Cyber Economic Espionage: Corporate Theft and the New Patriot Act

by GENNA PROMNICK*

Table of Contents

* J.D. candidate, University of California, Hastings College of the Law, expected graduation date May 2017; B.A., University of California, Santa Barbara, 2012. The author would like to thank Professor Ahmed Ghappour for his guidance and feedback. Steven Pavlov for always being a source of encouragement and for proofreading across Croatia, and my family for their love and support.

I. Introduction

On Friday, December 18th 2015, President Barack Obama signed a bill into law changing all of our lives. In a late-night session, Congress slipped the Cybersecurity Information Sharing Act of 2015 ("CISA") into the omnibus-spending package, which was pending the President's signature. This bill was very similar to a number of other cybersecurity bills Congress previously tried and failed to pass. They failed in large part due to protestation by civil liberty groups and citizens across the country claiming that the proposed legislation lacked fundamental protection for individual privacy rights. CISA, the bill that lived, was passed in order to create a law that would regulate information sharing concerning cyber crime among government and private entities, as well as between private entities. However, the legislation's broad language has created what some have called the Second Patriot Act.

Supporters of the bill argue that the bill's promotion of information sharing would contribute to the larger effort to fix the private sector's cybersecurity underinvestment[1] and provide companies with antitrust[2] and tort litigation protection.[3] Additionally, the bill would protect intellectual property rights by promoting information sharing relating to cyberattacks and help alleviate future attacks based on this information.[4]

CISA was hastily passed, arguably due to a spate of recent cyber attacks on large corporations. In 2013, "more than 600 breaches [ha[d] been] reported nationwide."[5] These included high-profile breaches that heavily affected the public. One of these breaches involved the theft of approximately 40 million

1. Proponents of CISA have argued that the availability of abundant information about "cyberincidents and cyberthreats" will allow more reliable data and help corporations (and the government) more accurately "calculate efficient levels of cybersecurity." Melanie J. Teplinsky, *Fiddling on The Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 279 (2013).

2. Antitrust laws may also affect a company's decision to share information. Andrew Nolan, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS 26–49 (2015), https://www.fas.org/sgp/crs/intel/R43941.pdf.

3. A company could be found negligent for failing to act upon a threat, if an individual can show actual damages for the claim. The fear of ligation may cause companies to not divulge information regarding a cyberattack. *Id.* at 29–31.

4. Companies fear that information shared with the government could prompt an investigation by government regulators or that this sensitive information will be used as evidence in a regulatory action against the company. *Id.* at 37–38; Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 271 (2010).

5. Howard M. Privette, et al., *The SEC Guidance on Cybersecurity Measures For Public Companies*, 37 L.A. LAW 14, 15 (2014).

credit and debit card account numbers from the Target Corporation.[6] Another, allegedly carried out by the Chinese government, involved a large-scale hack on the Office of Personnel Management.

However, opponents of the bill argue that it violates civil liberties and citizens' basic privacy rights. Representative Justin Amash (R-Mich.), with the support of other members of Congress, has written extensively on the negative impacts of the bill.[7] He has stated that its broad language would lead to over-sharing of a company's users' private information by allowing companies to share a wide range of information with multiple government agencies, including the National Security Agency ("NSA")[8] with complete immunity.[9] Additionally, leading technologists say that the type of information sharing promoted in CISA gets nothing accomplished by way of security.[10] Even technology companies have come out against the bill,

6. *Id.*

7. Press Release, Jordan Bush, Amash Introduces Measure to Repeal Anti-Privacy Cyber Bill, (Jan. 13, 2016), http://amash.house.gov/press-release/amash-introduces-measure-repeal-anti-privacy-cyber-bill. Amash was joined by Rep. John Conyers (D-Mich.), Rep. Zoe Lofgren (D-Calif.), Rep. Thomas Massie (R-Ky.), Rep. Ted Poe (R-Tex.), and Rep. Jared Polis (D-Colo.).

8. The bill establishes that companies will primarily be sharing information with the Department of Homeland Security (DHS), however it "requires DHS to establish processes to share the information it receives with other federal agencies," including intelligence agencies like the NSA. Justin Amash, Oversight and Government Reform Committee, 114th Cong., Oppose Omnibus to Stop Anti-Privacy Cyber Bill (Comm. Print 2015) [hereinafter *Oppose Omnibus*] http://amash.house.gov/sites/amash.house.gov/files/2015%201217%20OmniCISA%20DC.pdf.

9. This bill includes no exemption to the liability waiver for gross negligence or willful misconduct, meaning companies may "overshare their user's personal, private information with complete immunity." *Id.*; *see also,* Press Release, Jordan Bush, AMASH INTRODUCES MEASURE TO REPEAL ANTI-PRIVACY CYBER BILL (Jan. 13, 2016), http://amash.house.gov/press-release/amash-introduces-measure-repeal-anti-privacy-cyber-bill.

10. *See* Jennifer Granick, *Technologists Oppose CISA/Information Sharing Bills*, STANFORD CYBERLAW BLOG (Apr. 16, 2015), http://cyberlaw.stanford.edu/blog/2015/04/technologists-oppose-cisainformation-sharing-bills. "Private information about individual users is often a detriment in developing threat signatures because we need to be able to identify an attack no matter where it comes from and no matter who the target is. Any bill that allows for and results in significant sharing of personal information could decrease the signal-to-noise ratio and make [indicators of compromise] less actionable." Thus, when companies need to share address information, they are typically sharing the addresses of servers which are used to host malware, or to which a compromised computer will connect for the exfiltration of data. *Id.* "This addressing information helps potential victims block malicious incoming connections. These addresses do not belong to subscribers or customers of the victims of a security breach or of the companies whose systems we are helping to secure. Sharing this kind of addressing is a common current practice."□*Id.* (Quoting a letter written by technologists, academics, and computer and network security professionals who research, report on, and defend against Internet security threats). *See also* Jonathan Keane, *5 Things You Need to Know About the CISA Bill That Just Passed*, PASTE (Dec. 22, 2015), http://www.pastemagazine.com/articles/2015/12/5-things-you-need-to-know-about-the-cisa-bill-that.html (there is no way to prove that sharing this data could prevent a cyber-attack, moreover, the government's collection of this data could create more harm than good, by creating a "centralized database of user info[rmation] that hackers could target").

stating that more effective legislation is necessary to deal with cyber threats while maintaining individual privacy.[11]

This paper argues that as the bill stands, its lack of protections for individual security and privacy outweigh its effectiveness in preventing cyber economic espionage. It proceeds in three parts. Part Two will address the differences between traditional espionage and cyber economic espionage and why cyber economic espionage is a novel and significant problem. Part Three will provide the current legal framework to confront the problems cyber-economic espionage has created and will ultimately argue that these solutions have created their own problems. Finally, Part Four will examine other options the U.S. has as an alternative to combat cyber economic espionage.

II. Discernible Differences Between Traditional Espionage and Cyber Economic Espionage Demonstrate a New Problem Emerging and the Need for a Regulatory Framework

Espionage is the "world's second oldest profession."[12] It is a practice that states have continuously engaged in and "acknowledged as a matter of practical reality," even during peacetime.[13] Espionage is defined as "the activity of using spies to collect information about what another government or company is doing or plans to do."[14] Countries all over the world have continually conducted espionage operations in other nation states in order to "know more about the internal military, political, economic, and social developments in those countries, information that would otherwise be impossible to know from open sources."[15]

11. *See* Jonathan Keane, *5 Things You Need to Know About the CISA Bill That Just Passed*, PASTE (Dec. 22, 2015), http://www.pastemagazine.com/articles/2015/12/5-things-you-need-to-know-about-the-cisa-bill-that.html. ("Reddit, Yelp, Twitter, and unsurprisingly Apple have all voiced opposition to these measures"); *see also* Amul Kalia, *Tech Industry Trade Groups are Coming out Against CISA. We Need Individual Companies to do the Same*, EFF (Oct. 20, 2015), https://www.eff.org/deeplinks/2015/10/tech-industry-trade-groups-are-coming-out-against-cisa-we-need-individual.

12. Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1163 (2011); *see also* Casey M. Bruner, *Authorized Investigation: A Temperate Alternative to Cyber Insecurity*, 38 SEATTLE U. L. REV. 1463, 1477 (2015) ("[e]spionage between governments is nearly as old as government itself").

13. WILLIAMS, *supra* note 12, at 1163.

14. *Espionage*, BLACK'S LAW DICTIONARY (10th ed. 2014).

15. Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 444, 466 (2015).

A. Traditional Political or Military Espionage

Political military espionage (henceforth "conventional espionage"), or intelligence collection through surreptitious, intrusive means inside a foreign nation's territory without that nation's knowledge or consent for the purpose of national security, has not been considered a violation of international norms as long as it does not violate the nation's sovereignty.[16] Every nation has "some type of intelligence service" that is responsible for espionage activities worldwide.[17]

The current state of international law reflects the general acknowledgment among most countries that espionage is an acceptable practice conducted by most states during peaceful times.[18] United Nations Charter art. 2, ¶ 4, protects states from violation of their territory as well as protecting their political independence, but refers only to acts that involve the threat or use of force; under the U.N. Charter espionage does not reach the level of use of force.[19]

Another indication that espionage does not violate or implicate international law is that it is the practice used by most countries to apprehend spies. The offended state does not condemn the offending nation of the spy, rather the individual is held in violation of domestic law in the state where he or she is apprehended.[20] Therefore, because international law does not clearly condone nor explicitly prohibit the conduct, it tends to support the conclusion

16. *Id.*; *see also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (1987) (sovereignty "implies a state's lawful control over its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there.); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 206 (1987) (The sovereignty of a state is reflected also in immunity for the state and its public property from certain exercises of authority by other states").

17. LOTRIONTE, *supra* note 15, at 459.

18. *See id.* at 475, "as the Cold War evolved, espionage became a systematic, publicly recognized form of state activity essential to the conduct of international relations, with almost all countries actively engaging in the practice."

19. *See also*, David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 371 (2013).

20. *See* LOTRIONTE, *supra* note 15, at 461–479, "when a spy is caught abroad, there is no sense of legal culpability for the state from which the spy was sent, instead, culpability extends only to the individual . . . it is rare for the expelling state to claim that these activities themselves violate international law"; *see also*, WEISSBRODT, *supra* note 19, at 371, "espionage is used by nations at the risk that if their spies are apprehended in a foreign jurisdiction they may be prosecuted criminally." *But cf.*, John Radson, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 620 (2007), extradition treaties provide proof that a crime has reached a level of international consensus, in regards to espionage there is proof that it is treated more like a political offense, "that would suggest international disagreement or a contradiction between domestic norms and international norms."

that espionage is nothing more than the violation of another nation's laws.[21] Thus, espionage is seemingly a consensus among states.[22]

B. Traditional Economic Espionage

Espionage is primarily a method in which countries obtain information clandestinely in order to protect their nation's national security interests.[23] The information sought can come from a "foreign government, enemy or ally, as well as . . . foreign corporations."[24] U.S. Policy explicitly authorizes and regulates secret covert action pertaining to political, military, and economic conditions in other countries.[25] Therefore, there is not much of a difference in the way the U.S. treats traditional conventional espionage versus traditional economic espionage, when carried out for the protection or in the interest of national security.[26] Like conventional espionage, economic espionage is not a new phenomenon.[27]

Furthermore, like conventional espionage, the U.S. does prosecute those who conduct economic espionage. Similar to conventional espionage, those individuals who are caught are held in violation of domestic law.[28] Additionally, in 1996, the U.S. adopted the Economic Espionage Act ("EEA"), which made the theft of trade secrets from U.S. companies a Federal crime.[29] The EEA was the "first federal statute to criminalize the theft of trade secrets."[30] The EEA criminalized domestic economic espionage and economic espionage that intended to benefit foreign powers.[31]

21. WILLIAMS, *supra* note 12, at 1174–75; *see also* Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1180 (2014).

22. Rather than an international norm.

23. LOTRIONTE, *supra* note 15, at 466.

24. *Id.*; *see also* WILLIAMS, *supra* note 12, at 1177, "a number of (often classified) multilateral intelligence-sharing arrangements such as the relationship among the signals intelligence agencies of the United States, United Kingdom, Australia, Canada, and New Zealand — the 'five eyes' — may help to establish or evidence customary norms for what constitute acceptable forms of espionage."

25. WILLIAMS, *supra* note 12, at 1169.

26. LOTRIONTE, *supra* note 15, at 449.

27. *See* BRUNER, *supra* note 12, at 1477.

28. LOTRIONTE, *supra* note 15, at 461–79.

29. LOTRIONTE, *supra* note 15, at 470; 18 U.S.C.A. §§ 1831–183 (West 2013).

30. Jonathan Eric Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI.-KENT J. INTELL. PROP. 189, 200 (2009).

31. *Id.*; 18 U.S.C.A. § 1831 (West 2013) provides in part that:

> a) In general — Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly —

The EEA was passed to "prevent corporate insiders from stealing trade secrets and selling them to foreign governments and foreign or domestic companies."[32]

C. Cyber Economic Espionage

It is important to distinguish conventional or traditional espionage from cyber economic espionage.[33] The goal of cyber economic espionage, for the purpose of this paper, is to strengthen private corporate interests for the benefit of the offending nation while preventing the target from advancing economically.[34] Unlike traditional espionage, cyber economic espionage is not used to help make policy decisions for political or military security.[35] Furthermore, the current trend of foreign governments condoning or conducting economic espionage to assist their countries' businesses to gain a global economic advantage is a relatively new phenomenon in the global economy.[36]

In contrast, traditional espionage provides for reciprocal "acceptance and benefits between states,"[37] while cyber economic espionage only stands to benefit the state engaging in the practice.[38] With cyber economic espionage, there is no "custom of reciprocity or cooperation that states should be concerned about preserving."[39] Furthermore, traditional espionage "allows states to determine and verify other states' intentions,"[40] as well as learn about another state's military capabilities. This knowledge allows

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or byfraud, artifice, or deception obtains a trade secret;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.

32. LEWIS, *supra* note 30; 18 U.S.C.A. § 1831 (West 2013).

33. SKINNER, *supra* note 21, at 1183, "It would be a mistake to afford the same legal treatment to economic cyber espionage."

34. *Id.* at 1177.

35. *Id.*

36. BRUNER, *supra* note 12, at 1477.

37. LOTRIONTE, *supra* note 15, at 488, "traditional espionage can serve to increase the security of states, helping to decrease the chances of surprise attacks and minimizing conflict, thereby preserving global security."

38. *Id.*

39. *Id.*; SKINNER, *supra* note 21, at 1183.

40. LOTRIONTE, *supra* note 15, at 489.

states to prevent a threat, which might decrease the likelihood of a successful surprise attack.[41] Thus, in effect, traditional espionage functions as an operational restraint for conflict that helps preserve global stability.[42]

The U.S. has been unwilling to accept cyber economic espionage as an international norm.[43] Attacks on American companies have increased by seventy-five percent between 2011 and 2012.[44] According to Assistant Attorney General John Carlin, there has been an estimated loss in the U.S. of more than $300 billion from the theft of intellectual property.[45] Consequently, cyber economic espionage has been dubbed "the biggest intelligence disaster since the loss of nuclear secrets [in the late 1940s]."[46]

Furthermore, U.S. officials have maintained that intelligence agencies do not collect trade secrets of foreign companies nor provide those secrets to U.S. companies for business advantages.[47] According to scholars, "U.S. officials have taken great pains to reiterate the distinction between spying on foreign officials and conducting economic intelligence."[48] The former is important to protect U.S. national security while the latter is forbidden.[49]

It should be understood that this is how the U.S. defines cyber economic espionage. Some critics, like Jack Goldsmith, believe that the U.S. couches these statements broadly and that the collection of information is in fact, very "robust," implying the government may not only collect information purely for national security interests.[50] Additionally, Goldsmith notes that China has a

41. *Id.*

42. *Id.*

43. *Id.* at 451–52.

44. *Id*. at 453.

45. John Carlin, *Remarks at the Brookings Institute's Emerging National Security Threats Forum*, U.S. DEPARTMENT OF JUSTICE (May 22, 2014), https://www.justice.gov/nsd/pr/assistant-attorney-general-john-carlin-delivers-remarks-brookings-institutes-emerging. Assistant Attorney General John Carlin contends that there is a difference between nations carrying out traditional espionage versus cyber economic espionage. He purports that "responsible nations do conduct intelligence activities" but goes on to say that these intelligence activities are "focused on the national security needs of our country." Indeed, since the emergence of the practice of cyber economic espionage, the U.S. has drawn a line between foreign intelligence gathering for national security purposes and spying on foreign corporations to gain a "competitive economic advantage in the international market place."

46. TEPLINSKY, *supra,* note 1 at 258.

47. LOTRIONTE, *supra* note 15, at 452–63.

48. *Id*. at 465.

49. *Id*.

50. Jack Goldsmith, *Reflections on U.S. Economic Espionage, Post-Snowden*, LAWFARE (Dec. 10, 2013), https://www.lawfareblog.com/reflections-us-economic-espionage-post-snowden.

very different economic system and relationship with private businesses than the U.S.; this, combined with the fact that China is in a different stage of development than the U.S., leads him to believe that it is natural that China has adopted an "IP [intellectual property]-stealing" espionage strategy versus the U.S.'s "IP-preserving" espionage strategies, and that the U.S.'s treatment of China amounts to little more than a "complaint" that the Chinese are pursuing their own interests at the expense of the U.S.[51]

Despite justification for why cyber economic espionage exists, as provided by Mr. Goldsmith, the act itself should not be tolerated because it does not allow for the exchange of benefits that facilitate global stability and security.[52] For one, the spying state is harming the target state's "incentive to innovate, natural comparative advantages and robustness as trading partners."[53] Additionally, economic espionage fuels instability by providing the ability to cripple another nation's economy and possibly contribute to the destabilization of the global economy, thereby creating the ability to potentially risk the peace and security of the international community.[54] Thus, the need for a regulatory framework to curb the use of cyber economic espionage by foreign governments is paramount.

However, the EEA does not help protect the U.S. from the current form of cyber economic espionage being carried out by foreign nations.[55] Congress was unable to anticipate the use of the Internet to engage in the theft of intellectual property from domestic companies by foreign governments within their own boarders.[56] That is because the volume of information stolen via cyberspace is much more significant and happens at a quicker pace than traditional human or technical intelligence gathering.[57] Moreover, the infiltration of computer systems is far more difficult to detect and stop.[58]

51. *Id.*

52. SKINNER, *supra* note 21, at 1183–84.

53. *Id.*

54. *Id.; see* BRUNER, *supra* note 12, at 1478 ("[T]he economic losses due to cyber insecurity are significant."); O'HARA, *supra* note 4, at 242 (finding that the "the American economy is at risk "in a way that many policymakers could not have envisioned just a decade ago."); TEPLINSKY, *supra* note 1, at 258–59 (quoting Richard Clarke, the former counterterrorism czar in three U.S. presidential administrations, as saying, "every major company in the United States has already been penetrated by China, we are currently in a position to lose our competitiveness by having 'all of our research and development stolen by the Chinese,' while companies in the U.S. spends huge sums of money on research and development and that information goes free to China . . . after a while you can't compete").

55. O'HARA, *supra* note 4, at 243–44.

56. *Id.*

57. SKINNER, *supra* note 21, at 1183–84.

58. *Id.*

In 2013, the Mandiant report[59] shed new light on the *significance* of Chinese cyber economic espionage operations.[60] The report ignited concern from both the public and private sector and led to an increased initiative to stem the U.S.'s vulnerability to cyber attacks.[61] Subsequently, President Barack Obama signed Executive Order 13636 ("Order"), which called for the development of a cyber security framework that would facilitate the improvement of critical infrastructure.[62] The Order also called for information sharing between the public and private sectors.[63] However, the Order emphasized that the framework was voluntary and that businesses and organizations were encouraged to manage their cyber security risks effectively.[64]

The U.S.'s position on "economic espionage has always been that there should be a separation between the government and the private sector, and government resources should not be used to benefit specific companies."[65] Consequently, no federal agency is responsible for defending private businesses, and the federal government has avoided mandates regarding private sector cyber security practices.[66] However, a former member of the Clinton, Bush, and Obama administrations has recently been quoted as stating that companies can "'no longer fight the bad guys individually,'"[67]

59. The Mandiant report was publicly released by Mandiant, a cybersecurity consulting firm. The report was based on a seven-year long investigation that linked China to "a major cyber espionage campaign targeting several United States' business and industries." Kayla Morency, *Cybersecurity Finally Takes Center Stage in the U.S.*, 15 J. OF HIGH TECH. & L. 192, 195–96 (2014); MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (last visited Oct. 6, 2016).

60. TEPLINSKY, *supra* note 1, at 264; MORENCY, *supra* note 59, at 196.

61. MORENCY, *supra* note 59, at 210–11 ("[A]fter the news spread of this tangible proof, many reporters, politicians, and business institutions referred to the report as a 'wakeup' call, highlighting the immediate need for cybersecurity legislation or a comprehensive approach to minimize these threats.").

62. *Id.* at 218–19.

63. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013) ("[I]t is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.").

64. *Id.*; MORENCY, *supra* note 59, at 218–19.

65. LOTRIONTE, *supra* note 15, at 472; *see also* TEPLINSKY, *supra* note 1, at 232 (stating that the U.S. has adopted a "largely self-regulatory, market-based approach to cybersecurity, relying on the private sector to secure its own networks.").

66. TEPLINSKY, *supra* note 1, at 232.

67. Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches*, N.Y. TIMES (Apr. 22, 2015), http://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html.

and the security of these networks has become essential to U.S. economic and national security interests because of the emerging threat of nation-state sponsored cyber economic espionage.[68]

The significance of cyber economic espionage (i.e., the damage, lack of attribution) and the difficulties of using conventional methods (i.e., EEA) to respond to threats, have motivated a change of strategy from ex post mechanisms of deterrence (i.e., criminal justice system) to ex ante preventative measures. This in turn, bolstered previously unsuccessful efforts to pass an information-sharing bill.[69] At the end of 2015, Congress suddenly and underhandedly passed CISA, a suspicious bill that commentators have called the Second Patriot Act.[70] The next section will explore the privacy implications of CISA.

III. The Privacy Failures of the Cyber Information Sharing Act

Fast-forward to December 2015, Congress finally passed the Cyber Information Sharing Act of 2015 ("CISA") by slipping it into the 2016 omnibus-spending package.[71] Different versions of the cyber information-sharing bill were passed in the House and Senate, but Congress did not have a chance to resolve the differences between the two bills before it was "snuck

68. TEPLINSKY, *supra* note 1, at 233.

69. Prior to the Mandiant report and Executive Order 13636, Congress had tried to pass a number of bills that promoted information sharing among the government, businesses, and organizations. One such bill, the Cyber Intelligence Sharing and Protection Act ("CISPA"), failed to pass when it was first introduced in 2012 and when it was subsequently reintroduced in 2013. *HR 3523, Final Vote Results for Roll Call 192* (Apr. 26, 2012), http://clerk.house.gov/evs/2012/roll192.xml; Gerry Smith, *Senate Won't Vote on CISPA, Deals Blow to Controversial Cyber Bill*, HUFFINGTON POST (Apr. 25, 2013), http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html.

70. Andy Greenberg, *Congress Slips CISA Into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015), https://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/ (According to Robyn Greene from the Open Technology institute, "'they're kind of pulling a Patriot Act . . . they've got this bill that's kicked around for years and had been too controversial to pass, so they've seen an opportunity to push it through without debate. And they're taking that opportunity.'").

71. Russel Brandon, *Congress Passes Controversial Cybersecurity Bill Attached to Omnibus Budget,* THE VERGE (Dec. 18, 2015), http://www.theverge.com/2015/12/18/10582446/ congress-passes-cisa-surveillance-cybersecurity; *Obama Signs $1.1 Trillion Spending Package, Approves CISA Surveillance Legislation*, RT (Dec. 19, 2015), https://www.rt.com/usa/326481-obama-signs-budget-cisa-bill/ [hereinafter *Spending Package*]; Aaron Boyd, *Final CISA Bill Wrapped Into Omnibus Package,* FED. TIMES (Dec. 16, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/12/16/cisa-omnibus/77416226/; Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 358 (2015) ("[O]ver the last five years, almost 100 bills regarding cybersecurity have been introduced in Congress. None of this proposed legislation, however, has been enacted into law.").

into the federal budget."[72] For instance, the privacy protections that were put in the House bill were not included in the Senate bill.[73] After years of attempted legislation, this bill, which was modeled after the CISA bill that was passed in the Senate,[74] passed with much the same criticism and widespread opposition that the original bills had prompted.[75]

A. What Does CISA Do?

Proponents of CISA have argued that the availability of abundant information about "cyberincidents and cyberthreats" will allow more reliable data and help corporations (and the government) more accurately "calculate efficient levels of cybersecurity."[76] However, companies already share technical information when they are attacked with other companies while still complying with relevant privacy laws.[77] Companies have, for decades, continuously monitored their computer systems.[78] However, Federal and state law restrained an entity's ability to monitor and share detailed information of an attack. For instance, provisions within the Electronic Communications Privacy Act of 1986, may effect an entity's decision to share information.[79] Under the Wiretap Act, a company can monitor their own system and share information to protect this system but are not authorized to share that information with other entities or the government.[80] The Stored Communication Act is ambiguous concerning the legality of sharing information with other private entities, and companies may avoid sharing such information to avoid litigation.[81]

72. *Spending Package*, *supra* note 71; BOYD, *supra* note 71.

73. ERIC A. FISCHER, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 (PCNA AND NCPAA) AND S. 754 (CISA), Congressional Research Service (2015), https://www.fas.org/sgp/crs/misc/R44069.pdf; Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed,* WIRED (Oct. 27 2015), http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/; *Oppose Omnibus*, *supra* note 8 ("the House bill limited the used of cyber threat information to cybersecurity purposes the new bill allows the government to use the information shared with it by the private sector for numerous purposes unrelated to cybersecurity.").

74. *Id.*

75. *Id.*

76. TEPLINSKY, *supra* note 1, at 279.

77. *Oppose Omnibus*, *supra* note 8.

78. Cordero A. Delgadillo, *What's New With the Cybersecurity Information Sharing Act?*, LEXOLOGY (Feb. 11, 2016), http://www.lexology.com/library/detail.aspx?g=0705fae8-d5e9-42a8-9a17-e2b536e1cf81.

79. NOLAN, *supra* note 2, at 16.

80. *Id.* at 18.

81. *Id.* at 20.

Additionally, antitrust laws may also affect a company's decision to share information. This is notwithstanding the Department of Justice ("DOJ") and Federal Trade Commission ("FTC") official statements explaining that information sharing of this nature falls under the rule of reason, and that its positive effects will weigh in favor of its legality.[82] The agencies clarified that this does not mean it is definitively legal and antitrust suits may still be possible.[83] Companies may also fear the possible threat of tort litigation if they disclose information publicly. A company could be found negligent for failing to act upon a threat if an individual can show actual damages for the claim. Regardless, the fear of ligation may cause companies to withhold information regarding a cyber attack.[84] CISA addresses both of these concerns by providing protection from antitrust and tort litigation.

CISA also addresses concerns companies have about sharing information with the government. For instance, information shared with the government could be disclosed to the public under the Freedom of Information Act, which could result in public access to proprietary information.[85] Companies may also fear that once information is shared with the government, they would waive all intellectual property rights associated with that information.[86] Lastly, companies fear that information shared with the government could prompt an investigation by government regulators or that this sensitive information could be used as evidence in a regulatory action against the company.[87] Most, if not all these concerns have been addressed in CISA,[88] though privacy concerns remain.

B. The Privacy Implications of CISA

Criticism of CISA stems from industry leaders and the public alike; Salesforce, Reddit, Yelp, Twitter, and Apple have publicly opposed CISA.[89]

82. NOLAN, *supra* note 2, at 26–49.

83. *Id.*

84. *Id.* at 29–31.

85. *Id.* at 34.

86. *Id.* at 36.

87. *Id.* at 37–38; O'HARA, *supra* note 4, at 271 ("companies were often reluctant to come to the Federal Government and the Federal Bureau of Investigation because they do not want their trade secrets to be aired. They do not want their shareholders to know there are problems in the company").

88. The law has built in exceptions to Freedom of Information Act ("FOIA"), antitrust laws, and intellectual property rights. It also allows for the sharing of information notwithstanding already existing privacy laws. Lastly, it provides for protections from derivative lawsuits.

89. Amul Kalia, *Tech Industry Trade Groups are Coming out Against CISA. We Need Individual Companies to do the Same*, EFF (Oct. 20, 2015), https://www.eff.org/deeplinks/2015/10/tech-industry-trade-groups-are-coming-out-against-cisa-we-need-individual; KEANE, *supra* note 10.

Recently, Congressman Justin Amash (R-Mich.) introduced a bill that would repeal the cyber surveillance measure passed in the omnibus appropriations bills.[90]

The major critiques of the bill include: (1) the bill authorizes companies to share "cyber threat indicators" regarding "cybersecurity threats" with the federal government and other businesses despite privacy and consumer privacy laws that otherwise protect that information, that is to say the bill allows companies to monitor their information system or another entity's information system (with consent) for cybersecurity purposes, despite other laws that may prohibit monitoring;[91] (2) the bill's terms are broadly defined which allows companies to spy on a wide range of a user's personal private data — the terms "cybersecurity purpose" and "cybersecurity threat" are too broadly defined — "cybersecurity purpose" can mean anything related to protecting an information system, computer or software, whereas "cybersecurity threat," can include anything that can result in an "unauthorized effort to impact the availability of the information system," thus, the extent of the permissible monitoring is unclear;[92] (3) the bill does not prevent the government from searching "indicators" from private companies for information about a specific individual or for evidence of illicit activity;[93] (4) the bill "expressly permits the government to use the information . . . to respond to, investigate, and prosecute activities unrelated to cybersecurity," which has the potential to allow law enforcement to circumvent the warrant process;[94] (5) the bill permits "broad sharing of personal information" and incentivizes companies to adopt "lazy" processes that permit the flow of personal data to the government, and companies do have to make efforts to identify personally identifiable information before sharing; however, their responsibility and the repercussions for sharing that information is curbed because they only have to remove information they

90. BUSH, *supra* note 7.

91. *Id.*; Charles Blanchard, Ronald Lee, & Nicole Neuman, *Senate Intelligence Committee's Recent Cybersecurity Bill Doesn't Silence Privacy Advocates Concerns, Despite a Dozen Amendments*, ARNOLD & PORTER, LLP (Mar. 27, 2015), http://www.lexology.com/library/detail.aspx?g=69c1626c-dc89-4888-afba-3f9da15e62ff; Consolidated Appropriations Act 2016, Pub. L. No. 114-113 (2015); Cybersecurity Act of 2015, title I, sec. 105(a)(4) (Dec. 15, 2015).

92. Lee Tien, *Senate Intelligence Committee Advances Terrible Surveillance Bill in Secret Session*, EFF (Mar. 19, 2015); BLANCHARD, *supra* note 91.

93. Consolidated Appropriations Act 2016, Pub. L. No. 114–113 (2015), Cybersecurity Information Sharing Act of 2105, 129 Stat. 2242 (2016); BUSH, *supra* note 7.

94. Consolidated Appropriations Act 2016, Cybersecurity Act of 2105, Pub. L. No. 114–113, 129 Stat. 2242 (2016). *Accord id.* ("Including threats of serious bodily harm or economic harm, computer fraud, trade secrets violations, and several other criminal violations that have nothing to do with cyber attacks.").

know at the *time of sharing* to be personal identifiable information;[95] (6) the bill establishes that companies will primarily share information with the Department of Homeland Security (DHS), while it "requires DHS to establish processes to share the information it receives with other federal agencies," including intelligence agencies like the NSA, therefore, it is not transparent as to what the information is being used for; thereby, raising democratic legitimacy issues;[96] and (7) "unlike previous versions of cyber legislation, this bill includes no exemption to the liability waiver for gross negligence or willful misconduct," meaning companies may "overshare their user's personal, private information with complete immunity."[97]

Additionally, some have argued that it is impossible to prove that sharing data could prevent a cyberattack.[98] Therefore, if we are to look past the glaring disregard for individual civil liberties, we must look to the impact this legislation will have on preventing the theft of intellectual property through cyber economic espionage. Many have noted, including the President of the U.S., that information sharing alone is not enough.[99]

But is it even necessary to have legislation that asks companies to share this information? While the technical details are beyond the scope of this article, most commentators across disciplines agree that this bill, in and of itself, does not provide the necessary tools to combat this ever-increasing

95. Consolidated Appropriations Act 2016, Cybersecurity Act of 2105, Pub. L. No. 114–113, 129 Stat. 2242 (2016); NOLAN, *supra* note 2, at 45, ("Cybersecurity purpose," is a term of art that broadly encompasses nearly any effort that is aimed at protecting a system or network from a range of different cyberattacks).

96. KEANE, supra note 10 ("Senator Ron Wyden, from Oregon, called the bill 'badly flawed' filled with 'unacceptable surveillance provisions' that were in need of more rigorous debate. It contains substantially fewer oversight and reporting provisions than the Senate version did, he said, adding that bodies like the CIA will be less accountable for their actions and have few rules that compel them to take part in investigations into the use of data.").

97. *Oppose Omnibus*, *supra* note 8.

98. TEPLINSKY, *supra* note 1, at 282–319 ("corporations [can't] afford to rely solely on law enforcement efforts to track down and bring perpetrators to justice, as law enforcement is 'overwhelmed' by the problem, and hindered by a host of jurisdictional and other issues); *see also*, Mark Jaycox, *Congress Should Say no to Cybersecurity Information Sharing Bills*, EFF (Jan. 8, 2015), https://www.eff.org/deeplinks/2015/01/congress-should-say-no-cybersecurity-information-sharing-bills ("many security breaches are due to uneducated employees downloading malware.") *Accord,* Matthew Goldstein, Nicole Perlroth, and Michael Corkery, *Neglected Server Provided Entry for JP Morgan Hackers*, N.Y. TIMES (Dec. 22, 2014), http://dealbook.nytimes.com/ 2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?_r=0 ("the computer breach at JPMorgan Chase this summer — the largest intrusion of an American bank to date — might have been thwarted if the bank had installed a simple security fix to an overlooked server in its vast network").

99. The president has said that companies need to fill in the security gag by ensuring that they are protecting their consumers with at least basic protections, like a good password. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012), http://www.wsj.com/articles/SB10000872396390444330904577535492693044650.

problem. CISA essentially allows for better coordination against cyber threats, but does not provide the tools necessary to defend against those threats,[100] and will only "marginally help secure cyberspace."[101]

IV. Other Options the U.S. Has to Combat Cyber Economic Espionage

To provide at least a temporary solution or relief to the threat of cyber-economic espionage, the U.S. government should look to other options that may better help secure U.S. corporate entities intellectual property. Leading scholars have discussed three strategies: (1) using international law, (2) liability for private entities failing to meet basic security standards, and (3) allowing private entities with legislative guidance to engage in active self-defense. Each of these options poses a lesser privacy risk, as described below.

A. Using International Law to Create Global Norms

Many scholars have argued that domestic policy needs to be combined with diplomacy, whereby; international agreements are created to discourage cyber economic espionage.[102] In the past, the U.S. has attempted to enter into talks with China but the talks have failed to produce any results.[103]

However, existing principles of international law, such as state sovereignty and non-intervention laws, can evolve to address the issue of cyber economic espionage by implementing "norms" against cyber economic espionage, which can be established within already existing intergovernmental organizations.[104] These norms or practices can allow members of the organizations to assert claims of cyber economic

100. KALIA, *supra* note 89 ("CISA is fundamentally flawed in its approach to cybersecurity. Its information sharing regime wouldn't even fix the most recent public breaches, since it doesn't address basic problems, like unencrypted files, poor computer architecture, un-updated servers, and employees (or contractors) clicking malware links").

101. BRUNER, *supra* note 12, at 1470.

102. O'HARA, *supra* note 4, at 244; LOTRIONTE, *supra* note 15, at 471–72; Jyh-An Lee, *The Red Storm in Uncharted Waters: China and International Cyber Security*, 82 UMKC L. REV. 951, 963 (2014); Lawrence L. Muir, Jr., *Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth,* 71 WASH. & LEE L. REV. ONLINE, 73; LEWIS, *supra* note 30, at 189; *see also* TEPLINSKY, *supra* note 1, at 264 ("Tom Donilon, National Security Advisor to the President, delivered a speech to the Asia Society unequivocally setting forth the expectations of the U.S. with respect to China's role in cyber espionage. He said that building a constructive relationship with China is one of the pillars of the U.S. strategy in the Asia-Pacific region, and he identified cybersecurity as a 'growing challenge to [the U.S.-China] economic relationship'").

103. MUIR, *supra* note 102, at 83.

104. SKINNER, *supra* note 21, at 1194.

espionage.[105] This, in turn, would provide protection for users' privacy rights, and cause a foreign nation to be more cautious before engaging in state sponsored cyber economic espionage. However, for this model to work, a state would have to ensure that their cyberinfrastructure is not used for acts that "unlawfully affect other states," thus state responsibility is necessary to have cyber economic espionage covered within the bounds of international law.[106] This could seemingly work if a private entity were able to determine whether a foreign government was involved in the cyberattack, which they could do without providing the government with significant amounts of personally identifiable user information.

According to some scholars, one approach to regulate cyber economic espionage is through the World Trade Organization ("WTO").[107] The WTO already provides a framework that governs fair trade and competition; it has the authority to "ensure compliance" among member states.[108] The WTO protects intellectual and industrial property rights between member states through its treaties.[109] It is notable that China, who poses the most prominent threat in the area of cyber economic espionage, is a member of the WTO.[110] The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") provides for intellectual property rules and establishes levels of "protection that each government has to give the intellectual property of fellow WTO members, [thereby] bring[ing] protection of intellectual property under common international rule."[111]

The WTO requires that member states "protect innovative economic activity that is not necessarily developed or owned by the state itself, but rather by private economic actors."[112] The WTO also requires member states to protect other states' intellectual property, by not impeding on those rights.[113] Skinner argues that these rules may be interpreted to indicate that through TRIPS economic cyber espionage is prohibited.[114] While TRIPS does not directly address economic espionage, international law "fills the gaps left by treaties, unless there is a conflict between the provisions or an

105. *Id.* at 1191.

106. *Id.*

107. O'HARA, *supra* note 4; SKINNER, *supra* note 21 at 1194.

108. SKINNER, *supra* note 21, at 1165.

109. *Id.* at 1195.

110. Peter K. Yu, *Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats*, CARDOZO L. REV. 130, 134 (2015).

111. SKINNER, *supra* note 21, at 1195.

112. *Id.* at 1196.

113. *Id.* at 1195.

114. SKINNER, *supra* note 21, at 1197–98.

express exclusion of the customary principle."[115] Thus, because the WTO is designed to protect intellectual property it is "compatible with and reinforces the norms of economic sovereignty and noneconomic intervention, as well as the principle that states should be held responsible for the unlawful economic acts that they sponsor."[116]

Furthermore, the U.S., on its own, has failed to negotiate a treaty with China in a series of bilateral talks.[117] The WTO may be the appropriate authority to hold China responsible because China's ascension as a superpower depends on its reputation in the international community and part of maintaining a positive reputation is being a part of the "world economic community."[118] Thus, China needs the WTO's support.[119] Additionally, if some international agreement is not reached to propel China to circumscribe its use of economic espionage its relations with U.S. will continue to diminish.[120] This could have significant effects on the Chinese economy,[121] giving China even more incentive to agree to an international treaty.

One area of concern is that cyber attacks may be wrongfully attributed to China, which can cast doubt on whether international law can effectively enforce a treaty. Thus, some have argued that it may be imperative to "include[e] an enforcement system that features an elite professional staff, cutting-edge technology, and a robust international network."[122] Others have argued that cyber economic espionage is too new to develop customary international law.[123] However, the evolution of international law can be fueled by the needs of those affected by the activity.[124] Cyber economic espionage has the capacity to destabilize economies.[125] Therefore, an international treaty

115. *Id*.

116. *Id.* at 1204.

117. YU, *supra* note 110, at 150.

118. *Id.* at 1205.

119. *Id.*

120. *Id.*

121. MUIR, *supra* note 102, at 91.

122. LEE, *supra* note 102, at 965.

123. James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy*, 2 J.L. & CYBER WARFARE 64, 66 (2013), "the length of time to develop customary international law can vary greatly, but generally takes a significant number of years. The customary law of war has developed over thousands of years, but the practice of limiting conflict evolved primarily in the last 150 years."

124. SKINNER, *supra* note 21.

125. LEWIS, *supra* note 30, at 1179.

should play a role in combating the issue of cyber economic espionage, and the WTO may be the most effective forum to regulate it.

B. Companies Should Be Liable for Failing to Meet Regulatory Standards

Domestic policy is still a key component in tackling cyber economic espionage. However, bills like CISA may not be the best approach. One reform to domestic policy could be to hold companies liable for the failure to meet security standards, since "the national security implications of an insecure cyber network are just as significant, and in some ways more alarming, than the economic implications . . . insecure networks and compromised technology may threaten the U.S.'s ability to protect itself against its enemies."[126]

One substantial argument in favor of information sharing between private entities and the government was the theory that companies were not investing in cybersecurity and the collective mass of information would allow companies to easily fix their infrastructure. The reasoning given is that executives do not want to invest without a "clear understanding of the return on investment."[127] Reliable return on investment data would depend on "the frequency of cyber incidents, the costs of cyber incidents, and the effectiveness of mitigation methods."[128] This information, as some argue, could only be obtained through information sharing and offering protection to private entities.[129]

To counter this argument, it can be contended that without any threat of liability, information sharing will not incentivize private entities to invest in cyber security. Most corporations, due to recent public attacks, understand the threat of being targeted.[130] Furthermore, the National Institute of Standards and Technology ("NIST") has been active in creating a Framework for Improving Critical Infrastructure Cybersecurity.[131] Also, as long as the DOJ and FTC maintain that the rule of reason should apply to information sharing relating to cyber economic espionage, then the issues

126. BRUNER, *supra* note 12, at 1480.

127. TEPLINSKY, *supra* note 1, at 307–08.

128. *Id.*

129. *Id.,* "corporations may be reluctant to report cybersecurity breaches, for fear of repercussions in terms of compromised competitiveness, regulatory risk, consumer response, cost and/or reputation."

130. Companies such as Shadowcrew, Heartland Payment Systems, Target, and Anthem.

131. NAT'L INST. OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

relating to the lack of understanding on their return on investment would not apply.

Additionally, law suits would allow shareholders of public corporations to be "more aware of the threat of economic espionage and to apply pressure upon corporations to ensure that there are adequate internal safeguards for detecting espionage."[132] Recent litigation has shown that the FTC is willing to bring suits against companies for failure to maintain a set of standards that protect customer information.[133] In *Federal Trade Commission v. Wyndham*,[134] the FTC alleged that Wyndham had flawed security practices (including failure to erect firewalls, use appropriate passwords, or configure software to keep credit card information secure), and "FTC officials called the alleged security flaws 'obvious.'"[135] When a private entity has or should have the knowledge of a substantial economic espionage taking place, the FTC should be able to hold these companies liable for failure to secure their customers' information. Thus, bills like CISA should allow companies to be held liable for failure to meet cybersecurity standards.

C. Private Entities Should Be Allowed to Engage in Active Defenses or Hack Backs

Another approach to mitigate the threat of cyber economic espionage is a policy enabling private entities to engage in an active defense or a counteroffensive hack back.[136] This approach would allow a private entity to counterstrike the responsible party and refrain from handing over loads of data to the government. Teplinsky, among other scholars, argue that the use of passive defensive approaches by private entities is not enough because "determined adversaries will find a way to successfully breach even the most sophisticated and heavily fortified organizations, as demonstrated by the

132. LEWIS, *supra* note 30, at 220.

133. TEPLINSKY, *supra* note 1, at 303.

134. *F.T.C. v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602 (D.N.J. 2014).

135. *Id.*

136. BRUNER, *supra* note 12, at 1465–1486, a "hack-back is a method of cybersecurity that involves some level of retaliation, or 'counterstrike,' against the hacker . . . " counterstriking can range from things as simple as turning over the supposed hacker to law enforcement, to damaging the system to prevent it from perpetrating future attacks." *See also* TEPLINSKY, *supra* note 1; Jorge L. Contreras, Laura DeNardis, & Melanie Teplinksy, *Mapping Todays Cybersecurity Landscape*, 62 AM. U. L. REV. 113 (June 2013); Shane McGee, Randy V. Sabett, & Anand Shah, *Adequate Attribution: A Framework for Developing A National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1 (2013); BRUNER, *supra* note 12, at 1483.

successful attacks on DoD, RSA, Lockheed Martin, and Google."[137] However because the law limits the methods private entities may use as self-defense,[138] most secure their networks using only passive defense mechanisms.[139] Passive defense includes: "(1) controlling system access; (2) limiting data access; (3) security administration; and (4) secure system design."[140] Accordingly, in order for passive measures to ensure a network is secure it must work 100 percent of the time, if it does not, then hackers can keep making attempts to breach that network until they succeed.

Active defense, or a "hack back" can usually entail "(1) detecting the intrusion; (2) tracing the intruder; and (3) some form of counterstrike."[141] An example of a company engaging in an active defense occurred when Google, Inc.'s network had been infiltrated, and it was able to trace the servers to two Chinese educational institutions.[142] Google initiated a counteroffensive and hacked the source back, which allowed them to discover the possibility of the Chinese government's involvement in the attack.[143]

An important issue that relates to this approach is the attribution issue, whereby "attackers are traced using some form of traceroute technology."[144] Correctly tracing the source of a hack can happen, at best, 80 percent of the time.[145] It becomes increasingly harder when hackers spoof their Internet Protocol ("IP") address or use a third-party command and control system.[146] Such attribution problems are a cause for concern from a legal perspective, since a company may be held liable if it hacks an innocent bystander. Another concern is that private entities may respond "excessively or

137. TEPLINSKY, *supra* note 1, at 318.

138. BRUNER, *supra* note 12, at 1486, "section (a)(2) of the CFAA — the ban on unauthorized access for the purpose of obtaining information — should be amended to grant victims of cyberattacks criminal and civil immunity for the limited purpose of investigating their attackers. In practice, this would mean that network security professionals, businesses, or even private individuals who are technologically competent, would be able to use necessary means to: (1) access the attacking computer; and (2) gather information about the attack, its perpetrator, its origin, and its purpose — nothing more."

139. BRUNER, *supra* note 12, at 1483.

140. *Id.*

141. BRUNER, *supra* note 12, at 1485.

142. Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors As Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 276–77 (2013).

143. *Id.*

144. BRUNER, *supra* note 12, at 1485.

145. *Id.*

146. *Id.*; *see also* MESSERSCHMIDT, *supra* note 142, at 322, "when hackers are utilizing a large number of zombie or bot computers to carry out their hacks, some of which might be utilized by particularly vulnerable targets, such as hospitals."

disproportionately."[147] For these reasons, it is important that the state develop law and policies that will guide private entities in how to engage in a counter offensive.[148]

Despite these concerns, it is still important that companies have the option to engage in a counter offensive. For one, private entities "own the vast majority of [computer intelligence] in the U.S. and for that reason they are at a better position to identify attackers and "raise the cost of engaging in [cyber economic espionage]."[149] Further, some have argued that hack backs may be the best approach because government investigations take too much time, whereas an active defense is more rapid and could "significantly drive up the costs that hackers incur, deterring future conduct."[150] Additionally, if it is possible to accurately target the source of the hack, the "disruption caused by the hackback can raise the cost of hacking in the first place[;]"[151] it can also make hackers less effective by giving private entities the ability to be more knowledgeable on who is conducting the hack, thereby, conceivably allowing them to create effective barriers to entry — "potentially causing some hackers to exit the game due to ineffectiveness."[152] Therefore, the government should provide private entities the ability to engage in active defenses with some legislative guidance.

V. Conclusion

The essential difference between traditional espionage versus cyber economic espionage, is that cyber economic espionage has the ability to ruin a nation's economy and severely impact the global economy. This difference exposes the need for discernible political action.

The U.S. has recently attempted through various domestic policies to combat cyber economic espionage. The main strategy the U.S. has emphasized is information sharing between the private sector and the government as well as information sharing between private entities. The key

147. MESSERSCHMIDT, *supra* note 142, at 322.

148. *Id.*

149. CONTRERAS, *supra* note 136, at 1116.

150. MESSERSCHMIDT, *supra* note 142, at 293. *But cf*. BRUNER, *supra* note 12, at 1486 (stating that the attribution problem could create potential problems, for instance, where an innocent party is hackbacked (an attacker can use a third party's computer), the current state of technology for identifying attackers may not be sufficient to permit counter-offensive strategies.).

151. *Id.* at 321–322; *see also* BRUNER, *supra* note 12 (stating that hack backs increase the cost of hacking.).

152. BRUNER, *supra* note 12, at 1486.

legislation that was just secretly passed to promote information sharing was CISA. However, the U.S.'s domestic policy has caused considerably more harm than it has prevented cyber economic espionage. The overly broad protections the bill gives private entities effectively allows for an unregulated free-for-all of information sharing between the government and these entities. This has caused concern from many privacy advocates and it is the reason the bill has been dubbed the Second Patriot Act. Therefore, the law must evolve and move away from the notion that cyber economic espionage can only be combated through information sharing.

This note proposes three other methods that could be more effective in combatting cyber economic espionage, including: (1) a push for policy change in international law; (2) holding companies accountable for failure to meet certain regulatory standards; and (3) creating a policy framework that would give private entities the option to engage in active self defense. These outlined approaches do not represent an all-encompassing regulatory framework capable of definitively combating cyber economic espionage. However, the U.S. must shift away from the notion that information sharing is the key strategy in fighting cyber economic espionage. As those legislative policies stand, their effectiveness is substantially outweighed by their lack of protection for individual privacy rights.

***