OTI TO CONGRESS: VOTE NO ON OMNIBUS BILL H.R. 1625 UNLESS CLOUD ACT IS REMOVED

The Clarifying Lawful Use of Overseas Data Act (CLOUD Act, S. 2383, H.R. 4943) was attached to the omnibus spending bill (H.R. 1625) that is expected to be voted on today or tomorrow. The CLOUD Act would enable the U.S. government to obtain communications data regardless of whether it is held inside or outside of the United States. It would also create an exception to the Stored Communications Act to allow qualifying foreign governments to enter into an executive agreement to bypass the human rights protective Mutual Legal Assistance Treaty (MLAT) process when seeking data in criminal investigations and to seek data directly from U.S. technology companies. To qualify, foreign governments would need to be certified by the Attorney General (AG), in concurrence with the Secretary of State, as meeting certain human rights standards set forth in the bill.

New America's Open Technology Institute (OTI) opposes the CLOUD Act because even with changes to the bill as attached to the omnibus, it fails to ensure that privacy and human rights will be adequately protected. Thus, Members should oppose the omnibus unless the CLOUD Act is removed.

The version of the CLOUD Act that was attached to the omnibus included some improvements upon the bill as introduced, such as:

- **Making the Human Rights Factors Mandatory:** The AG and Secretary of State would now be required to determine that a foreign government has met each element of the human rights test before it can certify a country to enter into an executive agreement, whereas they were previously merely discretionary;
- **Increasing Accountability Around AG Certification Assessment:** The bill would now require the AG to issue a report to Congress that explains her or his justifications for the determination that a country qualifies for certification; and
- **Requiring the AG and Congress to Recertify Countries if an Agreement Changes:** If an executive agreement changes during the 5-year renewal period, it would now be required to go through the certification and congressional review process again.

However, other changes to the bill represent partial or ineffective fixes to substantial problems, including:

- **Not Requiring Prior Judicial Review of Foreign Government's Surveillance Orders:** The CLOUD Act fails to require that a foreign government's independent judicial or oversight body review each surveillance order *before* it is issued to a U.S. company. The bill includes new language requiring that oversight of orders must be "prior to, or in proceedings regarding,

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America's Open Technology Institute, at greene@opentechinstitute.org.

enforcement of the order," but that could still allow for review that is contemporaneous with or after the execution of the order, rather than before it; and

- **Failing to Stop Encryption Backdoor and Data Localization Mandates:** The CLOUD Act now prohibits executive agreements from being used to create an obligation to decrypt data, which is an improvement. However, it does not prevent foreign countries from attempting to demand -- outside of this new process -- that U.S. companies create encryption backdoors, and it does nothing to prohibit foreign governments that are party to these agreements from imposing data localization mandates on U.S. companies.

Finally, many core concerns that privacy and human rights groups raised were entirely unaddressed. The CLOUD Act:

- **Permits Real Time Intercepts (Wiretaps) Without Including Safeguards That Apply to U.S. Wiretaps:** It would allow foreign governments to ask U.S. companies for real-time intercepts of their users communications at standards that are lower than what would be required of the U.S. government under the Wiretap Act.;
- **Fails to Define Scope of Crimes:** It would allow for surveillance orders to be issued under the MLAT bypass process for “serious crimes, including the crime of terrorism” but it does not define or limit “serious crimes;”
- **Does Not Provide Congress with Meaningful Oversight Authority:** It would not require Congress to approve executive agreements. Instead Congress could only stop an agreement from going into effect by passing a Joint Resolution of Disapproval. This would require the president’s signature, so Congress would have to pass it with a veto proof majority; and
- **Fails to Adequately Protect Americans’ Data:** If Americans’ data are incidentally collected by a foreign government, that government would only have to minimize those data to the extent required by FISA;
- **Potentially Creates a New Backdoor Search Loophole:** It would allow foreign governments to share back Americans’ incidentally collected data. Those data may have been collected under a standard that falls short of probable cause, and there are few limits on how the U.S. government may use those data when they are back in its possession; and
- **Does Not Close ECPA’s 180 Days Loophole:** The bill fails to include an update to the Stored Communications Act to require the government to obtain a probable cause warrant before demanding the contents of communications that are over 180 days old, as similar bills like the LEADS Act and ICPA did.

The CLOUD Act represents a sea change in privacy law that protects the data U.S. companies hold on Americans and people abroad. It has had not been marked up in congressional committees, there have been no opportunities for votes on amendments, and there has been no debate on the House or Senate floor. Attaching it to the must-pass omnibus bill in order to circumvent this important process and force it into law, especially where so many critical problems remain unaddressed or inadequately addressed, is not only undemocratic, it threatens privacy and human rights.

Congress should VOTE NO on the omnibus unless this bill is removed.

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America’s Open Technology Institute, at greene@opentechinstitute.org.