

The Cybersecurity and Internet Freedom Act: Free Speech vs National Security?

Take a second to think about how many times each day you use a computer to complete routine tasks. Now, imagine that a government-instituted “Internet blackout” blocked all access to the Internet - no broadband, no Wi-Fi - not even a dial up connection. Without the Internet, you would lose the ability to read news, access Skype, Facebook, or Twitter, chat or email, and purchase products through Amazon or eBay. The recent events in Egypt have generated a lot of buzz about a government’s ability to regulate and potentially shut down the Internet. On January 27, 2011, thousands of Egyptian citizens flooded the streets of Cairo to [protest against the Egyptian government](#). Two days later, Internet access began to dwindle, until service was no longer available in Egypt. This Internet blackout continued for five days. Why would a government order a shut down of the Internet? Put simply, the Egyptian protesters were using social-networking sites such as Twitter and Facebook to organize the massive protests. In an attempt to stop the demonstrations, the Egyptian government [ordered the country’s four major Internet service providers](#) to shut down service. Meanwhile, in the U.S., the [Cybersecurity and Internet Freedom Act](#) (“CIFA”), aptly nicknamed the “Internet kill switch,” has been introduced in the Senate as a means to combat another kind of cyber threat.

IS THE CIFA AN “INTERNET KILL SWITCH”?

In January, Senate Majority Leader Harry Reid and other congressional members put forth a placeholder bill named the “[Cybersecurity and American Cyber Competitiveness Act of 2011](#),” and stressed that cybersecurity should be a top priority for the 112th Congress. Senators Lieberman, Collins, and Carper introduced the CIFA on February 17, 2011. The objective of the bill is to give the government the power to limit Internet traffic in the event of a cybersecurity emergency. It would grant the President the power to “authorize emergency measures to protect the nation’s most critical infrastructure, if a cyber vulnerability is being exploited or is about to be exploited.” Any system or resource is considered to be part of the “critical infrastructure” if its destruction or disruption would cause a national or regional catastrophe. The Department of Homeland Security and members of the private sector would work together to create a list of the systems and resources that would be part of the “critical infrastructure.” This list would include both government and private sector facilities, such as banks, power plants, telephone companies, and Internet service providers. In fact, [85% of the nation’s “critical infrastructure”](#) is likely to be operated by the private sector. Also, the President could demand that access to any part of the “critical infrastructure” be shut off in the face of a significant threat. [However, the exact meaning and scope of this language is being fiercely debated.](#)

CENSORSHIP CONCERNS

Opponents of the CIFA range from civil liberties groups to owners and operators of the “critical infrastructure.” They oppose the CIFA because they believe that the bill’s language is ambiguous. A [letter written by the ACLU](#) to the bill’s sponsors outlined three perceived risks with the CIFA. First, the bill seems to grant the President a broad expansion of power over private companies, especially those deemed a part of the “critical infrastructure.” Although the expansion of power would not authorize the President to take over the “critical infrastructure,” it would give him the authority to take undefined actions, such as limiting the public’s access for 30-day periods that may be renewed indefinitely. The second concern is the ambiguity over which parts of the Internet would qualify as “critical infrastructure,” and to what extent these facilities would be shut down during a “cyber emergency.” The ACLU is worried that the

emergency actions taken by the President may shut down or limit Internet communications, which would limit systems that are necessary for the economy to function and for the public to communicate and access information.

Finally, the ACLU claims that the bill lacks an adequate definition for the term “cyber emergency.” The CIFA does not define this term, but [authorizes the Department of Homeland Security](#) to “develop and coordinate the emergency measures necessary to preserve the reliable operation of the critical infrastructure.” The underlying fear is that the government could use this bill to declare a cyber emergency in order to silence free speech or censor parts of or the entire Internet. Although the intention behind the CIFA may not be to stifle free speech, the bill will provide the government the ability to limit Internet traffic, and critics like the ACLU caution that this power has the potential to be abused. In summary, the ACLU have asked that the power authorized under the CIFA be properly defined and restricted.

THE RESPONSE FROM THE SENATE: MYTH VS. REALITY?

After the ACLU’s letter was sent to the committee, the Senators who authored the bill released a [myth vs. reality fact sheet](#) to address the concerns. The fact sheet insists that the CIFA would not give the government the power to shut off all access to the Internet. In support of this claim, it points to a provision in the CIFA which states, “neither the President . . . [n]or any other officer or employee of the United States Government shall have the authority to shut down the Internet.” The Senators rebut the contention that the bill is an “internet kill switch” that will be used to regulate free speech or silence anti-government sentiment. Instead, they view it as legislation intended solely to protect the U.S. from cyber attacks that would wreak havoc on the U.S. network. They also argue that the bill is essential, because a cyber attack on certain areas of the “critical infrastructure” could affect a wide range of crucial components that are required to run the day-to-day activities of the US.

Each year, cyber attacks cost the government and private sector a significant amount of money. So far in 2011, [attacks on US government facilities have cost over \\$1.8 billion per month](#). In addition, American businesses employing more than 500 people lose an average of \$3,800,000 per year to cyber attacks. The attacks may worsen. A quick Internet search of “hacked government websites” produces numerous articles and the details of the latest government sites that have been compromised. Every government site from the military to NASA has been hacked, and on the black market [anyone with \\$500 can buy access](#) to a hacked government site of their choosing. The fear fueling the bill’s passage is that the next major cyber attack on either government or private sector facilities could prove to be disastrous.

The fact sheet also addressed the opponents’ concerns regarding the expansion of the President’s power over Internet traffic. The Senators point to a provision that requires the President to use the “least disruptive means feasible” to respond to the threat, but *does not* authorize the government to *take over* the “critical infrastructure.” In addition, the President would only be able to invoke this authority when a cyber attack results in mass casualties, severe economic consequences, long-term mass evacuations, or the severe degradation of national security capabilities. Lastly, the fact sheet argues that the CIFA is actually a restriction of the President’s power, and they refer back to 1942, when Japan attacked Pearl Harbor. In response to government fears about future foreign invasions, Congress passed legislation that gave President Franklin Roosevelt the authority to take over the telephone and telegraph networks. [After almost 70 years, the law is still on the books](#). Section 706(d) of the Communications Act grants the President broad authority to shutdown “any facility or station for wire

communication,” when there is a war or a threat of war. Although there is no mention of the Internet, this outdated provision would arguably extend the President’s ability to shut down the Internet any time there is a threat of war. Thus, the provision in the CIFA stating that no government official will have the “authority to shut down the Internet” would actually limit the power the President currently has to control Internet traffic. However, the effect that the CIFA would actually have on Section 706(d) is not clear.

THE FATE OF THE CIFA

The bill’s future is uncertain, and it has been referred to the Committee on Homeland Security and Governmental Affairs before it goes before the full Senate in the coming months. Is the CIFA really an “Internet kill switch”? Although it is unlikely that the President could actually shut down the Internet, there is always potential for abuse. Ultimately, people have a right to speak freely without fear of government suppression, and the Internet is vital to communication. But is governmental control of a private sector entity, even during a cyber emergency, what the U.S. needs? Would it hurt the economy and stifle the free speech? Or would it preserve the economic infrastructure for the greater good? Regardless of your stance, one thing is for sure: [any hint of a government-induced Internet blackout is bound to cause a ruckus.](#)