The Washington Post

August 14, 2017

What the United States can do to protect Internet freedom around the world

By Jared Genser

The story is largely forgotten. When Chinese journalist Shi Tao used his Yahoo account to post a summary of a confidential Communist Party memo to a U.S.-based website in 2004, he knew he was risking persecution and imprisonment. But he had no idea that Yahoo would directly assist his persecutors by handing over private data from his account to the Chinese government. Based on this information, Shi was sentenced to 10 years in prison for "leaking state secrets." Yahoo was widely condemned for its actions at the time. But in the 13 years since, surprisingly little has changed.

Today, U.S. technology companies adhere to a wide array of requirements from repressive governments that undermine Internet freedom and privacy. These demands violate international law, including the right to freedom of expression. But the enormous benefits of market access outweigh the relatively low costs associated with accepting repressive governments' demands.

Undoubtedly, there are circumstances in which requests for information or access to accounts are reasonable, such as when investigating terrorism and major crimes. But the misuse and abuse of this power by authoritarian governments are routine.

Take Apple's recent decision to remove numerous virtual private network (VPN) apps from its App Store in mainland China. The apps allowed users to evade Chinese censorship tools to access banned websites and send secure communications. Given that Apple is valued at $830 billion and is sitting on $262 billion in cash, it could have stood firm and insisted that China adhere to its global standards. Instead, by acquiescing to a new Chinese regulation requiring the "registration" of VPNs, Apple removed a critical tool that enabled its users to speak freely, access information and protect their privacy.

Nor is the problem limited to China. In June, reports emerged that Cisco and IBM had complied with demands from the Russian government to permit state-affiliated firms to examine the source code of their security products. This could allow Russia to discover

vulnerabilities in the code for software containing encryption, raising fears among dissidents that it could be used by security services to decrypt sensitive information. Companies, however, have cooperated with Russia over concerns that the government would have delayed or denied product approval, which would have impeded access to Russia's estimated $18.4 billion information technology market.

Some companies even try to justify their compliance as a means to serve the greater good. In a 2015 post, Facebook founder Mark Zuckerberg remarked, "If we ignored a lawful government order and then we were blocked, all of these people's voices would be muted." Needless to say, statements like this have elicited widespread alarm.

There have been voluntary efforts to address these concerns. The most prominent movement at the international level is the multi-stakeholder Global Network Initiative. A consortium of industry and civil society actors, the initiative works to end censorship and protect private data through its Principles on Freedom of Expression and Privacy. But despite the presence of big-name industry participants such as Facebook and Google, it has largely failed because it relies on self-reporting, involves non-binding commitments and has no enforcement mechanism.

As voluntary measures have proved insufficient, it's time for the U.S. government to step in with stronger laws to protect Internet freedom around the world. While there are no easy solutions here, some common-sense measures could help.

First, the State Department should designate countries with particularly restrictive or abusive Internet access and monitoring policies. This idea was previously proposed by Rep. Christopher H. Smith (R-N.J.) in a Global Online Freedom Act, but it never became law. The State Department's yearly human rights reports already discuss the status of "Internet freedom." But formally designating "Internet-restricting countries" would take those reports a step further, putting U.S. companies on notice that specific governments' practices violate international law.

Second, the U.S. government should require publicly traded American companies that operate in Internet-restricting countries to report publicly on their activities in those countries as a filing mandated by the Securities and Exchange Commission. Reports should disclose all requirements for market access imposed by that government and any specific requests for information that have been complied with, either by court order or voluntarily during each reporting period. Making it mandatory for companies to report on the requirements of market access would provide transparency on their practices and the associated risks for their shareholders.

And finally, Congress should adopt a new law to create legal liability for direct actions by U.S. technology companies abroad that result in wrongful arrest, torture, imprisonment or murder by a foreign government, as defined by international law. When knowingly operating in repressive countries that restrict Internet access, surveil their citizens and invariably persecute their

dissidents, U.S. companies should not be allowed to hide behind claims of following court orders.

Companies are looking for leadership. At a White House summit on cybersecurity, Apple chief executive Tim Cook said that privacy can "make a difference between life and death." Unless the U.S. government stands in support of companies that refuse to comply with wrongful requirements, authoritarian regimes will feel emboldened to make ever-increasing and unreasonable demands. And while U.S. technology companies should be able to invest in Internet-restricting countries, if their choices directly facilitate the persecution of these governments' political opponents, then they should bear the costs.

Jared Genser is an international human rights lawyer based in Washington.