https://doi.org/10.48009/1_iis_2013_54-60
Issues in Information Systems
Volume 14, Issue 1, pp.54-60, 2013

INTERNET FREEDOM POLICY VS. CYBER-CENSORSHIP

Janusz Ochota, D. Sc., Robert Morris University, jxost9@mail.rmu.edu
Matthew R. Kisow, D. Sc., NSABP Foundation, Inc., matt.kisow@nsabp.org

ABSTRACT

In late 2010 a revolutionary wave of demonstrations began in the Arab world; starting in Tunisia a series of protests and civil unrest spread across northern Africa and into many Middle Eastern countries. The overwhelming use of social media was instrumental in sparking many of these protests. In an effort to curtail these protests the governments in these countries began to aggressively censor or eliminate their citizen's access to the Internet. After the Iranian protest movement in 2009, the U.S. State Department announced its "Internet Freedom Policy" where the dissidents of oppressive regimes were supplied the tools and resources necessary to report the human rights violations of their countries leaders to the world. Admits this U.S. state department policy however; lawmakers in all branches of government have sought to curtail their own citizen's access to the Internet, with the proposal of laws and regulation aimed at censorship. Two proposed bills; SOPA and PIPA have sought to forgo many of the due process statutes of the rule of law and the first amendment right to the freedom of speech.

Keywords: Protecting Cyberspace as a National Asset Act, SOPA, PIPA, CISPA, ACTA, Internet Freedom Policy, Cyber-Censorship and Internet

INTRODUCTION

Originally designed to withstand a catastrophic communications failure the Advanced Research Projects Agency Network (ARPANET) was established in 1969 by linking research universities essential to the strategic defense of the United States [6, 19, 20, 25, 43]. It was through this openness of scientific research that the ARPANET serviced continued to evolve linking government agencies and research institutions around the world. It was this openness that that led the United States congress to pass legislation opening the Internet to the general public in 1996, with a hands-off attitude [6, 25, 43].

The Internet continues to accommodate openness and freedom by enabling individuals to virtually assemble and associate with their peers [15]. The freedom to promote, pursue and defend the interests that are common to a group of individuals has been paramount in bringing freedom to those in once closed societies and oppressive regimes bringing a voice to those who may not have otherwise had one [15, 23, 27, 40, 44]. In the same way the First Amendment to the United States Constitution has prevented congress from abridging the freedom of speech and the freedom of assembly.

The individual freedom and openness of the Internet is now under attack. Legislation is circulating through the United States House of Representatives and the United States Senate; seeking to prevent the theft of "government information" and "intellectual property" by forcing Internet Service Providers (ISP's) to censor the Internet from its customers and eliminating online privacy by forcing ISP's to log the actions of their customers [14, 27, 36, 44].

Our online personal liberties and freedoms are under attack. Well-funded special interest groups continue to ratchet up pressure on our congressional leaders [1, 14, 15, 27, 36]. We cannot stand idly by as the Internet is censored[11, 36]. We the people need stand up to the special interest groups contact our senators and congressional leaders because the individual liberty that the Internet provides mandates our urgent attention.

PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT

In June 2010, the "Protecting Cyberspace as a National Asset Act of 2010" also known as S. 3480 was introduced as an attempt to increase cyber security to prevent a potentially debilitating cyber-attack on the United States' telecommunications infrastructure [12, 13]. The "Protecting Cyberspace as a National Asset Act of 2010" was introduced in the U.S. Senate by Connecticut Senator Joseph Lieberman and Maine Senator Susan Collins. This bill

proposed the creation of the Office of Cyberspace Policy and the National Center for Cyber security and Communications (NCCC) within the already existing Department of Homeland Security.

The bill permitted emergency counter-measures in case of large-scale cyber-attacks on the nation's telecommunications infrastructure, financial industry and business sector. Numerous versions of S. 3480 had granted authority to the President of the United States to shutdown part of the Internet indefinitely without Congressional oversight. This power to flip the Internet "kill switch," was later amended to a maximum of 120 days after public outcry over Senator Joe Lieberman's inflammatory comments citing China's similar policy [28, 31].

This bill not only afforded the Presidential authority over critical Internet infrastructure during a national "cyber-emergency," it also affords the government the ability to determine what constitutes critical infrastructure [10, 11, 12, 26]. The amended version of the bill further expanded the definition to include providers of information technology. It is this inclusion that places the government's definition of critical infrastructure beyond judicial review [12, 26, 28]. Because the Internet's networks are substantially more than a complex communications system covered under the Communications Act of 1934 [9] and the Telecommunications Act of 1996 [8], recognizing – and protecting – their now-vital role in social communication is increasingly imperative. Interaction through virtual communities has become a primary means of human assembly crossing most cultural and political boundaries on a global scale. Therefore this level of Executive Branch power over the lives of its citizens is antithetical to the First Amendment and the nation's most basic freedoms – freedom of speech and freedom of assembly. The ability of the President of the United States to institute a "cyber-emergency" shutting down part-of or all Internet communication is akin to the President establishing martial law.

The Protecting Cyberspace as a National Asset Act of 2010 [12, 26] comes at a time when there is a global consciousness of the dignity of man that can be achieved through free and just societies [42]. The Internet has broken down walls and permitted the free flow of ideas that have led to this consciousness as well as the understanding that the Internet can be used to effect political changes and bring human rights violations to light worldwide – which has been seen in Egypt, Tunisia, and Libya [22, 29, 30, 34, 39, 41].

Political activism begins with free speech. Political change occurs through free assembly. Digital activism began with blogging and virtual assembly through social networking [22, 30]. Governments the world over have been attempting to protect existing political systems through technological control over these modern forms of communication. Digital activism began with bloggers, not with Twitter or social networking sites, though such devices make activism far easier [30]. Many governments have attempted to gain control of the Internet to subjugate their people, such as the case in China, where the cyber firewall is anecdotally said to mimic the Great Wall, and Cuba, where bloggers are routinely monitored, arrested, or harassed by the government [7, 29]. Yet despite attempts by countries such as China and Cuba, the Internet continues to afford people within repressive regimes the ability to organize and demand political change.

The bill itself defined the term "national cyber emergency" as any action designed to cause a disruption to or create a significant disturbance to "the information infrastructure essential to the reliable operation of covered critical infrastructure" [12]. The bill also defined the term "national information infrastructure" to include both government and non-governmental infrastructure, inside or outside the United States, whose disruption could cause catastrophic damage in the United States. Section 248 of the bill defines potential vulnerabilities to the infrastructure, that when threatened may result in the declaration of a national cyber emergency [12].

The bill also provided broad powers to the director of the NCCC and required compliance with emergency measures by owner-operators. This section calls for a process by which owner-operators can develop their own response plans; though these can be deemed insufficient during an emergency. Owner-operator compliance with emergency measures was mandatory and subject to civil and criminal compliance for non-compliance [12, 26, 27].

Although the purpose of the Protecting Cyberspace as a National Asset Act of 2010 [12, 26, 31] was to protect from malicious cyber-attacks, it ultimately would have provided complete Executive control over the Internet. This means that the President of the United States would have had the legal right to silence the Internet at a time when, arguably, the Internet was most vital to communication. Through the self-correcting nature of Internet communication [5, 19, 25] this would have meant telecommunications providers would have had to terminate

Internet communication, as Egypt had been able to accomplish [34]. The Protecting Cyberspace as a National Asset Act of 2010 was tabled by congress in late 2011.

SOPA, PIPA, CISPA and ACTA

A litany of bills have been introduced in both the House of Representatives and Senate after the "Protecting Cyberspace as a National Asset Act of 2010" was tabled in late 2011. Well-funded special interest groups have continued to ratchet up pressure on our congressional leaders [1, 14, 15, 27, 36]. The bills SOPA (Stop Online Privacy Act) [37], PIPA (Protect IP Act) [24], CISPA (Cyber Intelligence Sharing and Protection Act) [35] and ACTA (Anti Counterfeiting Trade Agreement) [1, 14] have been introduced by our congressional leaders. Two of these proposed bills; SOPA and PIPA have sought to forgo many of the due process statutes of the rule of law [14, 15, 36] and the first amendment right to the freedom of speech.

SOPA was a bill introduced in the House of Representatives by Texas congressman Lamar Smith [37], "[to] promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes" and PIPA was a bill introduced in the Senate by Vermont senator Patrick Leahy [24], "[to] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property." These bills sought to expand U.S. law enforcement abilities in combating copyright infringement, search engines such as Google would be forced to disable searches for pirated materials. Internet Service Providers would be forced to delete the domain name records (the records that translate domain names into TCP/IP addresses) for any sight suspected of disseminating copyrighted materials. SOPA also sought to give the U.S. Justice Department the power to take down any website for any perceived violation of copyright infringement without due process [14, 17, 37]. SOPA would have further sought compensation from any company or individual that did business with the website in question [14, 17]. PIPA was nearly identical to SOPA with greater judicial oversight [14, 17, 24]. In late January of 2012 the House Judiciary committee postponed consideration of SOPA, at the same time in the Senate PIPA was tabled until the issues of due process were resolved [17, 24, 37].

After SOPA and PIPA failed to pass, U.S. lawmakers in the House of Representatives introduced CISPA aimed at guarding against "cyber-threats" [17]. CISPA was introduced by Michigan congressman Mike Rogers [35], "[to] provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cyber security entities, and for other purposes." CISPA was introduced after the "Protecting Cyberspace as a National Asset Act of 2010", SOPA and PIPA all failed in the House of Representatives in 2011 [14, 17, 24, 35, 37]. CISPA seeks to amendment to the "National Security Act of 1947" with provisions for dealing with cybercrime, cyber terrorism and national security leaks. Even with recent amendments to this proposed bill it permits the American government to monitor all domestic Internet activity of its citizens without the threat of liability, denying its citizens due process under the law [1, 17, 35]. In April of 2012 this bill passed the House of Representatives and went on to the Senate for deliberation. In March of 2013 EFF (Electronic Frontiers Foundation) a nonprofit Internet rights watchdog group and thirty other Internet civil liberties organizations sent a petition with over 100,000 signatures to members of congress demanding a NO vote on CISPA. The petition called on congressional leaders to oppose CISPA due to "privacy and civil liberty" concerns [38].

ACTA is a trade agreement that has been negotiated from its inception in 2007 though 2010 by the United States, European Union, Switzerland, Canada, Australia, New Zealand, Mexico, Singapore, Morocco, Japan and South Korea. This trade agreement seeks to implement a new global intellectual property (IP) enforcement standard. In October of 2011 eight out of the eleven countries that had originally negotiated the ACTA trade agreement had signed it [4]. Japan is the only country that has ratified this agreement. Once six nations ratify this agreement it will go into effect. This trade agreement will turn ISP's (Internet Service Providers) into copyright police violating both privacy and the due process rights of its customers. ACTA's language is vague, left to interpretation and key terms like piracy and counterfeiting are never clearly defined [4, 17].

If international events have pushed this litany of proposed legislation into the forefront then where are the voices of reason within our own government? Our congressional leaders have yet to discuss the financial and civil liberty impact of any of this proposed legislation.

INTERNATIONAL EVENTS

Thomas Friedman [18] stated that the destruction of the Berlin Wall was a pinnacle moment in history, when the world symbolically rejected its barriers. It was with this event, the world re-oriented to a single system, "advocating democratic, consensual, free-market-oriented governance. "[Moving] away from systems advocating authoritarian rule with centrally planned economies" [18]. He also went on to point out the symbolic power of this destruction has affected the citizens of other countries to seek freedom seeing the world around them as "connected" [18].

The events sparked by Tunisia in late 2010 have demonstrated the power of the Internet to unite people in declaring their authoritarian governments illegitimate [22, 29, 30, 34, 39, 41]. On January 14, 2011, following Internet-organized mass protests, the president of Tunisia fled the country after 23 years of authoritarian rule. Particular significance is placed upon this event because it is the first time mass demonstrations ousted an Arab leader. Without the Internet, arguably, these demonstrations would have been less effective – or would have been crushed with little media attention.

Barely two weeks later, millions of Egyptian protesters demanded the overthrow of the current political regime of Egyptian President Hosni Mubarak [34]. Over the next several days, a series of demonstrations and labor strikes focusing on legal and political reforms were organized from various groups and socio-economic classes. The Egyptian government quickly moved to sever all Internet connections and cell phone services, doing so with help of international firms including U.K. based Videophone, and Egypt's five large Internet carriers. Within hours of mandating the shutdown, Egypt ceased to exist within cyberspace [34, 39].

This was not the first time that a government was able to disrupt the Internet due to political unrest supported by social networking sites. In 2009, the Iranian presidential elections were followed by mass demonstrations. In the effort to stop the spread if information related to the election and subsequent protests, the government severely attenuated bandwidth, significantly slowing the spread of information [42].

Since the Egyptian revolution there have been demonstrations in Yemen, Bahrain, Tunisia, and Libya. While not all have yet shown to be successful, the individual government's responses to these demonstrations indicate their awareness of the power of the Internet. For example, in the effort to quash future uprisings, Bahrain sent loyalty pledges to its students studying abroad. Bahrain officials, knowing that social media can be used to both organize protests and to broadcast events worldwide, specifically included the use of social media in the pledge – meaning that those who sign agree to refrain from using social media in any manner that supports anti-government actions [3].

Censorship of traditional media remains the main – most direct – method of suppressing political and civil dissent [2]. Government control of traditional media outlets, television, radio, and print media, for example are no longer adequate due to the proliferation of cellular phones and wireless networks. Nations can use the Internet to suppress, though how effectively remains to be seen [7]. China's authoritarian control over its Internet infrastructure has been described as the Great Firewall of China; however, technology does exist that is designed to bypass the censors allowing politically sensitive material to be published onto the World Wide Web. In cases where such technology is inaccessible, underground networks designed for the purpose of circumventing and disseminating these materials have been established [29]. Cuban blogger Yoani Sánchaz, named one of *Time Magazine's* 100 Most Influential People of 2008, passes her blog entries to trusted friends who then publish them for her [29].

FINANCIAL IMPLICATIONS

The financial impact of complying with any of these proposed bills will have unknown consequences regarding the global economy. With nations inextricably linked through commerce, any bill aimed at killing innovation or even the Internet itself means preventing U.S.-based Internet businesses from interacting with their customers, investors, and other financial stakeholders. According to a 2008 survey of 1,004 economists worldwide, even a single day without the Internet risks major economic repercussions [16]. Thus, a prolonged outage risks destroying smaller Internet-related businesses, which number over 20,000, and significantly damaging larger ones [21]. Foreign businesses that rely on U.S. companies for goods or services stand to lose as well, as they will find themselves unable to operate at full capacity.

The financial aftershocks of any proposed legislation impacting the Internet, are impossible to calculate. The financial impact of the Internet comes in three values: employment, time and payment [32]. The calculated annual impact of the Internet is as follows: employment accounts for $300 billion; time is estimated at $680 billion; and for payment is $444 billion [32]. There are no numbers available on the innovation that results from the collaboration made possible by the Internet.

Direct, quantifiable evidence, however, surrounding the financial damage that the kill switch or any other legislation impacting the Internet can be seen in immediate returns from the Egyptian shutdown. In this example the Egyptian economy lost approximately $18 million USD per day, or 3-4% of its GDP [33] during its outage.

CONCLUSION

Technically, the dissemination of propaganda, regardless of whether it comes from dissidents or governments, does not constitute a misuse of the Internet. Ultimately, it is the deliberate prevention and censorship of ideas that constitutes misuse.

The ability to kill the Internet violates the fundamental concept behind the First Amendment. Prohibiting the American people from interacting through cyberspace prohibits them from enjoying not only the ability to communicate freely but also prohibits them from freely assembling. While it is logical and rational to seek ways to protect the nation from cyber-attacks, the un-checked ability to shut down the Internet does not yet trump those freedoms. The fact that the Protecting Cyberspace as a National Asset Act of 2010, SOPA, PIPA, CISPA and ACTA have not yet passed, suggests that they all fail to adequately protect the nation as well as the freedoms of the nation's people.

The fact that the Internet has played such a strong role within the "Arab Spring" suggests that legislation that curbs the rights of the people of the United States is doomed to fail. Aside from the risk of government censorship, there exist financial implications that can cripple the U.S. economy, which still struggles to recover from the recent downturn.

Further research into potential cyber risks as well as alternate methods of protecting the Internet from legitimate threats is necessary. Providing the Executive or any other branch of government unchecked power to kill the Internet creates complications and a chilling effect on freedom.

The proposed legislation and trade agreement discussed in this paper all have one thing in common, their language is vague, terms are loosely or inadequately defined and open ended statements like "and for other purposes" [24, 35, 37] should scare the hell out of any U.S. citizen that believes in the first amendment's right to the freedom of speech, expression and assembly.

REFERENCES

1. Auerbach, D. (2012). Eff Opposes Cispa on Hackers and Founders Panel. Retrieved April 20, 2012, 2012, from https://http://www.eff.org/deeplinks/2012/04/eff-opposes-cispa-hackers-and-founders-panel
2. Boykoff, J. (2008). The Dialectic of Resistance and Restriction: Dissident Citizenship and Global Media. *Georgetown Journal of International Affairs, 9*(2), 23-31.
3. Bruton, F. B. (2011). Bahrain to Citizens Living Abroad: Spy on Countrymen, No Protests Permitted. Retrieved July 1, 2011, 2011
4. Carolina Rossini, M. S., and Gwen Hinze. (2010). Anti-Counterfeiting Trade Agreement. Retrieved March 19, 2013, 2013, from https://http://www.eff.org/issues/acta
5. Cerf, V., Dalal, Y., & Sunshine, C. (1974). Specification of Internet Transmission Control Program. Retrieved June 28, 2011, from http://tools.ietf.org/html/rfc675
6. Channel, T. H. (2002). Modern Marvels: The Internet. *Modern Marvels*. The History Channel: The History Channel.
7. Cody, E. (2007). Despite a Ban, Chinese Youth Navigate to Internet Cafes., *Washington Post*.
8. Commission, F. C. (1996). Telecommunications Act of 1996. from http://www.fcc.gov/telecom.html
9. Commission, F. C. (2009). Communications Act of 1934 (Copy of Congressional Act). from

http://www.fcc.gov/Reports/1934new.pdf
10. Commission, F. C. (2011). Fcc Public Safety and Homeland Security Bureau. from http://www.fcc.gov/pshs/techtopics/techtopics20.html
11. Commission, F. C. (2011). Tech Topic 20: Cyber Security and Communications. In Fcc Pshb (Ed.). *Economic Impact from "Doomsday" Scenario*.
12. Protecting Cyberspace as a National Asset Act of 2010, S. 3480, United States Senate (2010).
13. Ditz, J. (2010). Ditz: Militarized Internet Will Trample Freedom. *Washington Times*. Retrieved March 28, 2012, from http://washingtontimes.com/news/oct/7/militarized-internet-will-trample-freedom/
14. Drutman, L. (2012). How Sopa and Pipa Did and Didn't Change How Washington Lobbying Works. Retrieved 4/14/2012, 2012, from http://sunlightfoundation.com/blog/2012/01/30/sopa-lobbyin/
15. Dutton, W. H. D., Anna; Law, Ginette; Nash, Victoria. (2011). *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*: Paris, UNESCO.
16. Ecommerce. (2008). Economic Impact from "Doomsday" Scenario. from http://ecommerce-journal.com/articles/how_economic_impact_from_internet_doomsday_scenario
17. Editor. (2012). What Are Sopa, Pipa Cispa and Acta? Retrieved March 18, 2013, 2013, from http://www.techadvisory.org/2012/08/what-are-sopa-pipa-cispa-and-acta/
18. Friedman, T. L. (2007). *The World Is Flat, a Brief History of the Twenty-First Century* (3 ed.). New York: Picador/Farrar, Strauss and Giroux.
19. Hafner, K. (1998). *Where Wizards Stay up Late: The Origins of the Internet*: Simon & Schuster.
20. Hauben, R. (2001). From the Arpanet to the Internet. Retrieved June 28, 2011
21. IAB. (2009). Ad-Supported Internet Contributes $300 Billion to U.S. Economy, Has Created 3.1 Million Jobs, Confirms Groundbreaking Study. from http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-061009-value
22. Kirkpatrick, D., D. (2011). Tunisia Leader Flees and Prime Minister Claims Power. from http://www.nytimes.com/2011/01/15/world/africa/15tunis.html
23. Lander, M., & Knowlton, B. (February 14, 2011). U.S. Policy to Address Internet Freedom, *N.Y. Times*. Retrieved from http://www.nytimes.com/2011/02/15/world/15clinton.html?_r=2&ref=technology
24. Protect Ip Act of 2011, S. 968 (2011).
25. Licklider, J. C. R. (1960). Man-Computer Symbiosis. *IRE Transactions on Human Factors in Electronics, HFE-1*, 4-11.
26. Lieberman, J. (2010). Protecting Cyberspace as a National Asset Act. Washington, DC: U.S. Government Printing Office: The Committee on Homeland Security.
27. Lieberman, J. (2010). *Protecting Cyberspace as a National Asset Act of 2010*. (111-363). Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d111:S3480:.
28. McCullagh, D. (2011). Renewed Push to Give Obama and Internet "Kill Switch". from http://www.cbsnews.com/8301-501465_162-20029302-501465.html
29. McKinley, J. (2008). Cyber-Rebels in Cuba Defy State's Limits. from http://www.nytimes.com/2008/03/06/world/americas/06cuba.html
30. Moore, J. (2011). Did Twitter, Facebook Really Build a Revolution? . from http://www.msnbc.com
31. *Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses*, (2010).
32. Quelch, J. (2009). Quantifying the Economic Impact of the Internet. from http://hbswk.hbs.edu/item/6268.html
33. Reynolds, T., & Mickoleit, Arthur. (2011). The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt. Retrieved June 21, 2011, 2011, from http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html.
34. Rhoads, C., & Fowler, G. A. (2011). Egypt Shuts Down Internet, Cell Phone Services. Retrieved Septembe 15, 2012, 2012, from http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html
35. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, House of Represenatives (2011).
36. Schneider, A. R. (2007). Censorship: Language and Politics. Retrieved February 8, 2012, from http://april-rose-schneider.suite101.com/censorship-a15339
37. Stop Online Privacy Act, H.R.3261, House of Represenatives (2011).

38. Suri, I. (3013). Petition against Cispa Crosses 100,000 Signatures, Reaches White House. Retrieved March 19, 2013, 2013, from http://siliconangle.com/blog/2013/03/18/petition-against-cispa-crosses-100000-signatures-reaches-white-house/
39. Sutter, J. (2011). When the Internet Actually Helps Dictators [Cnn Tech]. Retrieved March 11, 2012, 2012, from http://www.cnn.com/2011/TECH/web/02/22/authoritarian.internet.morozov/index.html
40. Sutton, M. (2012). This Week in Censorship: News from Iran, India, Vietnam, and China. Retrieved April 20, 2012, 2012, from https://http://www.eff.org/deeplinks/2012/04/week-censorship-iran-india-vietnam-and-china
41. Times, N. Y. (2011). Libya-Protests and Revolt (2011) [Press Release]. from http://topics.nytimes.com/top/news/international/countriesandterritories/libya/index.html?scp=1&sq=Libyan Timeline&st=cse
42. Times, N. Y. (2011). State Department to Announce Internet Freedom Policy. from http://www.nytimes.com/2011/02/15/world/15clinton.html?_r=0
43. website, T. H. C. (2012). The Invention of the Internet. April 14, 2012, from http://www.history.com/topics/invention-of-the-internet
44. Zax, D. (2011). Could Egypt Happen Here? Obama's Internet "Kill Switch". Retrieved June 28, 2011, from http://www.fastcompany.com/1721753/egypt-internet-kill-switch