. but no one else. This would leave some of the world's biggest markets, such as India and Brazil, in the cold and would incentivize them to mandate localization. That is a problem inherent to any attempt to address this issue bilaterally rather than by simply amending SCA to not apply to U.S. providers abroad (as Woods argued in

his testimony before the House Judiciary Committee last year). One promising way to expand the "club" of countries that qualify could be to permit the executive agreements to apply to specific offices or agencies of a nation, rather than any criminal request from that nation. Swire and Deven Desai have suggested that approach for India, where requests from an office such as a specialized cybercrime bureau might qualify for the streamlined approach.

The challenges of the globalization of criminal evidence will not be solved by any one bill. Still, for a problem that has seen too little movement for too long, this represents a very compelling start.