Cisco's Position on Government Use of Technology to Curtail Freedom of Expression

At Cisco, we are strongly committed to an open global internet. We build our products to promote the free flow of information, privacy, and freedom of expression.

Cisco was founded in 1984 by two computer scientists at Stanford in order to enable communication among different computer systems. Decades later, our mission has not changed. Cisco supports free expression and open communication, and we recognize the importance of driving policies to enable people the world over to benefit from the freedom and empowerment that the internet can offer. To that end, our goal remains to expand access to information and promote innovation by building our products according to open, global standards that promote human rights, including privacy and freedom of expression.

As set out in the 2011 United Nations Guiding Principles on Business and Human Rights, businesses have a responsibility to respect internationally recognized human rights and fundamental freedoms, which includes avoiding infringing on the human rights of others and addressing adverse human rights impacts with which they are involved. Embracing this critical responsibility, Cisco's Global Human Rights Policy, first published in 2012, articulates our long-standing commitment to uphold and respect human rights for all people. Further, in 2018 Cisco published human rights position statements related to the development and use of disruptive technologies that are shaping our collective future, setting out our perspective on the potential human rights impacts of encryption, data localization and sovereignty, surveillance by governments, internet of Things, big data analytics, and artificial intelligence, and how we intend to address their potential adverse human rights impacts.

One additional area of technology in particular – network security – provides enormous protection to human rights. Network security technology allows people to work, send email messages, browse the internet, read articles, publish blogs, and shop in privacy. At Cisco, we are proud to be the industry leader in providing network security products that are designed to keep data and internet access safe and secure. We see this as critical to advancing human rights around the world.

The same capabilities that enhance network security can be deployed by end users to subvert these principles. Around the world, governments that fear the liberating power of ideas seek to block free expression by exploiting the very security technologies designed to protect internet users from outside threats. It is possible for these actors to use these capabilities to block their citizens from accessing, receiving, and sharing information from or with outside sources, thereby subverting their citizens' rights to privacy and freedom of expression.

Unfortunately, there is no effective way to provide network administrators the capabilities necessary to protect their networks (and end users) without also putting at their disposal powerful security capabilities that can be exploited in ways that can impair free expression. Disabling these security technologies would put networks, and the users of those networks, at risk. Take, for example, the use of Deep Packet Inspection (DPI) in networks. This ubiquitous networking and security capability enables visibility into network traffic packets to detect and block malware, distributed denial-of-service attack risks, viruses, spam, and other security threats. While leading DPI technologies have been designed to protect the security of network end users, press reports for more than a decade have alleged their (mis)use by governments to facilitate the control and censorship of the flow of information, blocking access to unfavored websites, and restricting the use of encrypted communication tools.

Governments are increasingly restricting free access to information by deploying security technologies to shut down access to content they oppose. They typically implement these shutdowns by issuing orders to telecommunications companies and internet service providers, often together with a gag order limiting transparency. These companies often have little choice but to comply because they are government-controlled or rely on government licenses to operate. According to Access Now, there were 196 documented internet shutdowns in 25 countries in 2018 alone. Shutdowns are often ordered in response to protests, in the lead-up to elections, or to prevent unlawful or policy-violating activities. No matter the reason,

Cisco's Position on Government Use of Technology to Curtail Freedom of Expression (continued)

internet shutdowns have a direct impact on human rights, including the right of access to information, freedom of expression, and the right to peaceful assembly.

Cisco will continue to follow certain internal rules that it has adhered to for decades with respect to its products to ensure that our business activities will not undermine the right of access to information and the right of freedom of expression:

- We sell the same products globally, built to global standards, thereby enhancing the free flow of information.
- Our networking products include basic features that are essential to the fundamental operation of the internet.
- These basic features — without which much of the internet could not function effectively — can, unfortunately, be used by network administrators for political and other purposes.
- In this regard, we do not customize or develop specialized or unique filtering capabilities in order to enable different regimes to block access to information with the intent of undermining these rights and freedoms.

We often are not in a position to determine how these features are used day to day, so we take these additional steps to promote these principles:

- We do not support attempts by governments to fragment the internet or otherwise create a "closed" internet.
- We do not support interception of telephone calls made over the internet using Voice over internet Protocol except in response to valid court orders consistent with due process of law.
- Consistent with Cisco's Security Vulnerability Policy, our product development practices specifically prohibit any intentional behaviors or product features that are designed to allow unauthorized device or network access, exposure of sensitive device information, or a bypass of security features or restrictions (including, but not limited to, undisclosed device access methods or "backdoors").

It's clear now more than ever that Cisco's networking and security products present an immense opportunity for advancing human rights, but governments can exploit these tools to control their citizens' ability to access, receive, and share ideas freely with one another. Through our human rights approach, we will continue to promote uses of technology that are respectful of human rights.