The US Government Just Destroyed Our Privacy While Nobody Was Paying Attention

By Carey Wedler | The Anti-Media

(ANTIMEDIA) — While the nation remained fixated on gun control and Facebook's violative practices last week, the U.S. government quietly codified the CLOUD Act, its own intrusive policies on citizens' data.

While the massive, $1.2 trillion omnibus spending bill passed Friday received widespread media attention, the CLOUD Act — which lawmakers snuck into the end of the 2,300-page bill — was hardly addressed.

The Clarifying Lawful Overseas Use of Data Act (CLOUD) *"updates the rules for criminal investigators who want to see emails, documents and other communications stored on the internet," CNET* reported. *"Now law enforcement won't be*

blocked from accessing someone's Outlook account, for example, just because Microsoft happens to store the user's email on servers in Ireland."

The CLOUD Act will also allow the U.S. to enter into agreements that allow the transfer of private data from domestic servers to investigators in other countries on a case-by-case basis, further globalizing the ever-encroaching surveillance state. The Electronic Frontier Foundation, which has strongly opposed the legislation, listed several consequences of the bill, which it called "far-reaching" and "privacy-upending":

- *Enable foreign police to collect and wiretap people's communications from U.S. companies, without obtaining a U.S. warrant.*
- *Allow foreign nations to demand personal data stored in the United States, without prior review by a judge.*
- *Allow the U.S. president to enter "executive agreements" that empower police in foreign nations that have weaker privacy laws than the United States to seize data in the United States while ignoring U.S. privacy laws.*
- *Allow foreign police to collect someone's data without notifying them about it.*
- *Empower U.S. police to grab any data, regardless if it's a U.S. person's or not, no matter where it is stored.*

The bill is an update to the current MLAT (Mutual Legal Assistance Treaty), the current framework for sharing internet user data between countries, which both legislators and tech companies have criticized as inefficient.

Some tech companies, like Microsoft, have endorsed the new CLOUD policy. Brad Smith, the company's president and chief legal officer, called it *"a strong statute and a good compromise,"* that *"gives tech companies like Microsoft the*

ability to stand up for the privacy rights of our customers around the world."

They echoed the sentiment of lawmakers like Orrin Hatch (R-UT). In February, he said of the bill:

"The CLOUD Act bridges the divide that sometimes exists between law enforcement and the tech sector by giving law enforcement the tools it needs to access data throughout the world while at the same time creating a commonsense framework to encourage international cooperation to resolve conflicts of law."

But one of the biggest complaints from privacy advocates, however, it that the new legislation places too much-unmitigated power in the hands of governments with abysmal human rights records while also giving too much discretion to the U.S. government's executive branch. Noting that the executive branch will decide which countries are human rights compliant and that those countries will then be able to engage in data collection and wiretaps without any further restrictions or oversight, the ACLU warned:

"Flip through Amnesty International or Human Rights Watch's recent annual reports, and you can find a dizzying array of countries that have ratified major human rights treaties and reflect those obligations in their domestic laws but, in fact, have arrested, tortured and killed people in retaliation for their activism or due to their identity."

The organization pointed out that no human rights organizations have endorsed the CLOUD Act, adding that *"in the case of countries certified by the executive branch, the CLOUD Act would not require the U.S. government to scrutinize data requests by the foreign governments — indeed, the bill would not even require notifying the U.S. government or a user regarding a request."*

Further, the ACLU says, if a foreign government's human rights

record deteriorates, there is no mechanism to revoke its access to data. Considering the U.S.' existing record on supporting regimes that severely restrict basic rights like freedom of expression, the expanded access the CLOUD Act provides is undoubtedly worrisome.

Also predictable is the government's stale justification for expanding its power. As the CLOUD Act claims, it is purportedly to *"protect public safety and combat serious crime, including terrorism"* – even if it further empowers governments that support and commit said terrorism.

In an age where the government already engages in mass surveillance and is eager to disable the people's efforts to protect their privacy through encryption technology, it is unsurprising, albeit dangerous, that Congress continues to encroach on what little is left of safeguards against unwarranted intrusions.