

May 7, 2018

Honorable Bob Corker
Chairman, Committee on Foreign Relations
United States Senate
Washington, D.C. 20510

Honorable Bob Menendez
Ranking Member, Committee on Foreign
Relations
United States Senate
Washington, D.C. 20510

Honorable John Thune
Chairman, Committee on Commerce,
Science, and Transportation
United States Senate
Washington, D.C. 20510

Honorable Bill Nelson
Ranking Member, Committee on Commerce,
Science, and Transportation
United States Senate
Washington D.C. 20510

Honorable Ed Royce
Chairman, Committee on Foreign Affairs
House of Representatives
Washington, D.C. 20515

Honorable Eliot Engel
Ranking Member, Committee on Foreign
Affairs
House of Representatives
Washington, D.C. 20515

Honorable Greg Walden
Chairman, Committee on Energy and
Commerce
House of Representatives
Washington, D.C. 20515

Honorable Frank Pallone, Jr.
Ranking Member, Committee on Energy and
Commerce
House of Representatives
Washington, D.C. 20515

Honorable Marco Rubio
Chair of the Congressional-Executive
Commission on China
United States Senate
Washington, D.C. 20510

Honorable Chris Smith
Co-Chair of the Congressional-Executive
Commission on China
House of Representatives
Washington D.C. 20515

Dear Members of Congress,

We write to ask your help in requesting that Amazon and Google reverse their recent decision to block U.S government funded anti-censorship tools from using the companies' servers to enable hundreds of millions of people in authoritarian countries to evade state firewalls. In doing so, these companies capitulated to repressive foreign governments and prioritized their own commercial interests over democracy, human rights, and access to independent news.¹

In the past two weeks, Amazon and Google have removed the ability for U.S. government funded anti-censorship technologies to function in repressive countries such as Russia, China,

¹ Russian Censor Gets Help From Amazon and Google -
<https://www.bloomberg.com/view/articles/2018-05-03/telegram-block-gets-help-from-google-and-amazon>

and Iran.² The technique they have disabled is known as domain fronting, which works by routing online communication through the infrastructure of a major technology company like Amazon or Google, in order to obscure the actual destination that would otherwise be blocked. This enables people using censorship circumvention apps to more effectively evade firewalls and surveillance that are widely used in authoritarian countries.³ Domain fronting prevents governments and state controlled internet service providers in closed societies from shutting down the anti-censorship tool without paying a heavy price by blocking access to the whole suite of popular Amazon or Google products, such as Gmail, Google Search, and YouTube, as well as the many other popular websites online that use their infrastructure.

The U.S. government through the U.S. Department of State, the Broadcasting Board of Governors, and the Open Technology Fund helped to incubate and support domain fronting over the course of the last six years. Until this change by Amazon and Google, domain fronting was the most effective and most widely used method of enabling free speech, free association, and freedom online in countries that aggressively filter and monitor internet access. For example, in recent weeks the tactic was utilized by the messaging app Telegram after it became blocked in Russia, where censors have blocked nearly 20 million IP addresses in attempts to shut the app down. Their efforts have been largely unsuccessful, due in part to the resiliency domain fronting provides.⁴ Indeed, the Russian government entity in charge of blocking Telegram called on Google to prevent Telegram from using domain fronting to circumvent censorship and were happy to share the news of Google's recent decision.⁵ Similarly, more than a dozen publicly funded tools, including Psiphon, Ultrasurf, Signal, Tor, Greatfire, and Lantern utilize domain fronting to allow millions of people every month to access uncensored, free, and open internet.

More, major public and private international media organizations rely upon these USG supported technologies and domain fronting to reach audiences globally within repressive countries who do not have access to a free press within their own countries. These include private media organizations such as the *New York Times*, the *Associated Press*, the *Wall Street Journal* and the *Washington Post*, international broadcasters including the Canadian Broadcasting Corporation, British Broadcasting Corporation, Deutsche Welle, and our own Voice of America, Radio Free Europe / Radio Liberty, Office of Cuba Broadcasting, Radio Free Asia, and Middle East Broadcasting Networks) and NGOs/CSOs that support democratic and human rights efforts such as Human Rights Watch, Reporters without Borders, and the Committee to Protect Journalists. Collectively, their use of USG supported anti-censorship technology built upon domain fronting allow hundreds of millions of people every month access

² Amazon Bends the Knee to Autocrats, Threatens to Cut Off Signal for Using Anti-Censorship Technique - <https://gizmodo.com/amazon-bends-the-knee-to-autocrats-threatens-to-cut-of-1825697153>

³ Threat modeling and circumvention of Internet censorship: Domain fronting - <https://www.bamssoftware.com/papers/thesis/#chap:domain-fronting>

⁴ This is why Russia's attempts to block Telegram have failed - <https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google>

⁵ <http://money.cnn.com/2018/04/23/technology/google-russia-blocked-telegram/index.html> and <https://twitter.com/roscomnadzor/status/986861412495581185>

to a free press and the ability to speak freely from within repressive countries such as Russia, Iran, China, Egypt, and many others.

Beyond access to a free press, within countries such as Iran and China, an unrestricted internet is the only way for religious minorities of many faiths to practice their beliefs. In their attempts to suppress religious freedom, these repressive regimes continue to evolve and deploy even more “high-tech methods to control religion and punish believers -- including surveillance and arrest of believers for sharing information online”.⁶ Here again, domain fronting remains one of the few reliable technologies within these countries that allow for the safe practice of one’s religion.

Google and Amazon have long known about domain fronting, and previously ignored complaints, and even threats from foreign governments.⁷ Unfortunately, these two American companies recently decided to quietly capitulate to these repressive countries, by prohibiting the practice of domain fronting through their cloud services, including by the developers of U.S. government supported internet freedom tools. In doing so, Amazon and Google have directly, intentionally or not, aided these authoritarian regimes’ efforts to limit their peoples’ access to information, at a dire cost to democracy and human rights movements within these countries.⁸

In a 2014 New York Times op-ed, then-Google CEO Eric Schmidt wrote about the important role both the private and public sectors would need to play in expanding Internet freedom worldwide. Highlighting the increasing censorship in places like Russia, Vietnam, and Ukraine, Schmidt wrote:

“Obfuscation techniques — when one thing is made to look like another — are also a path forward. A digital tunnel from Iran to Norway can be disguised as an ordinary Skype call. Deep packet inspection cannot distinguish such traffic from genuine traffic, and the collateral damage of blocking all traffic is often too high for a government to stomach...Much of the fight against censorship has been led by the activists of the Internet freedom movement. We can join this open source community, whether we are policy makers, corporations or individuals. Money, coding skills or government grants can all make a difference. Given the energies and opportunities out there, it’s possible to end repressive Internet censorship within a decade. If we want the next generation of users to be free, we don’t see any other option.”⁹

⁶ Bibles pulled from online stores as China increases control of religion - <https://edition.cnn.com/2018/04/05/asia/china-bible-online-christianity-intl/index.html>

⁷ China’s Great Cannon - <https://citizenlab.ca/2015/04/chinas-great-cannon/>

⁸ Amazon threatens to suspend Signal's AWS account over censorship circumvention - <https://signal.org/blog/looking-back-on-the-front/>

⁹ The Future of Internet Freedom <https://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html>

Just four years later, Google is disabling the very “obfuscation techniques” their leadership tacitly endorsed at the time - leading the way for other private sector actors to do the same and increase repressive Internet censorship, rather than end it.

For more than a decade, Internet Freedom has received broad bipartisan support from Congress, who’ve authorized the U.S. government to support:

“[...] Research of key threats to Internet freedom; the continued development of technologies that provide or enhance access to the Internet, including circumvention tools that bypass Internet blocking, filtering, and other censorship techniques used by authoritarian governments; and maintenance of the United States Government’s technological advantage over such censorship techniques [...]”.¹⁰

Domain fronting has been pivotal to the strategic foreign policy goal of advancing global Internet Freedom and leverages the global significance of U.S. based technology companies. These same companies have thrived due to the freedoms afforded to them in the United States and should be held to account for denying those same freedoms to the most repressed societies around the globe. The end of domain fronting will not permanently impede progress toward our shared goal of global internet freedom, but it will set it back, and the adverse effects will be felt most direly by those already experiencing repressive censorship and surveillance.

As such, we ask for your support in urging Google and Amazon to reverse their decision.

Sincerely,

Nathan White
Senior Legislative Manager
Access Now

Peter Micek
General Counsel
Access Now

¹⁰H.R.1625 - Consolidated Appropriations Act, 2018 -
<https://www.congress.gov/bill/115th-congress/house-bill/1625/text>