Skydiving Without a Parachute

A Close Look at the CLOUD Act Shows It Lacks Essential Protections

FEBRUARY 22, 2018

Robyn Greene
Policy Counsel and Government Affairs Lead, New America's Open Technology Institute

The Clarifying Lawful Use of Overseas Data Act (CLOUD Act, S. 2383, H.R. 4943) was recently introduced in the Senate and the House of Representatives. This bill is intended to accomplish two goals: First, it would change the law to enable the U.S. government to compel U.S. providers to hand over users' data even if those data are held outside the United States. The Supreme Court is currently considering the validity of extraterritorial warrants in the Microsoft Ireland case, where Microsoft is challenging a warrant issued by a U.S. court under the Stored Communications Act (SCA) for data that is stored in Ireland. The CLOUD Act would resolve this question in favor of the government, but in so doing, would raise certain concerns that we explain in a separate analysis.

Second, the CLOUD Act would allow qualifying foreign governments to bypass the 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 standards set forth in the bill. It would do this by creating an exception in the Electronic Communications Privacy Act (ECPA) to allow companies to voluntarily respond to those certified foreign governments' requests for stored and real-time data (Sec. 4(1)(A)"(J)"). This bill would enable the United States to implement the agreement negotiated two years ago between the U.S. and United Kingdom to allow British law enforcement and intelligence agencies to make direct requests of American internet companies for this information, and other countries are expected to seek similar bilateral agreements.

The MLAT process has not kept up with the pace of growth of the internet. As a result, it has become time-consuming and cumbersome as the sole means for foreign governments to obtain data held by U.S. companies that is needed for their domestic investigations. However, although it is important to find a solution to the cross-border problem, it is critical that any such solution includes robust safeguards for the rights of consumers. The CLOUD Act does not meet this test.

In September, 2017, New America's Open Technology Institute (OTI) joined a coalition of 21 groups in opposition to this proposal before it was introduced because it fails to provide adequate civil liberties and human rights protections which are necessary to make such a bypass workable. As we describe in more detail below, we continue to oppose this MLAT bypass process, now incorporated into the CLOUD Act, because it would:

- Permit foreign governments to conduct real-time surveillance (wiretaps) of U.S. technology companies' users, with the consent of those companies, for the first time without adding safeguards comparable to those in the Wiretap Act;
- Permit foreign governments to obtain communications contents without prior judicial authorization and under a weaker standard than the probable cause standard that is currently required under MLATs, and to obtain metadata without any evidentiary showing. The CLOUD Act would also permit foreign governments to make data requests for a broad and ill-defined set of crimes;
- Provide inadequate protections for Americans' privacy if their communications are incidentally collected. The CLOUD Act would allow some contents and all metadata to be shared back to the U.S. government without any U.S. legal process or judicial oversight, and without imposing any use limitations on the U.S. government. Unless the CLOUD Act were amended to require foreign governments to provide prior judicial authorization under a more robust standard of review, this creates the potential for a new backdoor through which the government could warrantlessly access and use Americans' communications. It would also allow some Americans' communications data to be shared with third party foreign governments;
- Fail to establish clear and strict standards to ensure that countries seeking to qualify for this MLAT bypass option have a strong record of protecting human rights. The CLOUD Act would also provide the Executive Branch with too much discretion when determining whether countries meet those insufficient standards; and
- Fail to prevent certified countries from establishing encryption backdoor or data localization mandates.

As introduced, the CLOUD Act would threaten the privacy of Americans and internet users.

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

PROBLEM #1: The CLOUD Act would, for the first time, permit foreign governments to conduct real-time surveillance of U.S. technology companies' users, without imposing safeguards comparable to those in the Wiretap Act.

The Electronic Communications Privacy Act (ECPA) makes it illegal for electronic communications or remote computing service providers to intercept or disclose the contents of their users' communications except pursuant to a warrant (18 USC 2511).[1] When a foreign government seeks information held by a U.S. service provider, the government must obtain a warrant by working with the Department of Justice and the Department of State through the MLAT process. However, foreign governments may only obtain stored contents of electronic communications(18 USC 3512 (a)(2)).[2]

The CLOUD Act significantly expands the type of surveillance certain foreign governments can conduct in the U.S. by permitting foreign government to obtain real-time interceptions of communications from the companies, in addition to stored data (Sec. 4(1)(A)"(J)"). This poses a new threat to internet users. When the U.S. government seeks access to communications in real-time it must meet additional safeguards under the Wiretap Act.

The CLOUD Act would permit foreign governments to obtain the same kinds of information that the U.S. government could only get pursuant to a wiretap order.

The Supreme Court and Congress have imposed strict protections for when wiretaps may be used, under what circumstances, for how long, and in conjunction with super-minimization procedures to reduce incidental collection. These limits and procedures are designed to protect the privacy of the surveillance target, as well as the privacy of those with whom the surveillance target is communicating.

Specifically, the Wiretap Act only permits the government to obtain a wiretap order in investigations that meet an enumerated list of (mostly) serious crimes (18 USC 2516(1)) based on a showing of probable cause that one of those crimes occurred, is occurring, or will occur. The government must also show that there are no other less-intrusive means of obtaining the same evidence, and wiretap orders are only valid for 30 days, at which point they must be reauthorized. Finally, the government must employ stringent real-time and post-collection minimization to ensure that it does not collect or retain communications that are unrelated to their investigation (18 USC 2518).

The CLOUD Act would permit foreign governments to obtain the same kinds of information that the U.S. government could only get pursuant to a wiretap order. However, the foreign government would not be subject to the same strict minimization requirements under the Wiretap Act, or the same restrictions of what investigations and for how long a wiretap could be used. Instead, the CLOUD Act would require only that minimization procedures be established, without any meaningful instruction as to what those procedures must entail except that they mirror FISA minimization procedures as much as possible (Sec. 5 "§2523(b)(2) & (3)(G)"). Additionally, wiretap orders must be issued for a "fixed, limited duration," though there is no upper limit on what that duration may be except that it "may not last longer than is reasonably necessary," and that may be issued only if there are no feasible less intrusive means of obtaining that information (Sec. 5 "§2523(b)(3)(D)(vi)").

[1] ECPA does not require the government to obtain a warrant for communications that are over 180 days old. However, current DOJ policy is to require a warrant to obtain communications contents, irrespective of when they were created. The absence of an amendment to ECPA to close the 180-day loophole is troubling, particularly since it has been included in related legislation, like the International Communications Privacy Act (S. 1671).

[2] In addition to the contents of stored wire or electronic communications, foreign governments may use MLATs to execute warrants for physical or remote access searches; pen register and trap and trace device orders; and to compel a witness to testify or provide a statement, or produce physical evidence.

SOLUTION #1: The CLOUD Act should be amended to remove the authorization for certified foreign governments to obtain real-time intercepts of their surveillance targets' communications. At the very least, the bill should be amended to impose requirements for real time intercepts that are comparable to the protections of the Wiretap Act.

PROBLEM #2: The CLOUD Act would permit foreign governments to obtain communications contents without prior judicial authorization and under a weaker standard than the probable cause standard that is currently required under MLATs, and to obtain metadata without any evidentiary showing. It would also permit foreign governments to make data requests for a broad and poorly defined set of crimes.

The bill's safeguards are insufficient to ensure that the foreign government's review would protect individual rights.

Under current law, any foreign government seeking access to the contents of communications from a U.S. company must proceed through the MLAT system, which requires the foreign government to establish probable cause of a crime and the U.S. Justice Department to obtain a warrant from a U.S. judge. The CLOUD Act's MLAT bypass process means that we would rely solely on review by the foreign government. However, the bill's safeguards are insufficient to ensure that the foreign government's review would protect individual rights. Rather, the new process would weaken existing safeguards in three ways.

First, the bill would not require the foreign government to obtain prior approval from an independent judge as would be required under the MLAT process. Instead, the CLOUD Act would merely require that orders be "subject to review or oversight by a court, judge, magistrate, or other independent authority (Sec. 5 "§2523(b)(3)(D)(v)"). This could include after-the-fact generalized oversight. Failing to require foreign governments to obtain independent pre-approval of their surveillance orders would increase the chances that orders will be issued that do not meet applicable standards.

Second, the CLOUD Act would permit certified countries to access the contents of communications under a lesser evidentiary standard than the probable cause standard that is required under the MLAT process. It would require only that a foreign government issue orders "based on a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation" (Sec. 5 "§2523(b)(3)(D)(iv)"). While this standard incorporates some elements that are required for searches under U.S. law, like particularity, it is drafted in a very vague manner, and does not require that the "reasonable justification" be connected to evidence of serious crimes or that it be "reasonable justification" of anything in particular.

Additionally, the bill would not address a longstanding concern under current law: Foreign governments are not required to obtain approval from an independent judge in the U.S. or abroad before issuing an order for sensitive metadata, such as web browsing history or email records. As a result, foreign governments can often obtain internet users' metadata from U.S. companies under a lower standard than that to which the U.S. government is held. The CLOUD Act fails to remedy this gap in the law and continues to allow foreign governments to obtain metadata from U.S. companies without any evidentiary showing or prior judicial review.

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

Third, the COULD Act does not sufficiently limit the types of investigations for which a surveillance order that bypasses the MLAT process can be issued. Currently, MLATs may only be used to obtain evidence of a crime, and the crime being investigated by the foreign government must also be a crime under U.S. law which is of such severity that it punishable by more than one year of imprisonment (18 USC 3512(e)).

The authorized purposes for which a foreign government could make a request for information under the CLOUD Act are far broader. It requires only that the purpose of the request be for "obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism" (Sec. 5 "§2523(b)(3)(D)(i)"). This standard does not require that the information sought be evidence of a crime; instead it must merely be related to criminal or terrorist activity. Additionally, while the bill requires that orders be issued in relation to "serious crimes," it provides no definition for what constitutes a "serious" crime. Finally, by allowing these orders to also apply to information that is relevant to terrorism investigations, the bill creates a troublingly broad category for surveillance. As is clear from the many concerns raised in the FISA Section 702 reauthorization debate, this provision may result in a significant number of innocent individuals' communications getting swept up.

SOLUTION #2: The CLOUD Act should be amended to require prior independent judicial authorization for data requests. Additionally, it should be amended to mandate a more robust standard that provides more comparable safeguards to the probable cause standard before a surveillance order for contents can be issued. It should also be amended to impose a standard under which metadata could be obtained. Finally, the bill should be amended to narrowly and clearly define the types of serious crimes that can be investigated using this MLAT bypass option, and remove the permission for foreign governments to request information that is relevant to terrorism investigations that do not also constitute criminal investigations.

PROBLEM #3: The CLOUD Act would provide inadequate protections for Americans' privacy if their communications are incidentally collected. The CLOUD Act would allow some contents and all metadata to be shared back to the U.S. government without any U.S. legal process or judicial oversight, and without imposing any use limitations on the U.S. government. Unless the CLOUD Act were amended to require foreign governments to provide prior judicial authorization under a more robust standard of review, this creates the potential for a new backdoor through which the government could warrantlessly access and use Americans' communications. It would also allow some Americans' communications data to be shared with third party foreign governments.

The CLOUD Act would allow Americans' communications contents and metadata to be incidentally collected by foreign governments, and then shared back to and

used by the U.S. government without any U.S. judicial process. The bill would prohibit foreign governments from intentionally targeting and reverse targeting U.S. persons and people located inside the U.S., and it would require the segregation or deletion of data that is not relevant to an investigation into "serious crime, including terrorism," or that is not needed to "protect against a threat of death or serious bodily harm," regardless of imminence (Sec. 5 "§2523(b)(3)(A-B) & (G)"). However, because the bill fails to include any rules for collection of metadata, foreign governments would be authorized to share any metadata they collect that pertains to a U.S. person back to the U.S. government for any reason whatsoever - or for no specific reason at all.

The bill would also permit foreign governments to share the contents of Americans' communications with the U.S. government if the communications are relevant to serious crime under the standard of Sec. 5 "§2523(b)(3)(G)" and also "relate[] to significant harm, or the threat thereof, to the United States or United States persons" (Sec. 5 "§2523(b)(3)(H)"). While the bill elaborates that this kind of harm could include "crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial crime," it does not impose a strict limit. This means that the foreign government is free to interpret what it considers to be a significant harm to the U.S., and could share Americans' data back to the U.S. under that interpretation.

The CLOUD Act would allow Americans' communications contents and metadata to be incidentally collected by foreign governments, and then shared back to and used by the U.S. government without any U.S. judicial process.

Under normal circumstances, to access highly sensitive metadata, like electronic communications transactional records (ECTRs), the U.S. government must obtain a court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the...records or other information sought, are relevant and material to an ongoing criminal investigation" (18 USC 2703(d)). To obtain stored contents, it would have to get a warrant based on probable cause (18 USC 2703(a)), and, as discussed above, to obtain real-time communications it would have to jump through several additional hoops under the Wiretap Act. However, as noted above, foreign governments are already permitted to access metadata directly from U.S. providers, and the CLOUD Act would impose no limitations on how metadata or contents could be accessed and used in investigations once it has been shared back to the U.S. government.

This could result in the FBI and other intelligence agencies making the same legal claim that they make with regard to Americans' incidentally collected communications under Section 702: if it was "lawfully" collected, it can be lawfully used for any investigation or other lawful purpose. Unless the CLOUD Act were amended as outlined above to require prior judicial authorization under a more robust standard of review, this could amount to the equivalent of a backdoor for warrantless searches, and here, unlike with Section 702 surveillance, U.S. courts have no authority to oversee any element of the foreign government's collection or the U.S. government's receipt of this information. Also like with Section 702, under the CLOUD Act, the U.S. government would not necessarily have to give an American notice, if their communications were shared back to the FBI and used in a criminal investigation.

Finally, the CLOUD Act fails to restrict foreign governments from sharing Americans' metadata and the contents of their communications that are relevant to serious crimes under the standard of Sec. 5 "§2523(b)(3)(G)", with third party governments. This could result in Americans' communications being shared with governments that violate international human rights obligations and laws, and would result in a further invasion of Americans' privacy.

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

SOLUTION #3: The CLOUD Act should be amended to prohibit foreign governments from sharing Americans' communications metadata and contents back to the U.S. government. At the very least, it should be amended to impose strict limits on the U.S. government to ensure that any data that is shared back is used only to prevent or mitigate an imminent threat of death or serious bodily injury. Finally, the bill should prohibit foreign governments from sharing Americans' communications data with third party governments.

PROBLEM #4: The CLOUD Act would fail to establish clear and strict standards to ensure that countries seeking to qualify for this MLAT bypass option have a strong record of protecting human rights. The CLOUD Act would also provide the Executive Branch with too much discretion and would fail to incorporate adequate oversight for determinations of whether countries meet the bill's standards.

The CLOUD Act would authorize the Attorney General to enter into bilateral agreements with foreign governments that would then enable those governments to bypass the MLAT process and make data requests directly to U.S. companies.

The CLOUD Act would authorize the AG to enter into bilateral agreements with foreign governments that would then enable those governments to bypass the MLAT process and make data requests directly to U.S. companies. In order to enter into such an agreement, the AG, with the concurrence of the Secretary of State, would have to certify to Congress that the foreign government has met certain requirements intended to protect privacy, civil liberties, and human rights. However, these protections are inadequate for two reasons.

First, in order to certify a foreign government, the AG would have to determine that the country's domestic laws adequately protect privacy and civil liberties (Sec. 5 "§2523(b)(1)"). However, this protection is inadequate because the bill only specifies "factors to be considered" in determining if the country qualifies, rather than imposing mandatory standards. So, the AG would have to consider factors like whether a country "has adequate substantive and procedural laws on cybercrime and electronic evidence," "demonstrates respect for the rule of law and principles of nondiscrimination," adheres to international human rights law and protects free expression, prohibits torture and "arbitrary arrest and detention," and requires "fair trial rights" (Sec. 5 "§2523(b)(1)(B)"). But, if a country does not guarantee fair trials, or if it arbitrarily arrests or detains its citizens, if it suppresses free speech, engages in mass surveillance, or otherwise violates human rights, there is nothing in the bill that would stop the AG and Secretary of State from certifying that country.

Second, the CLOUD Act fails to adequately protect privacy, civil liberties, and human rights because the AG and Secretary of State would have full discretion when making determinations about certifications, and those determinations would be subject to little oversight. While the bill indicates that when determining whether a country should be certified, the Executive Branch should consider credible information and expert input, such consideration would only be required "as appropriate" (Sec. 5 "§2523(b)(1)(A)"). This means that the AG and Secretary of State could simply determine that even where there is credible information that a country under consideration has committed human rights abuses, those abuses are inappropriate to consider in the context of that country's certification. The bill's language also fails to make clear that the government would be required to consult experts who are outside of government, to ensure that researchers and human rights workers are able to weigh in on these determinations.

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

Additionally, the CLOUD Act fails to provide for sufficient oversight for the Executive Branch's decisions about certifications. Congress would not be required to approve or ratify these agreements, as it would for bilateral or multilateral treaties. Instead, to stop a bilateral agreement from going into effect, Congress would have to pass, and the president would have to sign, a joint resolution of disapproval within 90 days of receiving the AG's certification (Sec. 5 "§2523(d)(2)"). Moreover, Congress would have little basis upon which to act, because although the Executive Branch must provide advance notice to Congress of its intent to enter into an agreement, the bill does not even require that they provide a report outlining why they believe the bill's standards are met. The bill would also, concerningly, exempt the AG's determinations from judicial or administrative review (Sec. 5 "§2523(c)").

Finally, the bill provides that the AG, with the concurrence of the Secretary of State, "must" renew their determination about a country's certification every five years (Sec. 5 "§2523(e)(1)"). This suggests that renewal would not even be at the discretion of the Executive Branch; rather, it would be mandatory. Unlike with the original certification, the bill does not provide an avenue through which Congress could stop a renewal by enacting a joint resolution, though Congress would receive a report justifying the renewal (Sec. 5 "§2523(e)(2)").

SOLUTION #4: The CLOUD Act should be amended in several ways to address these problems. The bill should make the factors to be considered in certifying countries mandatory, and it should require the Executive Branch to consider all credible information and consult with experts outside of government. The bill should also require Congress to proactively assent to a certification through legislative approval or ratification before a bilateral agreement can go into effect, and renewals should be subject to the same approval or ratification. At a minimum, the bill should require the Executive Branch to submit a public report outlining the reasons why it believes a proposed bilateral agreement meets the bill's standards.

PROBLEM #5: The CLOUD Act would fail to prevent certified countries from imposing encryption backdoor or data localization mandates on U.S. companies.

An animating concern behind proposals for a legal mechanism to bypass the MLAT process is that without a solution to the current cross-border problem, countries who are frustrated with how slow and cumbersome the MLAT process is will impose encryption backdoor or data localization mandates.

Increasingly, data in transit is protected by encryption, like HTTPS or end-to-end encrypted messaging services. Governments argue that this makes it difficult, if not impossible, for them to obtain real-time intercepts of many internet communications. As online communications and cloud storage have increased, governments have relied more heavily on obtaining stored data through the MLAT process. There is a risk that foreign governments would seek to take matters into their own hands and impose an encryption backdoor mandate as a means of relying less on obtaining data stored in the cloud from U.S. providers. For all of the reasons that U.S. security experts and privacy advocates have argued since the Crypto Wars re-erupted in 2014, encryption backdoor mandates imposed by foreign governments would undermine security, harm privacy, and threaten human rights.

Similarly, there is a risk that countries would seek to impose data localization mandates, and require that any data sent or received within that country's borders be stored within that country. This would ensure that foreign governments retain jurisdiction over those data, enabling them to compel U.S. companies to hand it over without going through the MLAT process. However, any such mandates would threaten privacy and civil liberties, and result in substantial costs and significant technical challenges for companies and consumers.

While the MLAT bypass mechanism that the CLOUD Act would create may lessen the need for countries to impose encryption backdoor and data localization mandates, it does not address every factor that may motivate a foreign government to pursue such policies. Additionally, the failure to incorporate such a prohibition also creates a new risk that the CLOUD Act could wind up being "backdoor" for encryption backdoors. This is because foreign governments could use orders under the MLAT bypass process to issue demands for exceptional access to plaintext data. Given the grave threats those mandates and exceptional access requests could pose to internet security and freedom, the CLOUD Act's failure to prohibit them as a condition of a foreign government's certification is a notable and dangerous omission.

SOLUTION #5: The CLOUD Act should be amended to prohibit any government that is a party to a bilateral agreement from imposing encryption backdoor or data localization mandates.