THE SOUND OF SILENCE:
THE LEGALITY OF THE AMERICAN "KILL SWITCH" BILL

Deborah Beth Medows

In today’s culture, many of our daily interactions depend on the Internet. Internet connectivity empowers us to engage in commerce, contact faraway relatives, or even find a future spouse. This begs the question: To what extent can the government of the United States deny a citizen’s Internet access, and under what legal framework is the effective silencing of the Internet lawful?

This Article explores the technicalities of how Internet censorship works. It then provides a basic introduction to cyberattacks and the types of dangers that such attacks pose. Then, it discusses the framework of the “kill switch” phenomenon by citing examples of governments that have interfered with their inhabitants’ Internet connectivity. Finally, this Article evaluates the legality of pending kill switch legislation in the United States under the scope of the President’s executive powers and the First Amendment’s free speech protections.

I. INTRANATIONAL SILENCING

A. How Intranational Censorship Technically Works

A government’s ability to disconnect a country’s Internet usage is widely known by the pejorative term “kill switch.” In actuality, the term is a misnomer. It is unrealistic to envision that governmental authorities could employ a physical switch to disconnect computers from the Internet. Instead, governmental officials would need to contact Internet Service Providers (ISPs), who would then authorize

1. See Bianca Bosker, Internet “Kill Switch” Would Give President Power to Shut Down The Web, HUFFINGTON POST (Jan. 17, 2010, 4:20 PM, updated May 25, 2011, 5:50 PM), http://www.huffingtonpost.com/2010/06/17/internet-kill-switch-would_n_615923.html (describing the proposed Protecting Cyberspace as a National Asset Act, which, if passed, would allow the “president the authority to seize control of or even shut down portions of the Internet.”).

their engineers to change the configuration of the Internet traffic flow to stop service to the populace. As a result of the governmental action, that portion of the population which previously could connect to the Internet would no longer be able to do so.

B. The Need for Intragovernmental “Kill Switches” in the Age of Cyberattacks

Governments, including that of the United States, may need to disconnect computers from the Internet to counteract the effects of, or to prevent, a cyberattack. This necessity is realistic because this form of attack is not brand-new; there are several notable instances of wide-scale cyberattacks. In 1982, the United States allegedly attacked the Siberian pipeline by placing a logic bomb into software, which caused an explosion. Iran blamed Israel and the United States for planting the Stuxnet worm, which was capable of seizing control of industrial plants, in Iran’s nuclear facilities. The cyberattack eliminated approximately twenty percent of the facility’s nuclear centrifuges. In 2007, a cyberattack in Brazil that was propagated for unclear motives, distressed millions of Brazilians and cost the country millions of dollars. Over three million people across dozens of Brazilian cities lost Internet connection and the world’s largest iron ore producer, located in one of those cities, lost seven million dollars when the attack disconnected seven of its plants from the Internet.

In March of 2001, a disgruntled former employee successfully hacked into the Australian computerized sewage system and released millions of liters of waste into public waterways. These examples are alarming, and as a result of the scope of devastation made possible by these forms of attacks, government-perpetrated cyberattacks may constitute an act of warfare. Although the public may not generally be cognizant of the risks posed by cyberattacks, governments must be allowed to develop a strategy to counteract this new method of attack. Cyberattacks are different from conventional acts of warfare due to the speed with which cyberattacks devastate infrastructure, the perpetrator’s low cost of creating such devastation, and the obstacles that prevent law enforcement from learning the attacker’s identities. As theorist Herman Kahn wrote, virtual attacks are complicated because [the
their engineers to change the configuration of the Internet traffic flow to stop service to the populace. As a result of the governmental action, that portion of the population which previously could connect to the Internet would no longer be able to do so.

B. The Need for Intriguepolitical “Kill Switches” in the Age of Cyberattacks

Governments, including that of the United States, may need to disconnect computers from the Internet to counteract the effects of, or to prevent, a cyberattack. This necessity is realistic because this form of attack is not brand-new; there are several notable instances of wide-scale cyberattacks. In 1982, the United States allegedly attacked the Siberian pipeline by placing a logic bomb into software, which caused an explosion. Iran blamed Israel and the United States for planting the Stuxnet worm, which was capable of seizing control of industrial plants, in Iran’s nuclear facilities. The cyberattack eliminated approximately twenty percent of the facility’s nuclear centrifuges. In 2007, a cyberattack in Brazil that was propagated for unclear motives, distressed millions of Brazilians and cost the country millions of dollars.

Although the public may not generally be cognizant of the risks posed by cyberattacks, governments must be allowed to develop a strategy to counteract this new method of attack. Cyberattacks are different from conventional acts of warfare due to the speed with which cyberattacks devastate infrastructure, the perpetrator’s low cost of creating such devastation, and the obstacles that prevent law enforcement from learning the attacker’s identities. As theorist Herman Kahn wrote, virtual attacks are complicated because “the

1. See id. (describing how the cyberattacks in Brazil caused harm to the country).
2. Id.
3. Id. (describing how a “kill switch” would allow the government to disconnect a portion of society from the Internet).
4. See, e.g., Amar Toor, The Internet “Kill Switch” Bill: What It Is, and Why It Won’t Die, SWITCHED (Feb. 1, 2011, 3:00 PM), http://www.switched.com/2011/02/01/internet-kill-switch-bill-what-it-is-wont-die/ (describing the proposed bill and how the legislation “would provide a mechanism for the government to work with the private sector in the event of a true cyber emergency.”).
5. See Olivia Solon, Do We Need a Geneva Convention for Cyber Warfare?, WIRED (Oct. 1, 2010), http://www.wired.com/news/archive/2010/10/cyber-warfare-convention (describing different examples of when cyber attacks have occurred, such as the Siberian pipeline logic bomb, and attacks in Estonia, Georgia, and even on Google).
6. See id. (“In 1982, the U.S. reportedly sabotaged the Siberian pipeline through a logic bomb planted in software, causing an explosion.”).
7. See id.; see also Stuxnet Worm Hits Iran Nuclear Plant Staff Computers, BBC NEWS MIDDLE EAST (Sept. 26, 2010, 10:57 AM), http://www.bbc.co.uk/news/world/middle-east-11444883 (describing how the worm has infected the personal computers of staff members).
9. See Dan Rivers, On the Frontline of Cyber Warfare, CNN TCH (Nov. 4, 2010, 4:48 AM), http://www.cnn.com/2010/TECH/web/10/28/malaysia.cyber.security/index.html (“In the future, warfare may shift from a battlefield to a keyboard. Superpowers might deem a nuclear exchange too destructive, but already they are developing Weapons of Mass Disruption; software viruses that are designed to cripple the operating systems of power stations, dams, traffic lights and public transport.”).
10. See id. (describing how the cyberattacks in Brazil caused harm to the country).
11. Id.
12. Id.
14. See id. at 98-99 (“The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons... to pose a significant threat to U.S. military capabilities. A dozen determined computer programs can... threaten the United States’ global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target.”).
15. See Kim Zetter, Former NSA Director: Countries Spewing Cyberattacks Should be Held Responsible, WIRED (Jul. 29, 2010, 3:30 PM), http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/ (“Attribution is one of the biggest problems on the internet when it comes to cyberwarfare. How do you hold a nation responsible for malicious attacks if you can’t determine whether the activity was state-sponsored?”).
aggressor has to find only one crucial weakness; the defender has to find all of them, and in advance.\textsuperscript{17}

Since cyberattacks can be incredibly dangerous, it is important to consider the legality of potential prophylactic measures. Some guidance may exist in international law. The provisions of the Geneva Conventions do not adequately address the modern-day issues posed by cyberwarfare and thus fail to serve as a relevant legal framework.\textsuperscript{18} Articles 2(4) and 39 of the United Nations Charter may provide a lawful basis for defense of cross-border cyberattacks.\textsuperscript{19} Alternatively, the international law doctrine known as the Common Heritage of Mankind, which is based on the right of freedom of expression, may protect the public from governmental interference in the ability to use the Internet.\textsuperscript{20} The alleged right to Internet connectivity may also be derived from Article 15, Paragraph 3 of the International Covenant on Economic, Social, and Cultural Rights (ICESCR), which protects the freedom of scientific research and creative activity, and under Articles 13 and 14, which guarantee the right to education.\textsuperscript{21}

Still, international legal provisions do not answer the question of how the United States can protect itself from cyberattacks under domestic law. Over a hundred foreign intelligence organizations have attempted to infiltrate American computer networks,\textsuperscript{22} demonstrating the need for the U.S. to prepare technological and legal defenses to counter these attacks, such as the kill switch. This Article first explores the frameworks through which other countries have used kill switches to disconnect their citizens' Internet connectivity, and subsequently examines the legality of the United States implementing and utilizing a kill switch.

\section*{C. Contextual Examples}

The most noteworthy use of a kill switch occurred in the relatively recent watershed events in Egypt, which has been regarded as "unprecedented in Internet history."\textsuperscript{23} Activists in Egypt used social network websites, such as Twitter and Facebook, to organize protests.\textsuperscript{24} The Egyptian government attempted to cease activists' ability to communicate and to organize dissident political movements by barring access to specific targeted websites.\textsuperscript{25} In its failed attempt to protect its reigning government, the Egyptian government acted in a manner previously considered "unthinkable for any country with a major Internet economy."\textsuperscript{26} The government contacted each of the country's four major ISPs, and "[a]n engineer at each ISP would then access the ISP's routers, which contain a list of all the IP addresses, thus cutting off anyone who wants to access them from within or outside the country."\textsuperscript{27} The ISP connector that supports Egypt's stock exchange, Noor Group, continued to function, but nearly all of the rest of the ISPs complied with the government's order to change access to protect its reigning government, the Egyptian government

\begin{itemize}
\item 18. See Patricia Donovan, Cyberwar: Already Underway with No Geneva Conventions to Guide Them, UNIV. OF BUFFALO NEWSCTR. (Oct. 14, 2010), http://www.buffalo.edu/news/11862 ("But unlike conventional warfare, there is nothing remotely close to the Geneva Conventions for cyberwar. There are no boundaries in place and no protocols that set the standards in international law for how such wars can and cannot be waged.").
\item 19. Antonio Segura-Serrano, Internet Regulation and the Role of International Law, 10 MAX PLANCK Y.B. U.N. L. 191, 221 (2006) ("Because of the novelty of this threat . . . the question arises whether an actual Internet attack . . . might come within the terms of Arts 2 (4) and 39 of the UN Charter, triggering collective action and possibly allowing the right of self-defense.").
\item 20. Id. at 233 (describing how the Common Heritage of Mankind has been largely ignored by developed states, but might be applicable to Internet usage).
\item 21. Id. at 264 ("Under article 15 of the ICESCR, cultural rights [grant] . . . the right to enjoy the benefits of scientific progress and its applications . . . [and] parties undertake to respect the freedom indispensable for scientific research and creative activity. Alternatively, this right of access may form part of the right to education, protected by articles 13 and 14.").
\end{itemize}
aggressor has to find only one crucial weakness; the defender has to find all of them, and in advance.17

Since cyberattacks can be incredibly dangerous, it is important to consider the legality of potential prophylactic measures. Some guidance may exist in international law. The provisions of the Geneva Conventions do not adequately address the modern-day issues posed by cyberwarfare and thus fail to serve as a relevant legal framework.18 Articles 2(4) and 39 of the United Nations Charter may provide a lawful basis for defense of cross-border cyberattacks.19 Alternatively, the international law doctrine known as the Common Heritage of Mankind, which is based on the right of freedom of expression, may protect the public from governmental interference in the ability to use the Internet.20 The alleged right to Internet access may form part of the right to education, protected by articles 13 and 14, which guarantee the freedom of scientific research and creative activity, and under Articles 2(4) and 39 of the United Nations Covenant on Economic, Social, and Cultural Rights (ICESCR), which protects the freedom of scientific research and creative activity, and under Articles 13 and 14, which guarantee the right to education.21

Still, international legal provisions do not answer the question of how the United States can protect itself from cyberattacks under domestic law. Over a hundred foreign intelligence organizations have attempted to infiltrate American computer networks,22 demonstrating the need for the U.S. to prepare technological and legal defenses to counter these attacks, such as the kill switch. This Article first explores the frameworks through which other countries have used kill switches to disconnect their citizens' Internet connectivity, and subsequently examines the legality of the United State implementing and utilizing a kill switch.

C. Contextual Examples

The most noteworthy use of a kill switch occurred in the relatively recent watershed events in Egypt, which has been regarded as "unprecedented in Internet history."23 Activists in Egypt used social network websites, such as Twitter and Facebook, to organize protests.24 The Egyptian government attempted to cease activists' ability to communicate and to organize dissident political movements by barring access to specific targeted websites.25 In its failed attempt to protect its reigning government, the Egyptian government acted in a manner previously considered "unthinkable for any country with a major Internet economy."26 The government contacted each of the country's four major ISPs, and "[a]n engineer at each ISP would then access the ISP's routers, which contain a list of all the IP addresses, thus cutting off anyone who wants to access them from within or outside the country."27 The ISP connector that supports Egypt's stock exchange, Noor Group, continued to function, but nearly all of the rest of the ISPs complied with the government's order to change

18. See Patricia Donovan, Cyberwars: Already Underway with No Geneva Conventions to Guide Them, UNIV. OF BUFFALO NEWSCTR. (Oct. 14, 2010), http://www.buffalo.edu/news/11862 (“But unlike conventional warfare, there is nothing remotely close to the Geneva Conventions for cyberwar. There are no boundaries in place and no protocols that set the standards in international law for how such wars can and cannot be waged.”).
19. Antonio Segura-Serrano, Internet Regulation and the Role of International Law, 10 MAX PLANCK Y.B. U.N. L. 191, 221 (2006) (“Because of the novelty of this threat ... the question arises whether an actual Internet attack ... might come within the terms of Arts 2 (4) and 39 of the UN Charter, triggering collective action and possibly allowing the right of self-defense.”).
20. Id. at 233 (describing how the Common Heritage of Mankind has been largely ignored by developed states, but might be applicable to Internet usage).
21. Id. at 264 (“Under article 15 of the ICESCR, cultural rights [grant] ... the right to enjoy the benefits of scientific progress and its applications . . . [and] parties undertake to respect the freedom indispensable for scientific research and creative activity. Alternatively, this right of access may form part of the right to education, protected by articles 13 and 14.”).
the “lines of code,” and consequently disabled the majority of Egypt’s Internet connectivity.  

Egypt is not the only country that has disabled its inhabitants’ ability to connect to the Internet. Nepal and Burma have both experienced intranational government Internet shutdowns. In response to the Egyptian uprising, Chinese officials blocked information relating to the Egyptian revolt from its estimated four hundred and fifty-seven million Internet users. On a broader scale, the Chinese government completely disabled Internet connectivity in the Xinjiang region in 2009 following dissident political activity.  

These aforementioned international examples demonstrate that foreign governments have been successful, at least to a noteworthy degree, in disabling or limiting Internet use within their own borders. However, even if the United States had the ability to disable Internet access within its borders, it is unclear whether it would be legally able to do so, given the Nation’s rich history of protecting free speech and upholding the separation of powers. Arguably, the Internet is itself a distinctly American concept, built upon the “freedom of information to do so, given the Nation’s rich history of protecting free speech and upholding the separation of powers. Arguably, the Internet is itself a distinctly American concept, built upon the “freedom of information and free flows of data.” Measures to constrain this freedom should be critically evaluated, even when balanced against the importance of safeguarding national security.

II. THE PROPOSED “KILL SWITCH” BILL
A. Provisions of the Bill

In 2010, legislation was introduced in the U.S. Senate specifying the conditions under which the government would have the ability to activate a kill switch. The proposed bill, “S.3480: Protecting Cyberspace as a National Asset Act,” would grant the President the power to disable the Internet in the event of an emergency. This bipartisan bill was co-sponsored by Senators on the Homeland Security and Governmental Affairs Committee: Maine Senator Susan Collins, the ranking Republican on the Committee, Connecticut Independent Senator Joseph Lieberman, the Committee Chairman, and Delaware Democratic Senator Tom Carper. This bill, which was approved by a Senate panel, would create a governmental agency called the National Center for Cybersecurity

28. See id. ("[S]ome 93 percent of Egyptian networks have been taken offline. There’s at least one major ISP — Noor Group — up and running, the same one that hosts Egypt’s stock exchange.").


590744.html ("China’s state media have provided limited coverage of the unrest in Egypt, including the scores of reported deaths, the cutting of Internet and cellphone access, and President Hosni Mubarak’s appointment of a vice president.").

31. See id. ("Chinese authorities also stepped up their efforts to control the Internet after the "color revolutions" in the former Soviet Union in 2003-05, and the pro-democracy protests in Iran in 2009. They completely shut down Internet access in the northwestern Chinese region of Xinjiang for several months after riots there in 2009.").

32. Segura-Serrano, supra note 10, at 231.

33. S. 3480 § 249, 111th Cong. (2010); Chloe Albanesius, Lieberman Blocks Away from “Internet Kill Switch”, PC MAG (June 21, 2010, 3:19 PM), http://www.pcmag.com/article2/0,2817,2365393,00.asp (recounting that the controversy swirling around the bill “prompted many to dub [the] option an ‘Internet kill switch’”); Jon Orin, In Search of the Internet Kill Switch, TECH CRUNCH (Mar. 6, 2011), http://techcrunch.com/2011/03/06/in-search-of-the-internet-kill-switch/ (“It became known as the Internet ‘kill switch’ bill even though the words ‘kill’ and ‘switch’ are not found in the bill.”); Matthew Schaefer, How the Internet “Kill Switch” Bill Became the Bulwark of Internet Indepence, GROUND REP. (Feb. 21, 2011), http://www.groundreport.com/Media_and_Tech/How-the-Internet-Kill-Switch-Bill-Became-the-Bulwark/2934942 (noting that the bill “subject to a maelstrom of controversy” after being dubbed a kill switch); see also Declan McCullagh, Senators Propose Granting President Emergency Internet Power, CNET NEWS (June 10, 2010, 8:25 PM), http://news.cnet.com/8301-13578_3-20007418-38.html (recognizing “few limits on the president’s emergency power, which can be renewed indefinitely,” and noting industry concerns over “the potential for absolute power.”).


35. S. 3480 § 249; see Knowles, supra note 2 ("Championed by Sen. Joe Lieberman, the bill would give President Barack Obama . . . control to snuff out the Internet in one fell swoop during a so-called “cyber-emergency”.").


37. Id.

38. Id.
the “lines of code,” and consequently disabled the majority of Egypt’s Internet connectivity. 28

Egypt is not the only country that has disabled its inhabitants’ ability to connect to the Internet. Nepals and Burma have both experienced intranational government Internet shutdowns.29 In response to the Egyptian uprising, Chinese officials blocked information relating to the Egyptian revolt from its estimated four hundred and fifty-seven million Internet users.28 On a broader scale, the Chinese government completely disabled Internet connectivity in the Xinjiang region in 2009 following dissident political activity.30

These aforementioned international examples demonstrate that foreign governments have been successful, at least to a noteworthy degree, in disabling or limiting Internet use within their own borders. However, even if the United States had the ability to disable Internet access within its borders, it is unclear whether it would be legally able to do so, given the Nation’s rich history of protecting free speech and upholding the separation of powers. Arguably, the Internet is itself a distinctly American concept, built upon the “freedom of information and free flows of data.”31 Measures to constrict this freedom should be critically evaluated, even when balanced against the importance of safeguarding national security.

28. See id. ("[S]ome 93 percent of Egyptian networks have been taken offline. There’s at least one major ISP — Noor Group — up and running..."


30. See Jeremy Page, Beijing Blocks Protest Reports, WALL ST. J. (Jan. 31, 2011), http://online.wsj.com/article/SB100014240527487043270457613181077990744.html ("China’s state media have provided limited coverage of the unrest in Egypt, including the scores of reported deaths, the cutting of Internet and cellphone access, and President Hosni Mubarak’s appointment of a vice president.").

31. See id. ("Chinese authorities also stepped up their efforts to control the Internet after the ‘color revolutions’ in the former Soviet Union in 2003-05, and the pro-democracy protests in Iraq in 2009. They completely shut down Internet access in the northwestern Chinese region of Xinjiang for several months after riots there in 2009.").

32. Segura-Serrano, supra note 19, at 231.

II. The Proposed “Kill Switch” BILL

A. Provisions of the Bill

In 2010, legislation was introduced in the U.S. Senate specifying the conditions under which the government would have the ability to activate a kill switch.32 The proposed bill, “S.3480: Protecting Cyberspace as a National Asset Act,”33 would grant the President the power to disable the Internet in the event of an emergency.34 This bipartisan bill was co-sponsored by Senators on the Homeland Security and Governmental Affairs Committee: Maine Senator Susan Collins, the ranking Republican on the Committee,35 Connecticut Independent Senator Joseph Lieberman, the Committee Chairman,36 and Delaware Democratic Senator Tom Carper.37

This bill, which was approved by a Senate panel, would create a governmental agency called the National Center for Cybersecurity
and Communications ("NCCC"). The NCCC, which would operate under the auspices of the Department of Homeland Security, would have the broad power to control the Internet, including the ability to shut down the web for a 30-day period. The proposed agency would "oversee the U.S. Computer Emergency Readiness Team, which disseminates cybersecurity information from researchers and the government to the private sector." This bill would also create a White House Office of Cyberspace Policy to supervise all "instruments of national power relating to ensuring the security and resiliency of cyberspace," and enforce security standards governing the public and private sector established by the National Institute of Standards and Technology (NIST).

No one yet understands the bill's full possible ramifications. In fact, it may not be realistically feasible to implement, as the United States has more decentralized ISPs than Egypt. As a result of public outrage over the pending legislation, the new draft of the 221-page bill explicitly forbids the government from entirely disconnecting a user's computer from the Internet. The proposed bill stipulates that the President would have the power to shut down "critical infrastructure" during a devastating cyberattack on the country, or in anticipation of such an attack. This bill calls for the Department of Homeland Security to establish and maintain a list of systems or assets that constitute critical cyber-infrastructure. The Department would also be authorized to take action against privately-owned computer systems. The proposed legislation precludes judicial review for critical infrastructure, and requires the President to consult Congress before taking action.

The breadth of power that the proposed bill facially imparts is not without serious checks. According to Senator Lieberman, the legislation is limited to protecting only "the most critical infrastructures that Americans rely on in their daily lives—energy transmission, water supply, [and] financial services." The President may be precluded from taking action pursuant to the bill unless a cyberattack would cause more than twenty-five billion dollars in damages in the span of a year, kill more than 2,500 people, and force mass evacuations. Under the bill, the Executive's emergency actions are only authorized for thirty days, with potential thirty-day extensions.

These drastic restrictions make the possibility of action pursuant to the bill rather unlikely, or so one hopes. In order to constitute the kind of emergency covered by the proposed bill, the danger would need to be "a massive computer-virus or physical attack in which

39. S. 3480 § 242(a)(1); see Jessup, supra note 34.
40. S. 3480 § 242(a)(1); Zittrain and Sauter, supra note 29 (describing the structure of the proposed National Center for Cybersecurity and Communications).
41. S. 3480, § 249(b)(1); Jessup, supra note 34.
42. S. 3480 § 244; Zittrain and Sauter, supra note 29.
43. S. 3480 § 102(b)(9) ("The Director shall . . . coordinate and ensure, to the maximum extent practicable, that the standards and guidelines developed for national security systems and the standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) are complementary and unified.").
44. Jessup, supra note 34 ("The U.S. telecommunication industry is much more complex and far more decentralized than Egypt's. To do something similar in the U.S. would require a lot more than four phone calls.").
45. S. 3480 § 249(a)(3)(A); see Dechan McCullagh, Internet "Kill Switch" Bill Gets a Makeover, CNET (Feb. 18, 2011, 6:27 PM), http://news.cnet.com/8301-31921_3-20034717-281.html (describing the revised bill and its potential ramifications); see also Zittrain and Sauter, supra note 29 (stating that critical infrastructure protected by the bill is narrowly defined as "systems whose disruption or destruction would cause a mass casualty event which includes an extraordinary number of fatalities; severe economic consequences; mass evacuations with a prolonged absence; or severe degradation of national security capabilities, including intelligence and defense functions."). Most Web servers would not qualify as that type of infrastructure—nor would a small ISP.

46. S. 3480 § 249(a)(1); Suzanne Phan, Egypt Flips Internet Kill Switch, Congress Considers Similar Bill, News10 ABC (Feb. 2, 2011, 11:35 AM), http://www.news10.net/news/local/story.aspx?storyid=120866& PROVIDE=TOP ("The Bill wouldn't allow the president to actually shut down the Internet. But it would give him the ability to shut down 'critical infrastructure' if there was ever a serious cyber attack on the country.").
48. S. 3480 § 249(a)(3)(A); see McCullagh, supra note 45 ("The 221-page bill hands Homeland Security the power to issue decrees to certain privately-owned computer systems after the president declares a 'national cyberemergency.'").
49. Swartz, supra note 9.
50. McCullagh, supra note 45.
51. Id. (describing how Senators "hope" that Homeland Security will take a combination of these types of factors into consideration before utilizing the kill switch, however, these restraints are "nonbinding and [do not] actually appear in the legislation."); see also Swartz, supra note 9 (stating that the bill specifically does not grant the President power to act unless those factors are met, and the President would be empowered to "pinpoint what to clamp down on without causing economic damage to U.S. interests.").
52. S. 3480 § 249(b)(2); see also Zittrain and Sauter, supra note 29.
and Communications ("NCCC"). The NCCC, which would operate under the auspices of the Department of Homeland Security, would have the broad power to control the Internet, including the ability to shut down the web for a 30-day period. The proposed agency would "oversee the U.S. Computer Emergency Readiness Team, which disseminates cybersecurity information from researchers and the government to the private sector." This bill would also create a White House Office of Cyberspace Policy to supervise all "instruments of national power relating to ensuring the security and resiliency of cyberspace," and enforce security standards governing the public and private sector established by the National Institute of Standards and Technology (NIST).

No one yet understands the bill's full possible ramifications. In fact, it may not be realistically feasible to implement, as the United States has more decentralized ISPs than Egypt. As a result of public outrage over the pending legislation, the new draft of the 221-page bill explicitly forbids the government from entirely disconnecting a user's computer from the Internet. The proposed bill stipulates that the President would have the power to shut down "critical infrastructure" during a devastating cyberattack on the country, or in anticipation of such an attack. This bill calls for the Department of Homeland Security to establish and maintain a list of systems or assets that constitute critical cyber-infrastructure. The Department would also be authorized to take action against privately-owned computer systems. The proposed legislation precludes judicial review for critical infrastructure, and requires the President to consult Congress before taking action.

The breadth of power that the proposed bill facially imparts is not without serious checks. According to Senator Lieberman, the legislation is limited to protecting only "the most critical infrastructures that Americans rely on in their daily lives—energy transmission, water supply, [and] financial services." The President may be precluded from taking action pursuant to the bill unless a cyberattack would cause more than twenty-five billion dollars in damages in the span of a year, kill more than 2,500 people, and force mass evacuations. Under the bill, the Executive's emergency actions are only authorized for thirty days, with potential thirty-day extensions. These drastic restrictions make the possibility of action pursuant to the bill rather unlikely, or so one hopes. In order to constitute the kind of emergency covered by the proposed bill, the danger would need to be "a massive computer-virus or physical attack in which
ISPs stood idly by as malware spread like wildfire.

This makes the realistic necessity of enforcing the bill unclear. In the event of a catastrophe rising to the level specified in the proposed legislation, it is unlikely that governmental action would be able to mitigate the situation. ISPs would likely take measures on their own to counter any such adumbrated disasters, and arguably, the ISP’s engineers would already be in a better position to take action than the government. Yet the bill’s extra protection, even if never used, may be critical in the remote likelihood that a catastrophic event occurs and the ISPs are either unable or unwilling to take action.

B. The Legality of the “Kill Switch” Bill

1. The Power of the Executive Branch

The President may already possess the necessary authority to shut down Internet’s infrastructure without resorting to using the powers conferred by the proposed bill.

Under section 706 of the Communications Act of 1934, pursuant to a provision added in 1941, the President has the power to shut down “any facility or station for wire communication.” Thus, theoretically the President may lawfully take control of these infrastructures if a triggering event causes a “state of war.” In the wake of such an event, the federal government may control these facilities for up to six months.

The Department of Homeland Security has cited section 706 as “one of the authorities the President would rely on if the nation were under a catastrophe rising to the level specified in the proposed legislation, it is unlikely that governmental action would be able to mitigate the situation. ISPs would likely take measures on their own to counter any such adumbrated disasters, and arguably, the ISP’s engineers would already be in a better position to take action than the government.”

Yet the bill’s extra protection, even if never used, may be critical in the remote likelihood that a catastrophic event occurs and the ISPs are either unable or unwilling to take action.

53. Zittrain and Sauter, supra note 29.

54. Id. (in the event of a massive attack “it is not clear that government intervention would make any difference. The ISPs would already be doing everything they could to counter the attack. And there’s no reason to believe that the government would have any comparative advantage in understanding the situation better than the Internet engineers themselves.”)

55. See id. (describing how ISPs would be better suited to deal with a cyberattack, which leads to the inference that the government may only need to act if the ISPs are unable or unwilling to do so).

56. Id.

57. Communications Act of 1934 § 706; 47 U.S.C. § 606(d)(2011); Zittrain and Sauter, supra note 29 (“Section 706 of the Communications Act of 1934—written into the Act shortly after the 1941 attack on Pearl Harbor—gives the President the power to shut down “any facility or station for wire communication” or take federal control of such facilities in the event of a “state of war” and for up to six months after the expiration of such a state.”)

58. Zittrain and Sauter, supra note 29.


60. Notably, in congressional testimony, Phillip Reitinger, the former Deputy Undersecretary of the Department of Homeland Security, stated that “Congress and the Administration should work together to identify any needed adjustments to the [1934] Act, as opposed to developing overlapping legislation.”

The Founding Fathers’ caution towards the power of the federal government is reflected in the spirit of the Constitution. Each branch is limited to the powers bestowed upon it by the Constitution, in a system of checks and balances. The Constitution imbuies each of the three branches of government with inherent but limited powers. Article 1 imbues the Legislature with power; Article 2, the Executive; and Article 3, the Judiciary.

In Youngstown Sheet & Tube Co. v. Sawyer, Justice Jackson’s concurring opinion demarcated a tripartite model of the separation of powers, stipulating that the Executive’s powers are at their strongest when supported by the explicit authority of the legislature.

Under this constitutional analysis, the President’s authority to disable Internet connectivity should the kill switch bill become law is likely justified under the powers delineated in Article I and Article II, in conjunction with Section 706 of the 1934 Act.

However, the constitutional rights afforded to citizens must continue to check the breadth of the Executive’s powers, which...
ISP's stood idly by as malware spread like wildfire. This makes the realistic necessity of enforcing the bill unclear. In the event of a catastrophe rising to the level specified in the proposed legislation, it is unlikely that governmental action would be able to mitigate the situation. ISP's would likely take measures on their own to counter any such adumbrated disasters, and arguably, the ISP's engineers would already be in a better position to take action than the government. Yet the bill's extra protection, even if never used, may be critical in the remote likelihood that a catastrophic event occurs and the ISP's are either unable or unwilling to take action.

B. The Legality of the "Kill Switch" Bill
1. The Power of the Executive Branch

The President may already possess the necessary authority to shut down Internet's infrastructure without resorting to using the powers conferred by the proposed bill. Under section 706 of the Communications Act of 1934, pursuant to a provision added in 1941, the President has the power to shut down "any facility or station for wire communication." Thus, theoretically the President may lawfully take control of those infrastructures if a triggering event causes a "state of war." In the wake of such an event, the federal government may control these facilities for up to six months. The Department of Homeland Security has cited section 706 as "one of the authorities the President would rely on if the nation were under a cyberattack." Notably, in congressional testimony, Phillip Reitinger, the former Deputy Undersecretary of the Department of Homeland Security, stated that "Congress and the Administration should work together to identify any needed adjustments to the [1934] Act, as opposed to developing overlapping legislation." The Founding Fathers' caution towards the power of the federal government is reflected in the spirit of the Constitution. Each branch is limited to the powers bestowed upon it by the Constitution, in a system of checks and balances. The Constitution imbues each of the three branches of government with inherent but limited powers. Article 1 imbues the Legislature with power; Article 2, the Executive; and Article 3, the Judiciary. In Youngstown Sheet & Tube Co. v. Sawyer, Justice Jackson's concurrence opinion denounced a tripartite model of the separation of powers, stipulating that the Executive's powers are at their strongest when supported by the explicit authority of the legislature. Under this constitutional analysis, the President's authority to disable Internet connectivity should the kill switch bill become law is likely justified under the powers delineated in Article I and Article II, in conjunction with Section 706 of the 1934 Act.

However, the constitutional rights afforded to citizens must continue to check the breadth of the Executive's powers, which

53. Zittrain and Sauter, supra note 29.
54. Id. (in the event of a massive attack "it's not clear that government intervention would make any difference. The ISPs would already be doing everything they could to counter the attack. And there's no reason to believe that the government would have any comparative advantage in understanding the situation better than the Internet engineers themselves.").
55. See id. (describing how ISPs would be better suited to deal with a cyberattack, which leads to the inference that the government may only need to act if the ISPs are unable or unwilling to do so).
56. Id.
57. Communications Act of 1934 § 706; 47 U.S.C. § 606(d)(2011); Zittrain and Sauter, supra note 29 ("Section 706 of the Communications Act of 1934—written into the Act shortly after the 1941 attack on Pearl Harbor—gives the President the power to shut down "any facility or station for wire communication" or take federal control of such facilities in the event of a "state of war" and for up to six months after the expiration of such a state.").
58. Zittrain and Sauter, supra note 29.
Executive branch must confine use of its emergency powers unless the powers of the kill switch bill? If the corresponding likelihood of the attack need to be in order to trigger Executive Powers would be a "blank check" 79 to encroach on the separation of powers by disproportionately strengthening the power of the Executive. 71

When considering the proposed kill switch bill under the provisions of Hamdi, it is clear that individual rights limit the Executive’s powers, even in the case of exigent circumstances. However, Hamdi does not delineate the extent to which the Executive’s powers can be strengthened in a time of peril or when exactly that peril is sufficient to justify otherwise extra-legal action. While the proposed terms of the kill switch bill include a high threshold of collateral damage to trigger the Executive’s interference with Internet connectivity, some might argue that the resulting broad Executive Powers would be a "blank check" forbidden under Hamdi. If just one keystroke can render severe damage, how high would the corresponding likelihood of the attack need to be in order to trigger the powers of the kill switch bill? 71

Justices Souter, in his Hamdi concurrence, emphasized that the Executive branch must confine use of its emergency powers unless

67. Hamdi v. Rumsfeld, 542 U.S. 507, 533 (2004) ("We therefore hold that a citizen-detainee seeking to challenge his classification as an enemy combatant must receive notice of the factual basis for his classification[]. . . . [E]nemy-combatant proceedings may be tailored to alleviate their uncommon potential to burden the Executive at a time of ongoing military conflict.").

68. Id. at 536-37 (noting that “it would turn our system of checks and balances on its head to suggest that a citizen could not make his way to court with a challenge to the factual basis for his detention.”).

69. Id. at 530 ("[H]istory and common sense teach us that an unchecked system of detention carries the potential to become a means for oppression and abuse of others who do not present that sort of threat.").

70. Id. at 536 ("We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation’s citizens.").

71. Id. ("Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.").

supported by specific instances of emergencies. However, in the age of the Internet, the question becomes how the Government can determine whether a specific emergency is occurring, when many cyberattacks may occur simultaneously. Given the ease and speed in which attacks can be perpetrated, it may be unrealistic for the Executive Branch to ask Congress for permission to act or consult with the Attorney General regarding the legality of the intended measures.

2. Protections Granted by the First Amendment

i. The Individual Right

In addition to implicating the scope of the Executive power, the kill switch bill may impede on an individual’s First Amendment right to post content on the Internet. 75 As the measures proposed by the bill would allow the NCCC to shut down the Internet for a thirty-day period, 74 these concerns also may encompass the ability of Americans to access another person’s writing. For example, nearly sixty percent of Americans access the news from their computers. 75

Many civil rights organizations have questioned the kill switch bill’s effect on American freedom and civil liberties. 76 The American Civil Liberty Union’s legislative counsel, Michelle Richardson, claimed that the issue surrounding the proposed bill was never that a literal kill switch could eviscerate Internet access completely. 77 Richardson explained that “[t]he question is bigger than that. It’s generally, can the government interfere with communications . . . The question is: Are there significant protections in there?” 78 Similarly, the Electronic Frontier Foundation’s legal director and general counsel, Cindy Cohn, stated that what happened in Egypt “highlights the dangers of any

72. Id. at 541 (Souter, J. concurring) (noting that in the absence of a specific reason for detention, the detainee, in the matter at hand, may be entitled to release).

73. See Jessup, supra note 34 (noting the concern that various interest groups have voiced that “the measure, if it became law, might be used to censor the internet”).

74. S. 3480 § 242; see Jessup, supra note 34.

75. Jessup, supra note 34 (“at least 60% of Americans get their daily news from the Internet.”).

76. Id. (“About two dozen groups, including the American Civil Liberties Union, the American Library Association, Electronic Frontier Foundation and Center for Democracy &Technology, were skeptical enough to file an open letter opposing the idea.”).

77. McCullagh, supra note 45 (“The ACLU’s Richardson believes the problem was never a ‘kill switch.’”).

78. Id.

79. Id.
expand in times of danger and warfare. In Hamdi v. Rumsfeld, the Supreme Court ruled, inter alia, that an enemy combatant must receive notice of the allegations against him; however, the government may tailor these proceedings to help alleviate the burden that this type of trial places on the government. The plurality stressed the need to balance governmental concerns with those of individuals. The Hamdi Court stated that "history and common sense" have demonstrated that "war is not a blank check" to encroach on the separation of powers by disproportionately strengthening the power of the Executive. When considering the proposed kill switch bill under the provisions of Hamdi, it is clear that individual rights limit the Executive's powers, even in the case of exigent circumstances. However, Hamdi does not delineate the extent to which the Executive's powers can be strengthened in a time of peril or when exactly that peril is sufficient to justify otherwise extra-legal action. While the proposed terms of the kill switch bill include a high threshold of collateral damage to trigger the Executive's interference with Internet connectivity, some might argue that the resulting broad Executive Powers would be a "blank check" forbidden under Hamdi. If just one keystroke can render severe damage, how high would the corresponding likelihood of the attack need to be in order to trigger the powers of the kill switch bill?

Justices Souter, in his Hamdi concurrence, emphasized that the Executive branch must confine use of its emergency powers unless supported by specific instances of emergencies. However, in the age of the Internet, the question becomes how the Government can determine whether a specific emergency is occurring, when many cyberattacks may occur simultaneously. Given the ease and speed in which attacks can be perpetrated, it may be unrealistic for the Executive Branch to ask Congress for permission to act or consult with the Attorney General regarding the legality of the intended measures.

2. Protections Granted by the First Amendment

i. The Individual Right

In addition to implicating the scope of the Executive power, the kill switch bill may impede on an individual's First Amendment right to post content on the Internet. As the measures proposed by the bill would allow the NCCIC to shut down the Internet for a thirty-day period, these concerns also may encompass the ability of Americans to access another person's writing. For example, nearly sixty percent of Americans access the news from their computers. Many civil rights organizations have questioned the kill switch bill's effect on American freedom and civil liberties. The American Civil Liberty Union's legislative counsel, Michelle Richardson, claimed that the issue surrounding the proposed bill was never that a literal kill switch could evict Americans from the Internet completely. Richardson explained that "[t]he question is bigger than that. It's generally, can the government interfere with communications . . . The question is: Are there significant protections in there?" Similarly, the Electronic Frontier Foundation's legal director and general counsel, Cindy Cohn, stated that what happened in Egypt "highlights the dangers of any

67. Hamdi v. Rumsfeld, 542 U.S. 507, 533 (2004) ("We therefore hold that a citizen-detainee seeking to challenge his classification as an enemy combatant must receive notice of the factual basis for his classification,[...]. . . . [E]nemy-combatant proceedings may be tailored to alleviate the unknown potential to burden the Executive at a time of ongoing military conflict.").

68. Id. at 536-37 (noting that "it would turn our system of checks and balances on its head to suggest that a citizen could not make his way to court with a challenge to the factual basis for his detention.").

69. Id. at 530 ("[H]istory and common sense teach us that an unchecked system of detention carries the potential to become a means for oppression and abuse of others who do not present that sort of threat.").

70. Id. at 536 ("We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nations' citizens.").

71. Id. ("Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.").

72. Id. at 541 (Souter, J. concurring) (noting that in the absence of a specific reason for detention, the detainee, in the matter at hand, may be entitled to release).

73. See Jessup, supra note 34 (noting the concern that various interest groups have voiced that "the measure, if it became law, might be used to censor the internet").

74. S. 3480 § 242; see Jessup, supra note 34.

75. Jessup, supra note 34 ("at least 60% of Americans get their daily news from the Internet.").

76. Id. ("About two dozen groups, including the American Civil Liberties Union, the American Library Association, Electronic Frontier Foundation and Center for Democracy & Technology, were skeptical that the measure, if it became law, might be used to censor the internet").

77. McCullagh, supra note 45 ("The ACLU's Richardson believes the problem was never a 'kill switch.'").

78. Id.
government having unchecked power over our Internet infrastructure.\textsuperscript{77}

The issue then becomes whether there are grounds for these concerns, and to what extent the Constitution protects a citizen’s First Amendment freedom of speech and expression in regard to the Internet. The First Amendment states, “Congress shall make no law...”\textsuperscript{78} abridging the freedom of speech,\textsuperscript{79} but does this text actually protect the right to access the Internet? “Under the public forum doctrine, U.S. courts impose on the government the affirmative obligation to make public facilities available for persons wanting to exercise their free speech rights.”\textsuperscript{80} But, can the kill switch bill meet judicial scrutiny under the First Amendment? To answer these questions, this Article explores the case law that defines the parameters of accepted limitations on free speech under the First Amendment.

\textbf{i. Applicable Tests for First Amendment Limitations}

In Whitney v. California, the Supreme Court held that there is no absolute freedom of speech.\textsuperscript{81} Whitney sets forth the standard that states do not violate an individual’s Constitutional rights when they prohibit speech that may “incite to crime, disturb the public peace, or endanger the foundations of organized government and threaten the overthrow by unlawful means.”\textsuperscript{82} In his celebrated concurrence, Justice Brandeis expounded that freedom of speech rights are “fundamental [but] they are not in their nature absolute.”\textsuperscript{83} He stressed that “fear of serious injury cannot alone justify suppression of free speech and assembly,” and to justify such suppression, the implicating speech must pose an imminent danger which is “relatively serious.”\textsuperscript{84} In accordance with the standard set forth in Whitney, the kill switch bill would likely meet the necessary standards to render First Amendment protections inapplicable. Since the Executive can only rely upon this legislation in times of, or in the fear of, catastrophic calamity, the Whitney standard would almost certainly be met if the Executive were correct in his or her assessment of the likelihood of danger on the basis of known information at the time of the threat.

The kill switch bill may further be proven legal pursuant to the historical standards set forth that the government must meet before encroaching upon First Amendment rights. In evaluating when dangerous conditions override First Amendment concerns, the Supreme Court in Schenck v. United States created and applied the “clear and present danger” test.\textsuperscript{85} This Court noted that “[w]hen a nation is at war many things that might be said in times of peace are such a hindrance to its effort that their utterance will not be endured[.]”\textsuperscript{86} This allows the abridgement of free speech when the resulting advocated action is one that Congress has the right to prevent.\textsuperscript{87} In subsequent decisions, the Supreme Court has held that a causal link between the speech and disturbance is necessary when abridging First Amendment rights, and that the speech must have more than a tenuous relationship to the feared repercussions.\textsuperscript{88} While this is a common standard for evaluating the abridgement of First Amendment rights, a dormant, yet not overruled test put forth in Dennis v. United States, focuses on whether the “gravity of the evil,”

\textsuperscript{77} Egypt’s Internet Blackout Revives U.S. “Kill Switch” Debate, HOMELAND SECURITY NEWS WIRE (Feb. 7, 2011), http://www.homelandsecuritynewswire.com/egypts-internet-blackout-revives-us-kill-switch-debate (“The lesson of Egypt is that no one, not even the President of the United States, should be given the power to turn off the Internet.”).

\textsuperscript{78} U.S. CONST. amend. I.

\textsuperscript{79} Segura-Serrano, supra note 19, at 261.

\textsuperscript{80} Whitney v. California, 274 U.S. 357, 371 (1927) (“The freedom of speech which is secured by the Constitution does not confer an absolute right to speak, without responsibility, whatever one may choose, or an unrestricted and unbridled license giving immunity for every possible use of language and preventing the punishment of those who abuse this freedom; and that a State in the exercise of its police power may punish those who abuse this freedom by utterances iminical to the public welfare, tending to incite to crime, disturb the public peace, or endanger the foundations of organized government and threaten its overthrow by unlawful means, is not open to question.”).

\textsuperscript{81} Id. at 371.

\textsuperscript{82} Id. at 373 (Brandeis, J., concurring).
government having unchecked power over our Internet infrastructure.  

The issue then becomes whether there are grounds for these concerns, and to what extent the Constitution protects a citizen's First Amendment freedom of speech and expression in regard to the Internet. The First Amendment states, "Congress shall make no law ... abridging the freedom of speech," but does this text actually protect the right to access the Internet? Under this [public forum] doctrine, U.S. courts impose on the government the affirmative obligation to make public facilities available for persons wanting to exercise their free speech rights. But, can the kill switch bill meet judicial scrutiny under the First Amendment? To answer these questions, this Article explores the case law that defines the parameters of accepted limitations on free speech under the First Amendment.

ii. Applicable Tests for First Amendment Limitations

In Whitney v. California, the Supreme Court held that there is no absolute freedom of speech. Whitney sets forth the standard that states do not violate an individual's Constitutional rights when they prohibit speech that may "incite to crime, disturb the public peace, or endanger the foundations of organized government and threaten the overthrow by unlawful means." In his celebrated concurrence, Justice Brandeis expounded that freedom of speech rights are "fundamental [but] they are not in their nature absolute." He stressed that "fear of serious injury cannot alone justify suppression of

free speech and assembly," and to justify such suppression, the implicating speech must pose an imminent danger which is "relatively serious." In accordance with the standard set forth in Whitney, the kill switch bill would likely meet the necessary standards to render First Amendment protections inapplicable. Since the Executive can only rely upon this legislation in times of, or in the fear of, catastrophic calamity, the Whitney standard would almost certainly be met if the Executive were correct in his or her assessment of the likelihood of danger on the basis of known information at the time of the threat.

The kill switch bill may further be proven legal pursuant to the historical standards set forth that the government must meet before encroaching upon First Amendment rights. In evaluating when dangerous conditions override First Amendment concerns, the Supreme Court in Schenck v. United States created and applied the "clear and present danger" test. This Court noted that "[w]hen a nation is at war many things that might be said in times of peace are such a hindrance to its effort that their utterance will not be endured[.]" This allows the abridgement of free speech when the resulting advocated action is one that Congress has the right to prevent. In subsequent decisions, the Supreme Court has held that a causal link between the speech and disturbance is necessary when abridging First Amendment rights, and that the speech must have more than a tenuous relationship to the feared repercussions. While this is a common standard for evaluating the abridgement of First Amendment rights, a dormant, yet not overruled test put forth in Dennis v. United States, focuses on whether the "gravity of the evil,"
discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger. 94

The kill switch legislation would likely comply with the Schenck standard and meet the stringency of the conditions necessary to trigger the Executive’s power under the proposed bill. However, the analysis is less clear under Dennis. Although attackers may intend to cause damage serious enough to meet the first prong of the test, the probability of the danger coming from its fruition would need to be high enough to merit resorting to the powers granted in the bill. Considering the ease with which cyberattacks can occur, the Executive may consider multiple attacks “probable.” Thus, it is unclear when governmental action, taken in conjunction with the proposed bill, could lawfully occur under the second prong95 of the Dennis test.

The modern doctrine, put forth in Brandenburg v. Ohio, concerns the dangers of political rhetoric and the countervailing First Amendment rights.96 In Brandenburg, the Court found that the government could not suppress speech unless the speech in question aimed to incite “imminent lawless action.”97 However, this standard is likely inapplicable to the proposed bill because political speech would not be an issue unless it somehow involved activist terrorists collaborating to carry out a cyberattack for political causes. Engaging in political speech would not be considered extreme enough to warrant limiting access to the Internet under the kill switch bill. Accordingly, the Schenck and Dennis tests remain the benchmark standard by which this legislation should be evaluated. Thus, the judiciary is not likely to declare the bill unconstitutional pursuant to First Amendment concerns. Even if the political action triggered the kill switch powers, the bill still meets the Constitutional standard articulated in Brandenburg because the potential calamities would likely be imminent and unlawful.

91. Id. ("[T]he gravity of the evil.").
92. Id. ("[D]iscounted by its improbability.").
93. Brandenburg v. Ohio, 395 U.S. 444, 448 (1969) (discussing whether an act can punish advocating or teaching violence as opposed to punishing the actual intent to cause criminal acts).
94. Id. at 447 ("[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.").
95. N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam) (explaining that the government must show justification when it encroaches upon First Amendment free speech rights).
96. Id. at 714-15 (Black, J., concurring) (describing the government’s attempt to censor newspapers).
97. Id. at 714 (per curiam) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity... The Government ‘thus carries a heavy burden of showing justification for the imposition of such a restraint.’").
98. Id. at 717 (Black, J., concurring) ("In the First Amendment the Founding Fathers gave the free press the protection it must have to fulfill its essential role in our democracy.").
99. Id. at 714 (per curiam) (noting that the government must show justification for placing a restraint on First Amendment free speech).
discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger.\textsuperscript{94}

The kill switch legislation would likely comply with the Schenck standard and meet the stringency of the conditions necessary to trigger the Executive’s power under the proposed bill. However, the analysis is less clear under Dennis. Although attackers may intend to cause damage serious enough to meet the first prong of the test,\textsuperscript{96} the probability of the danger coming from its fruition would need to be high enough to merit resorting to the powers granted in the bill. Considering the ease with which cyberattacks can occur, the Executive may consider multiple attacks “probable.” Thus, it is unclear when governmental action, taken in conjunction with the proposed bill, could lawfully occur under the second prong\textsuperscript{97} of the Dennis test.

The modern doctrine, put forth in Brandenburg v. Ohio, concerns the dangers of political rhetoric and the countervailing First Amendment rights.\textsuperscript{98} In Brandenburg, the Court found that the government could not suppress speech unless the speech in question aimed to incite “imminent lawless action.”\textsuperscript{99} However, this standard is likely inapplicable to the proposed bill because political speech would not be an issue unless it somehow involved activist terrorists collaborating to carry out a cyberattack for political causes. Engaging in political speech would not be considered extreme enough to warrant limiting access to the Internet under the kill switch bill. Accordingly, the Schenck and Dennis tests remain the benchmark standard by which this legislation should be evaluated. Thus, the judiciary is not likely to declare the bill unconstitutional pursuant to First Amendment concerns. Even if the political action triggered the kill switch powers, the bill still meets the Constitutional standard articulated in Brandenburg because the potential calamities would likely be imminent and unlawful.

\textsuperscript{90} Denis v. United States, 341 U.S. 494, 510 (1951).
\textsuperscript{91} Id. (“[T]he gravity of the evil[,]”).
\textsuperscript{92} Id. (“[D]iscounted by its improbability[,]”).
\textsuperscript{93} Brandenburg v. Ohio, 395 U.S. 444, 448 (1969) (discussing whether an act can punish advocating or teaching violence as opposed to punishing the actual intent to cause criminal acts).
\textsuperscript{94} Id. at 447 (“[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.”).
connectivity appears likely to withstand scrutiny under the New York Times legal analysis.

In Reno v. ACLU, the Supreme Court considered the issue of censorship of Internet speech and held that the CDA of 1996 was a violation of the First Amendment.\(^\text{100}\) The Court declared that the Internet does not "invade an individual's home" but users do access it through their own free will.\(^\text{101}\) The Court found that the CDA did not pass strict scrutiny because less restrictive means could not have been available other than that utilized by the statute.\(^\text{102}\) Thus, the Internet receives stronger First Amendment protection than broadcast media.\(^\text{103}\)

The kill switch bill likely would withstand judicial consideration under Reno. It is possible that the Supreme Court may determine that the ends of protecting the nation from calamity warranted the means set forth in the proposed legislation. While the triggering events are undoubtedly serious, the question becomes whether a more tailored method of protecting critical infrastructure exists without granting the Executive additional authority to interfere with Internet connectivity. This question warrants serious evaluation. Nevertheless, it would be expected that the judiciary would uphold the bill, given the extenuating and extreme triggering circumstances.

iv. Commercial speech

The proposed kill switch bill may nevertheless violate an individual's right to engage in commercial speech. In addition to considering the free speech rights of individuals, the courts also evaluate an individual's right under this First Amendment rubric. Companies use the Internet to run their businesses and advertise. Although advertising is generally protected by the First Amendment, the Constitution "affords a lesser protection to commercial speech than to other constitutionally guaranteed expression."\(^\text{104}\) To evaluate commercial speech, courts use the test set forth in Central Hudson.

---

100. Reno v. ACLU, 521 U.S. 844, 885 (1997) (affording the same constitutional protections to the Internet as are provided to other types of speech).

101. Id. at 869 ("[C]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'").

102. Id. at 870 ("We are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.").

103. See id. at 866 ("Relying on the premise that "of all forms of communication" broadcasting has received the most limited First Amendment protection.").

connectivity appears likely to withstand scrutiny under the New York Times legal analysis.

In *Reno v. ACLU*, the Supreme Court considered the issue of censorship of Internet speech and held that the CDA of 1996 was a violation of the First Amendment.100 The Court declared that the Internet does not "invade an individual's home" but users do access it through their own free will.101 The Court found that the CDA did not pass strict scrutiny because less restrictive means could not have been available other than that utilized by the statute.102 Thus, the Internet receives stronger First Amendment protection than broadcast media.103

The switch bill likely would withstand judicial consideration under *Reno*. It is possible that the Supreme Court may determine that the ends of protecting the nation from calamity warranted the means set forth in the proposed legislation. While the triggering events are undoubtedly serious, the question becomes whether a more tailored method of protecting critical infrastructure exists without granting the Executive additional authority to interfere with Internet connectivity. This question warrants serious evaluation. Nevertheless, it would be expected that the judiciary would uphold the bill, given the extenuating and extreme triggering circumstances.

iv. Commercial speech

The proposed kill switch bill may nevertheless violate an individual's right to engage in commercial speech. In addition to considering the free speech rights of individuals, the courts also evaluate an individual's right under this First Amendment rubric. Companies use the Internet to run their businesses and advertise. Although advertising is generally protected by the First Amendment, the Constitution "affords a lesser protection to commercial speech than to other constitutionally guaranteed expression."104 To evaluate commercial speech, courts use the test set forth in *Central Hudson*.

100. *Reno v. ACLU*, 521 U.S. 844, 885 (1997) (affording the same constitutional protections to the Internet as are provided to other types of speech).

101. *Id.* at 869 ("[C]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'").

102. *Id.* at 870 ("We are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.").

103. See *id.* at 866 ("Relying on the premise that "of all forms of communication" broadcasting has received the most limited First Amendment protection.").


Gas & Electric Corp. v. Public Service Communication.105 In *Central Hudson*, the Court held that the government may regulate commercial speech if the regulation directly advances an important interest and is no more restrictive of speech than necessary.106 The kill switch bill meets this standard. First, as previously discussed, if the kill switch bill does not violate the free speech rights of an individual, it probably would be lawful under the lesser standard used to protect commercial speech. Second, the bill would likely meet the *Central Hudson* test because it would be no more restrictive of speech than necessary and would advance the interest of national security protection.

Moreover, while *Central Hudson* concerns the specific right to advertise, the kill switch bill would not affect the contents of the advertisements themselves but rather the vehicle through which they advertise. As such, the bill would not deny advertisers the right to promote their products but only their ability to market those products on the Internet. Hence, this analysis is likely not the appropriate First Amendment test and other legal frameworks should be applied.

v. Media

The First Amendment standards regarding free speech in media do not apply to the kill switch bill. These standards are put forth in *Red Lion v. FCC*, in which the Supreme Court evaluated the constitutionality of a FCC regulation that mandated broadcasters to notify individuals they defamed in their program and accord these individuals an opportunity to respond.107 The Court affirmed the constitutionality of the FCC regulation, holding that those who obtain licenses to broadcast must comply with the applicable conditions to retain that license.108 However, broadcast media is distinguishable from the Internet, as the unique characteristics of the
Internet include that it is not limited to a finite number of individuals or organizations who can post, nor are licenses necessary for its use. The Supreme Court affords more protection under the First Amendment to the rights of newspapers as opposed to those of licensed broadcasters. In *Miami Herald Publishing Co. v. Tornillo*, the Supreme Court held that a Florida law that required newspapers to grant equal coverage to political candidates was an unlawful violation of the freedom of the press. The Court explained that the First Amendment applies to newspapers because they are "more than a passive receptacle or conduit for news, comment, and advertising." The Court clarified its decision by explaining that "the choice of material to go into a newspaper . . . constitutes the exercise of editorial control and judgment," and it "has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time." Although, as envisioned under the kill switch bill, the regulation of the Internet may impede the media's ability to disseminate information, *Tornillo* cannot be used to analyze the legality of the bill. *Tornillo* represents the First Amendment as it applies to print media and grants strong protection to the content of newspapers. As was the case with the *Red Lion* broadcasting example, the kill switch bill is distinguished from *Tornillo*. *Tornillo* concerns the right of the media to choose its subject matter in accordance with the law, whereas the bill would affect the general ability to disseminate information on the Internet. In essence, *Tornillo* focuses on what information can be communicated *ipso facto* while the appropriate discussion of the bill should focus on the ability to express the material through the Internet. As such, the analysis of this bill in conjunction with the freedom of expression enjoyed by the media is inappropriate.

### III. Conclusion

In the modern technological era, cyberattacks continue to be a real and serious threat. The proposed kill switch bill attempts to bar Internet connectivity in response to certain anticipated national security threats. Considering the existing Executive powers under the 1934 Communications Act in conjunction with congressional approval for the bill, this legislation is within the scope of the Executive's power. Additionally, the First Amendment's high threshold is unlikely to trigger action under the bill, which leads to the conclusion that evaluation under this amendment is unnecessary.

**Acknowledgements**

The author wishes to thank Jennifer Shkabatur for her thought-provoking suggestions and for inspiring the author's interest in Internet law. She also wishes to express gratitude to Lee Medows and A. Michal Medows for their encouragement. This scholarship is dedicated in memory of her father, Dr. Gary S. Medows.
Internet include that it is not limited to a finite number of individuals or organizations who can post, nor are licenses necessary for its use. The Supreme Court affords more protection under the First Amendment to the rights of newspapers as opposed to those of licensed broadcasters. In *Miami Herald Publishing Co. v. Tornillo*, the Supreme Court held that Florida law that required newspapers to grant equal coverage to political candidates was an unlawful violation of the freedom of the press. The Court explained that the First Amendment applies to newspapers because they are "more than a passive receptacle or conduit for news, comment, and advertising." The Court clarified its decision by explaining that "the choice of material to go into a newspaper . . . constitute[s] the exercise of editorial control and judgment," and it "has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time." Although, as envisioned under the kill switch bill, the regulation of the Internet may impede the media's ability to disseminate information, *Tornillo* cannot be used to analyze the legality of the bill. *Tornillo* represents the First Amendment as it applies to print media and grants strong protection to the content of newspapers.

As was the case with the Red Lion broadcasting example, the kill switch bill is distinguished from *Tornillo*. *Tornillo* concerns the right of the media to choose its subject matter in accordance with the law, whereas the bill would affect the general ability to disseminate information on the Internet. In essence, *Tornillo* focuses on what information can be communicated *ipsa facto* while the appropriate discussion of the bill should focus on the ability to express the material through the Internet. As such, the analysis of this bill in conjunction with the freedom of expression enjoyed by the media is inappropriate.

III. CONCLUSION

In the modern technological era, cyberattacks continue to be a real and serious threat. The proposed kill switch bill attempts to bar Internet connectivity in response to certain anticipated national security threats. Considering the existing Executive powers under the 1934 Communications Act in conjunction with congressional approval for the bill, this legislation is within the scope of the Executive's power. Additionally, the First Amendment's high threshold is unlikely to trigger action under the bill, which leads to the conclusion that evaluation under this amendment is unnecessary.

Acknowledgements

The author wishes to thank Jennifer Shkabatur for her thought-provoking suggestions and for inspiring the author's interest in Internet law. She also wishes to express gratitude to Lee Medows and A. Michal Medows for their encouragement. This scholarship is dedicated in memory of her father, Dr. Gary S. Medows.