Ocean and Coastal Law Journal

Volume 19 | Number 1 Article 2

2014

The Cloud And The Deep Sea: How Cloud Storage Raises The Stakes For Undersea Cable Security And Liability

Lixian Loong Hantover

THE CLOUD AND THE DEEP SEA: HOW CLOUD STORAGE RAISES THE STAKES FOR UNDERSEA CABLE SECURITY AND LIABILITY

Lixian Loong Hantover[*]

[T]he Internet is many things, in many places. But one thing it most certainly is, nearly everywhere, is, in fact, a series of tubes. There are tubes that connect London and New York. Tubes that connect Google and Facebook. There are buildings filled with tubes, and hundreds of thousands of miles of road and railroad tracks, beside which lie buried tubes. Everything you do online travels through a tube. Inside those tubes (by and large) are glass fibers. Inside those fibers is light. Encoded in that light is, increasingly, us.[1]

I. INTRODUCTION

Our data is moving into the cloud. While in the past we stored data on the computers on our desks, now we increasingly give control of our data to far-away professionals and give up our hard drives for storage online in the "cloud."[2] A PEW report in 2008 found that sixty-nine percent of Americans had either stored files online or used a web-based software application at least once.[3] Now over one exabyte, or over one

* J.D., UCLA School of Law; B.A. University of Chicago; Associate, Wilson, Sonsini, Goodrich & Rosati, P.C. I would like to thank Curtis Hessler for his help and encouragement and my parents for their constant support. In addition, I would like to thank Ciera Dye and the editors of the Ocean & Coastal Law Journal for their hard work. The views expressed in this article reflect the views of the author alone and do not necessarily reflect the views of Wilson, Sonsini, Goodrich & Rosati, P.C.

1. ANDREW BLUM, TUBES: A JOURNEY TO THE CENTER OF THE INTERNET 5-6 (2012). Blum writes this in response to Senator Ted Stevens' famous quote that the Internet is just a series of tubes. *Id.* at 5.

2. *Id*. at 230. The cloud refers to any storage on the Internet, but it is hardly cloudlike. *Id.* Data is in fact being stored on massive data centers. *Id.*

3. Janna Q. Anderson & Lee Rainie, *The Future of Cloud Computing,* PEW INTERNET & AM. LIFE PROJECT 8 (Jun. 11, 2010), http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx. This figure does not include popular cloud services like

billion gigabytes, of data is stored among the many cloud services like Gmail and Dropbox.[4] Amazon's S3 cloud storage service, which provides the cloud storage space for companies like Dropbox,[5] stores 762 billion objects.[6] That is enough for 108 objects per person on earth.[7] In 2013, the cloud market is predicted to grow by 18.5 percent.[8] By 2016, it is estimated that users will store more than one third of their digital content in the cloud.[9]

It is not just individuals accessing their documents via Dropbox that make up this migration to the cloud. Companies looking to save on expensive hardware and the salaries of the IT professionals required to maintain that expensive hardware are also looking toward the cloud for their own data storage.[10] Because individuals and businesses increasingly rely on the cloud to perform basic functions, reliable access to that cloud is not merely important – it is critical. The concerns about

---

Dropbox which launched in 2008 and has been accumulating users ever since. *See* Jason Kincaid, *Dropbox Acquires The Domain Everyone Thought It Had: Dropbox.com,* TECH CRUNCH (Oct. 13, 2009), http://techcrunch.com/2009/10/13/dropbox-acquires-the-domain-everyone-thought-it-had-dropbox-com/.

4. John Callaham, *Over One Exabyte of Data is Now Stored in the Cloud*, NEOWIN (Feb. 20, 2013, 02:45), http://www.neowin.net/news/research-firm-over-1-exabyte-of-data-is-now-stored-in-the-cloud. To put this amount of data in perspective, Eric Schmidt, the former CEO of Google estimated that the total of all human knowledge created from the dawn of man until 2003 amounted to five exabytes. James Bamford, *The Black Box*, WIRED (Mar. 30, 2012), *available at* http://www.wired.co.uk/magazine/archive/2012/05/features/the-black-box?page=all.

5. *Where Does Dropbox Store Everyone's Data?,* DROPBOX, https://www.dropbox.com/help/7/en (last visited Mar. 17, 2013).

6. Rich Miller, *Amazon: 762 Billion Objects Stored on S3 Cloud*, DATA CENTER KNOWLEDGE (Jan. 31, 2012), http://www.datacenterknowledge.com/archives/2012/01/31/amazon-762-billion-objects-stored-on-s3-cloud/. In this article, the cloud refers to both cloud services like Google, which are considered Saas (Software as a service) and cloud services like Amazon or Rackspace, which are considered Iaas (Infrastructure as a service).

7. *Id*.

8. Brandon Butler, *Gartner: Public Cloud Market to Grow 18.5% this Year*, NETWORK WORLD (Feb. 28, 2013), http://www.networkworld.com/news/2013/022813-gartner-public-cloud-267223.html.

9. *Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016*, GARTNER (June 25, 2012), *available at* http://www.gartner.com/newsroom/-id/2060215.

10. Joseph A. Schoorl, Comment, *Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls*, 80 GEO. WASH. L. REV. 632, 634-5 (2012); Pete Eppele, *Six Reasons to Move to the Cloud*, WIRED (Oct 4, 2012, 1:55 PM), http://www.wired.com/insights/2012/10/move-to-cloud-consider-saas/.

cloud storage are thus two-fold: the security of the data itself[11] and the security of our access to that data.[12]

This article focuses on the latter concern. Specifically, this article focuses on the security of one critical component of the global Internet infrastructure that we use to access the cloud: undersea cables. These cables once carried only transatlantic telegraph messages. Now they carry any kind of communication – telephone calls, emails, bank account transfers – across the globe.[13] Accessing files from the cloud is just one of the many ways we rely on this infrastructure.

As cloud storage grows and multinational companies begin to rely on these cables to access their files, the potential economic impact of a breach of these cables becomes catastrophic. This article argues that the growth in cloud storage has raised the stakes when it comes to undersea cable security by making our ability to access our day-to-day files dependent on them. Furthermore, it is unclear who, if anyone, would be responsible for the economic loss associated with a loss of access to those files.

Part II of this article explores the idea of cloud storage and how access to information in the cloud has become a global issue that relies on undersea cables. It examines the structural flaws in undersea cable security and the inability of the current legal system to compensate victims for the loss of access to data in the event of a breach of undersea cable security. Part III explores and critiques various solutions to ensure that access to data in the cloud remains safe from undersea cable breaches and that any economic loss due to cable breaches can be compensated. This article then advocates in Part IV for a solution that includes a shift of liability to cloud storage providers and increased redundancy requirements.

---

11. John Villasenor, *Addressing Export Control in the Age of Cloud Computing*, BROOKINGS 1 (July 25, 2011), http://www.brookings.edu/research/papers/2011/07/25-cloud-computing-villasenor.

12. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 637 (2011) (explaining the importance of access to information).

13. *See* PROTECTIVE SEC. DIVISION, DEP'T OF HOMELAND SEC., CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: CABLE LANDING STATIONS 7 (Draft - Jan. 15, 2004) *available at* http://info.publicintelligence.net/DHS-UCL-CV.pdf; BLUM, *supra* note 1, at 6. Stephen Malphus, the chief of staff to Federal Reserve Chairman Ben Bernake was quoted as saying that when communications networks go down, the financial sector does not merely grind to a halt, it snaps to a halt. MICHAEL MATIS, THE PROTECTION OF UNDERSEA CABLES: A GLOBAL SECURITY THREAT 1 (U.S. Army War College 2012), *available at* www.hsdl.org/?view&-did=718794.

II. UNDERSEA CABLES TODAY: USE, SECURITY, AND LIABILITY FOR DAMAGES

A. Why the Cloud (and the Global Economy) Needs Undersea Cables

These days, the answer to the question "where is my data" is no longer simple. In the past, the answer would have been "on my computer," "on this disk," or "on my server in my office." Now companies and consumers are moving their data to the cloud: a vast network of servers that can be accessed anywhere there is an Internet connection.[14] For users, the cloud enables them to be a few clicks away from their data no matter what computer they are using. If a user's computer breaks or becomes infected, the data in the cloud is insulated and can just be accessed from a different computer.[15] Put simply, your data is in on a separate server, which you can access from any Internet connected device. While the user, be it an individual or a company, might be in Los Angeles, the server with their data could be anywhere from Wyoming to Singapore.[16]

So if your files are on a server in Singapore and you are living in Los Angeles, how do you access these servers all around the world?[17] If asked, many of us might think that our communications are carried mostly over the air via satellite. Therefore, many of us may assume that we access the cloud via satellite connections – literally in the "clouds." But this is not the case.[18] In fact, it is estimated that satellites only have the capacity to carry seven percent of the total Internet traffic to and from

14. Schoorl, *supra* note 10, at 635; *see also* Jonathan Strickland, *How Cloud Storage Works,* HOW STUFF WORKS, http://computer.howstuffworks.com/cloud-computing/cloud-storage1.htm (last visited Sept. 4, 2013, 5:55 PM).

15. Schoorl, *supra* note 10, at 634.

16. For example, Google has servers in Singapore, Finland and Taiwan. *Data Centers*, GOOGLE, http://www.google.com/about/datacenters/inside/locations/ (last visited Dec. 4, 2012).

17. This article does not suggest that all access to data stored in the cloud utilizes undersea cables. If your data is stored in the same country or city that you are in, it is likely that no undersea cables will be used to access your data.

18. Douglas R. Burnett, *Cable Vision*, U.S. NAVAL INST. PROCEEDINGS, Aug. 2011, at 67 [hereinafter Burnett, *Cable Vision*]. *See also* Jon Brodkin, *Bandwidth Explosion: As Internet Use Soars, Can Bottlenecks be Averted?,* ARS TECHNICA (May 1, 2012, 9:40 AM), http://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/.

the United States.[19] Instead, it is the global undersea cable network that is the "fundamental medium of the global village."[20]

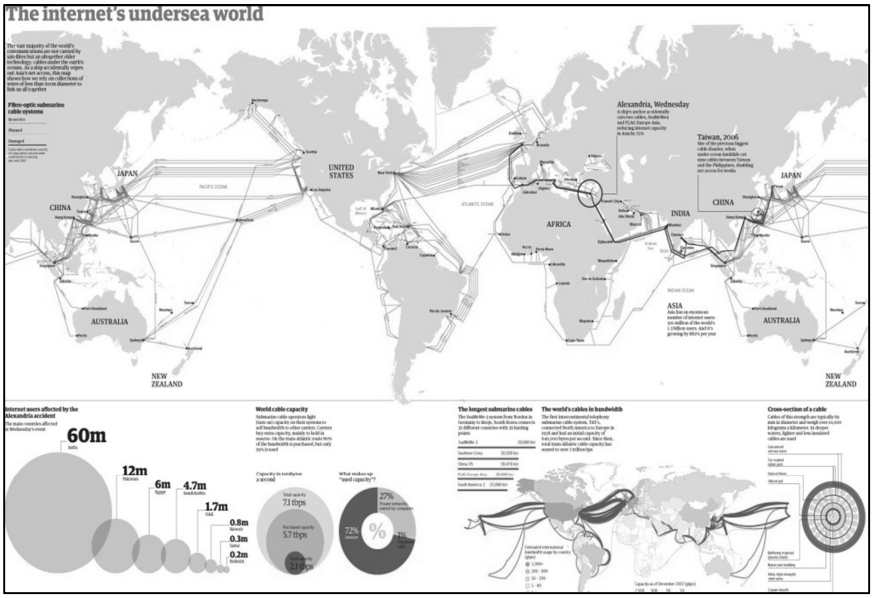

Fig. 1.1. Reprinted from Bobbie Johnson, *How One Clumsy Ship Cut Off the Web for 75 Million People*, THE GUARDIAN (London), Feb. 1, 2008, at 22.

This undersea cable network, illustrated in Figure 1.1, is made up of over two hundred submarine cables that crisscross the ocean floor,[21] carrying millions of messages and facilitating over one trillion dollars in daily transactions. [22] The longest cable, called the "Southern Cross"

19. Burnett, *Cable Vision*, *supra* note 18, at 67.

20. BLUM, *supra* note 1, at 193. *See also* Sebastian Anthony, *The Secret World of Submarine Cables,* EXTREME TECH (Sept. 21, 2011, 7:30 AM), http://www.extremetech.com/computing/96827-the-secret-world-of-submarine-cables ("Across these cables, which span distances of up to 13,00o [sic] km (8,000 miles) and have total lengths over 21,000 km (13,000 miles), terabits of information squirt from one side of the planet to another. To get from London to Tokyo, your packets can traverse Europe, the Mediterranean, the Red Sea, the Arabian Sea, the Indian Ocean, and finally the South China Sea — or they can hop across the Atlantic, the entirety of continental North America, and then long haul over the Pacific.").

21. John Brandon, *Protecting the Submarine Cables That Wire Our World*, POPULAR MECHANICS (Mar. 15, 2013, 1:00 PM), http://www.popularmechanics.com/technology/engineering/-infrastructure/protecting-the-submarine-calbes-that-wire-our-world-15220942?click=pm_latest.

22. MATIS, *supra* note 13, at 1.

stretches over 18,500 miles across the Pacific Ocean.[23] In addition, twelve more lines are scheduled for construction in 2013, which will connect more countries than ever before, including the small island nation of Tonga.[24] In the United States, just thirty-six cables carry more than ninety-five percent of all international voice, data and video communications.[25] Thus, the global communications system depends heavily on undersea cables, regardless of cloud storage.[26]

With the rise of cloud storage, our need to access international servers has increased our reliance on this global undersea cable infrastructure.[27] In general, undersea cables carry our data to servers to be stored, and subsequently carry requested data back from the servers to us.[28] If cables were severed between a user in Country A and a server on which the user's data was stored in Country B, the user would be unable to access their data.[29] Our access to the cloud and cloud storage currently relies on undersea cables.[30]

This is not to say that if one cable connecting Country A to Country B is cut, all Internet traffic between the two countries will cease. A single cut to a submarine cable "typically has little impact [on Internet traffic because] the communications may be rerouted through alternative

---

23. Brandon, *supra* note 21. "In 2004 alone, approximately $7.4 trillion [was] traded on cables transmitted between 208 countries [on a daily basis]." MATIS, *supra* note 13, at 1.

24. Brandon, *supra* note 21.

25. Burnett, *Cable Vision, supra* note 18, at 67. *See also* MATIS, *supra* note 13, at 9 (stating that "[i]f the exact location[s] of the [thirty-six] cables in the [United States] were identified, a successful [terrorist] attack on a few of those locations could affect roughly [ninety-five] percent" of Internet traffic on the East Coast).

26. Bamford, *supra* note 4, at 83. This dependence on undersea cables will only increase because global Internet traffic is estimated to reach 966 exabytes per year by 2015. *Id*. Many of the security risks and subsequent liability issues discussed in this article apply just as readily to other services that rely on undersea cable infrastructure. This article focuses on access to data in the cloud but acknowledges that disruptions to other cloud-reliant services could be equally catastrophic. For example, given the reliance of the financial industry on these cables to transfer billions of dollars per day, a large-scale disruption could cripple the industry.

27. *See, e.g., SEACOM Upgrades Submarine Network Capacity to Turbo-Boost African Internet,* SEACOM (Mar. 11, 2013), http://www.seacom.mu/news/article-124/seacom-upgrades-submarine-network-capacity-to-turbo-boost-african-internet/ (noting that the rise in cloud computing has been cited as a reason to upgrade undersea cables).

28. *See* Brandon, *supra* note 21.

29. *Id.*

30. *Id*.

cables."[31] Countries like the United States, for example, are connected to the outside world by multiple cables.[32]

As the amount of cable disruptions increases (i.e., more cables are cut), on the other hand, the amount of data traffic that is lost increases exponentially.[33] For example, an analysis was done of possible disruptions of the cable lines connecting Europe and India.[34] It found that although "India is fairly resilient in the case of one or two cable disruptions," nearly seventy percent of traffic to and from India would be lost with just three concurrent cable disruptions.[35] Actual data exists that supports similar predictions.[36] In 2006, an earthquake along the coast of Taiwan triggered undersea landslides and broke nine undersea cables.[37] This event had repercussions extending beyond the country of Taiwan.[38] Internet telecommunications linking Southeast Asia were seriously impaired.[39] More than six hundred gigabits of capacity went offline, and trading of the Korean won temporarily stopped.[40] Even a week after the quake, an Internet provider in Hong Kong publicly apologized for continued slow Internet speeds.[41]

If companies and users continue to move their data into the cloud, and therefore continue to rely more on undersea cables to access the cloud for their day-to-day needs, we must consider two key problems. First, we must consider structural issues, which concern potential

---

31. John K. Crain, Assessing Resilience in the Global Cable Infrastructure 13 (Jun. 2012) (unpublished M.S. thesis, Naval Postgraduate School) (on file with the Naval Postgraduate School), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA562772; *but see* Tom Parfitt, *Georgian Woman Cuts off Web Access to Whole of Armenia*, THE GUARDIAN, (Apr. 6, 2011, 15:12) http://m.guardiannews.com/world/2011/apr/06/georgian-woman-cuts-web-access (a 75 year old woman in Georgia cut one terrestrial cable with her shovel and accidentally cut off the Internet for the entire country of Armenia).

32. That being said, all but one of the U.S. transatlantic cables lands within the same thirty-mile radius on the east coast of the United States. Limited access to landing stations in the United States has created chokepoints for cables, increasing the vulnerability of the system as a whole. MATIS, *supra* note 13, at 7.

33. Crain, *supra* note 31.

34. *Id.* at 35.

35. *Id.* at 41. It is important to note that these disruptions did not even have to occur in Indian waters; some of the more devastating scenarios involved breaches off the coast of France. *Id.* at 47.

36. *Id.* at 9.

37. *Id.*

38. *Id.*

39. *Id.*

40. BLUM, *supra* note 1, at 200.

41. *Id.*

disruptions to the undersea cable infrastructure. Second, we must recognize liability issues, which relate to the fallout of large-scale disruptions. Who will compensate parties for the ever-increasing potential economic damages? How do we protect companies and users from the economic impact undersea cable disruptions will have on them?

The security concerns about undersea cable disruptions are by no means new. In World War II, for example, undersea cable operators in Porthcurno, England installed flamethrowers on beaches and took other precautions to protect cable stations against Nazi sabotage.[42]

Likewise, the question of who will pay for damage caused by cable disruptions is not a new concern and has been litigated extensively.[43] The stakes, however, have changed because cables no longer concern only communication. Now financial markets and multi-billion dollar businesses rely on the efficiency and strength of the undersea cable infrastructure.[44] Individuals and entities rely on cables not only to communicate or transfer funds, but also to access their day-to-day files.[45] As a result, the adoption of cloud storage has drastically increased the potential economic fallout of a major cable disruption. The rise of cloud storage has not created the problem of undersea cable security and liability; it has simply made these problems critical.

---

42. *Id.* at 203-205; *see also* Burnett, *Cable Vision*, *supra* note 18, at 69. In fact cable cutting as a tactic of war spans all the way back to the Spanish American War when the United States cut the cables linking Spain to its colonies. BLUM, *supra* note 1, at 200. Similarly, the first offensive action taken by the British Navy during World War I was to cut off Germany's links to the rest of the world by severing its undersea cables. *Id.*

43. *See, e.g.,* AT & T Corp v. Tyco Telecomms., Inc., 255 F. Supp. 2d 294, 307 (S.D.N.Y. 2003) (confirming an arbitration award requiring the owner of a vessel that severed a submarine underwater transatlantic telecommunications cable to compensate the owners of the cable for damages incurred in repairing the cable and restoring affected traffic by rerouting it across other networks while repairs were being completed); Brooklyn E. Dist. Terminal v. United States, 287 U.S. 170, 177 (1932) (libel in admiralty).

44. The financial sector would not suffer from the effects of a cable breach in isolation. Industries enmeshed in the global economy through the Internet also include shipping, airlines and manufacturing. Burnett, *Cable Vision*, *supra* note 18, at 67; *see also* MATIS, *supra* note 13, at 3 (stating that "[w]hen a cable loses service, it has a definite, but difficult impact [on] the global financial sector"). The International Cable Protection Committee (ICPC) legal advisor estimates that interruptions of underwater fiber optics communications systems have a financial impact in excess of one and a half million dollars per hour. MATIS, *supra* note 13, at 3.

45. *Id.*

B. Structural Vulnerability of Undersea Cables: Breaks are Likely to Occur

The previous section discussed how merely a few simultaneous breaches of undersea cables could cause huge disruptions in data traffic and therefore have huge ramifications for businesses relying on those cables. But how likely is it that simultaneous disruptions will actually occur? Are the cables themselves safe? Structurally, undersea cables are extremely vulnerable and therefore disruptions are likely. Despite the huge amounts of data traffic that flow through these cables, each one is merely the size of a garden hose.[46] In water depths of less than fifteen hundred meters, cables are buried in yard-deep trenches beneath the ocean floor and armored with a steel sheath.[47] This helps to protect against the most common kind of undersea cable disruption: accidental breakage by trawl fishing and ship anchors.[48] In water depths in excess of fifteen hundred meters, however, where breakages from anchors are unlikely, cables are laid on the ocean floor and are otherwise unprotected.[49] Even with these precautions, there are an average of two hundred cable faults[50] worldwide each year.[51]

Although the majority of these faults are caused unintentionally by anchors, fishing equipment, and occasionally sharks,[52] terrorism and piracy are genuine concerns.[53] The location of cables along the ocean floor is made readily available to mariners, commercial bottom fishermen, and undersea seabed developers so that they do not accidentally damage the cables.[54] Anyone who wishes to tamper with the cables by cutting or using explosives[55] could easily access their location via the Internet.[56]

---

46. Burnett, *Cable Vision*, *supra* note 18, at 67.

47. MATIS, *supra* note 13, at 8.

48. Of the roughly two hundred submarine fiber-optic cable faults worldwide every year, up to seventy-seven percent are caused by anchors and fishing gear. Burnett, *Cable Vision*, *supra* note 18, at 67.

49. *Id.*

50. In this article, the terms "fault," "breach," and "disruption" are used interchangeably.

51. Burnett, *Cable Vision*, *supra* note 18, at 67.

52. *Id*.; *see also* Sudmike, *Shark Attack on Subcable*, YOUTUBE (Apr. 22, 2010), http://www.youtube.com/watch?v=1ex7uTQf4bQ.

53. Burnett, *Cable Vision*, *supra* note 18, at 67.

54. MATIS, *supra* note 13, at 2.

55. *Id.* at 13.

56. *Id*. at 2.

Undersea cable expert Douglas R. Burnett argues that "it is naïve to assume that submarine-cable landing stations, cables, the cable ships, and the marine depots that maintain the systems will escape asymmetric terrorist acts,"[57] and recent cases have proven that Burnett's concern is not unfounded. In 2007, "piracy was blamed in the theft of active submarine cables and equipment" off the coast of Vietnam.[58] "In early 2008, over the course of just a few days, multiple cables were cut off the coasts of Egypt and Dubai," causing at least fourteen countries to lose a significant amount of data traffic.[59] The "Maldives was entirely disconnected from the rest of the world."[60] The short time span and close proximity of these cuts raised suspicions of a deliberate attack.[61] Most recently, in June 2010, terrorists in the Philippines struck an international cable.[62] The public location of the cables and their lack of sophisticated armor or protection make them incredibly vulnerable to intentional attacks.

A further concern is the security of cable landing stations. These stations are the "dry" component of the undersea cable infrastructure that connects the undersea cables to domestic terrestrial cable infrastructure.[63] The landing stations are above ground and highly visible and thus are vulnerable to attack.[64] These attacks need not be as sophisticated as attacks on undersea cables. For example, cars with explosives could be parked close to a landing station.[65] While damage to cable stations can be more easily repaired than breaches that occur in the deep sea, these cable landing stations often serve multiple undersea cables.[66] As a result, a successful attack on one cable landing station can simultaneously disrupt multiple cables.[67]

---

57. Burnett, *Cable Vision*, *supra* note 18, at 69.

58. Crain, *supra* note 31, at 9.

59. *Id.*

60. *Id.*

61. *Id.*; *but see* Bobbie Johnson, *How One Clumsy Ship Cut Off the Web for 75 Million People*, THE GUARDIAN (Jan. 31, 2008), http://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet (reporting that the cut was initially thought to have been the result of a boating accident).

62. Burnett, *Cable Vision*, *supra* note 18, at 69.

63. DEP'T OF HOMELAND SEC., *supra* note 13, at 3-6.

64. *Id.* at 7.

65. *Id.* at 9 (listing many security vulnerabilities of cable landing stations).

66. *See id.* at 7.

67. *See* SUBMARINE CABLE NETWORKS, http://submarinenetworks.com/stations/north-america (last visited Sept. 23, 2013) (listing U.S. cable stations and the undersea cables that they serve). The U.S. satellite system contains similar "earth stations" that house

C. Governments Are Not Taking Adequate Measures to Protect Undersea Cables and Deter Attackers

Perhaps even more troubling than the above-mentioned structural vulnerability of undersea cables is the lack of security efforts and criminal sanctions by governments to protect undersea cables and deter future attacks.[68] U.S. National Intelligence director James Clapper recently testified that cyber attacks, (by which he meant purely digital attacks like computer worms or viruses that can shut down the electrical grid or financial markets),[69] are the nation's number one security priority.[70] Clapper highlighted how much governments, utilities, and financial services rely on the Internet and therefore are vulnerable to cyber attack.[71] Yet at the same time, protection of undersea cables (a critical infrastructure that supports the Internet) from physical attacks is sorely lacking. For example, in the United States, the willful destruction of an international submarine cable is punishable by a maximum of two years in prison and a mere $5,000 fine.[72] This fine is hardly a deterrent, and is far out of proportion to the damage that such an act would cause. Furthermore, the United States has not joined the 162 countries that have signed onto the United Nations Convention on the Law of the Sea (UNCLOS).[73] As a result, there are no UNCLOS security protections for

---

numerous receivers, Bamford, *supra* note 4, at 83, and are thus vulnerable to the same kinds of attacks as cable landing stations. For example, one of AT & T's powerful earth stations, located in Roaring Creek, Pennsylvania, houses three 105-foot dishes that handle much of the U.S. communications to and from Europe and the Middle East. *Id.* Another AT & T earth station in California contains three dishes that service the Pacific Rim and Asia. *Id.* An attack on one of these stations could significantly disrupt satellite communication. While this article does not discuss the U.S. satellite system and its security in detail, it is definitely worth further study.

68. Burnett, *Cable Vision*, *supra* note 18, at 68.

69. A cyber-attack is usually thought of as a completely digital attack that utilizes a computer network or system to carry out the attack. *Cyberattack*, TECHOPEDIA.COM, http://www.techopedia.com/definition/24748/cyberattack (last visited Mar. 21, 2013). However, Oona Hathaway and her co-authors have advocated for a definition of "cyber attack," which focuses on the ends (attacking cyber systems). Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 826-27 (2012). A bombing of an undersea cable meant to disrupt the Internet would fall under Hathaway's definition of cyber-attack because its intended effect is to disrupt the cyber system. *See id.*

70. Matt Vasilogambros, *America's 3 Biggest Cybersecurity Vulnerabilities*, NAT'L J. (Mar. 13, 2013, 4:00 PM), http://www.nationaljournal.com/whitehouse/america-s-3-biggest-cybersecurity-vunerabilities-20130313.

71. *Id.*

72. 47 U.S.C.A. § 21 (2006); Burnett, *Cable Vision*, *supra* note 18, at 68.

73. *Id.* at 69.

U.S. undersea cables outside of U.S. waters.[74] Only Australia and Singapore have created a single point of contact within their governments to address issues of undersea cable security and to coordinate with cable owners to combat hostile actions.[75] On a worldwide level, no organization is responsible for undersea cables and there have been no international tests of cable defense systems.[76] The maintenance and security of the cables is left to private trade organizations.[77] Given the extent to which governments themselves rely on these cables,[78] the current lack of a coherent undersea cable security strategy by governments must be remedied. The infrastructure itself is vulnerable, and governments like the United States are not yet taking adequate actions to protect it. It is not enough for governments like the United States to focus on digital attacks on Internet systems. They must also take action to protect the physical structure of the Internet.[79]

D. Who Pays for the Damages Resulting from Undersea Cable Disruptions?

The second issue surrounding undersea cables is the question of liability. In the event that a breach of an undersea cable does occur, who pays for the damage? In 1998, the privately owned TAT-10 undersea cable than runs across the Atlantic Ocean was severed by a ship operated

74. Burnett, *Cable Vision*, *supra* note 18, at 69.

75. *Id.* at 70.

76. MATIS, *supra* note 13, at 10.

77. Burnett, *Cable Vision*, *supra* note 18, at 67-69.

78. MATIS, *supra* note 13, at 10 (explaining that the Department of Defense's net-centric warfare and global information grid rely on undersea cables and that breaches to these cables would risk the capabilities of modern U.S. warfare).

79. The Obama administration recently released an executive order on cybersecurity. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013). Part of the order focused on the need to develop a framework to gather and share intelligence on risks to privately owned critical infrastructure. *Id.* This is a step forward in that it indicates awareness that there is a lack of protection of critical infrastructure. However, it is unclear what this intelligence framework would entail and how much the government would be involved in the physical protection of Internet infrastructure. *See id.*; *see also* Roland L. Trope & Stephen J. Humes, *By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities*, IEEE SEC. & PRIVACY (Mar./Apr. 2013), *available at* http://www.hklaw.com/files/Publication/ab69bb14-30d2-41f0-bcab-5ae08947a7ab/Presentation/PublicationAttachment/5226c0f7-8993-48a0-9c40-6262cef78e27/By%20Executive%20Order%20%28final%20submission%20draft%29.pdf (analyzing the implications of the executive order for infrastructure providers).

by Tyco, Inc.[80] Tyco was ordered to pay the owners of TAT-10 over five million dollars in damages.[81] This amount included not only costs incurred in repairing the damaged cable but also the costs incurred by the owners of TAT-10 when they had to re-route the traffic via rival-owned undersea and terrestrial cable lines.[82] This scenario, in which one party negligently severs a cable belonging to another party, is the typical case addressing damages to undersea cables after they occur. In these cases, both in the United States and internationally, the party that causes the breach is liable to the cable owner for the costs of repair and replacement.[83] For example, in the United States, cable owners recover based on the law of torts.[84] The doctrine of trespass to chattel (in this case, the cable) enables a cable owner to recover for loss of use based on difference in value or cost of repair.[85] In cases like *AT & T v. Tyco*, this measure of damages has been interpreted to include the costs of rerouting traffic to other cables.[86] On average, the cost of a single repair is one to three million dollars plus.[87] Costs vary based on factors such as the distance between the breach and the repair ship, weather, coastal state permitting requirements, and the engineering skills of the crew.[88]

Not included in these cases are economic damages to third parties who are unable to conduct business when cable lines go down, whether they be individual consumers or multinational companies. These cases merely involve the cable owner and the tortfeasor who damages the cable. The question remains whether third party consumers who rely on the cloud have a cause of action against either the party who causes the cable fault or the cable owners themselves for losses that they incur from not being able to access their data.[89]

What would this potential claim look like? In most cases of undersea cable breaches, which are due to anchors or trawl fishing, a

---

80. AT & T Corp. v. Tyco Telecomms., Inc., 255 F. Supp. 2d 294, 297 (S.D.N.Y. 2003).

81. *Id.* at 298.

82. *Id.*

83. Douglas R. Burnett, *Recovery of Cable Repair Ship Cost Damages From Third Parties That Injure Submarine Cables*, 35 TUL. MAR. L.J. 103, 122 (2010) [hereinafter Burnett, *Recovery*].

84. *See id.* at 112.

85. *Id.*

86. *AT & T Corp.*, 255 F. Supp. 2d at 302.

87. Burnett, *Recovery*, *supra* note 83, at 108.

88. *Id.* at 108-109.

89. Note that this section and other sections in this article that have to do with issues of ex-post liability are focused on U.S. law only. However, many of the ideas could potentially be applicable in other countries as well.

tortfeasor's negligence leads to the cutting of one cable.[90] Cable operators are typically prepared for this and have created re-routing agreements whereby one cable company agrees to carry the traffic of its competitor should the competitor's cable sustain damage and vice versa.[91] As a result, the dangers of severe economic damage to third parties are slim in these cases. On the other hand, a natural disaster or pirate or terrorist attack that disables several cables simultaneously could lead to loss of access to data, as both the original cable and the re-routing cable would potentially be severed. Repairs often take up to one to two weeks to complete.[92] As a result, companies and users could lose access to their data for a prolonged period of time and could incur huge amounts of financial losses.[93] These users would look to the legal system to recover for the economic damage they had suffered. Unfortunately, it is unlikely that the current legal framework offers them much recourse.

Firstly, who would these users sue to recover? In the case of natural disasters, there is no tortfeasor from whom to recover. In the case of pirates or terrorists there are issues of sovereignty,[94] and even if there were not, these tortfeasors would probably not have the means to compensate victims. The only feasible claim is against the owner of the cables themselves, which would in turn be backed by insurers. Users would want to bring actions under tort law against cable companies (who would hopefully have adequate insurance) for negligence in failing to take precautions against foreseeable attacks and disasters.[95]

Unfortunately for these consumers, the majority rule in tort actions is that damages for "economic loss" are not recoverable on a negligence claim when the economic damages are not accompanied by property

90. *See* Burnett, *Recovery*, *supra* note 83, at 104.

91. *AT & T Corp.*, 255 F. Supp. 2d at 297.

92. MATIS, *supra* note 13, at 6.

93. These damages could range from lesser amounts for a small business that is unable to operate for a day to huge amounts for businesses like financial institutions that can handle trillions of dollars and millions of transactions each day. *See, e.g.,* Burnett, *Cable Vision, supra* note 18, at 67.

94. *Id.* at 68 (discussing how prosecuting pirates has proven difficult because of these issues).

95. It is not that these terrorist attacks are not foreseeable. The vulnerability of the undersea infrastructure and increased frequency of attacks makes a simultaneous attack on the cable infrastructure if not probable, at least foreseeable. However, from a broader policy perspective, it is unclear whether we would want consumers to be able to bring actions against cable companies. If companies knew they were potentially on the hook for billions of dollars in damage they would likely be unable to obtain insurance and may choose to exit the market entirely.

damage.[96] Exceptions to the economic loss rule cover cases involving physical injury or malpractice suits against lawyers and accountants, but do not apply to this situation.[97] In the case of undersea cable disruptions, users have not themselves incurred any physical damage. They have only lost revenue due to the loss of access to their data. As a result, it is unlikely a court would allow recovery for these economic damages in claims of negligence against cable owners. Consumers relying on cloud storage may find themselves unprotected from losses of data due to undersea cable damage.

It is possible, however, that contract law could provide some recourse in situations where the consumer and the cable operator are in contract with one another. In cases governed by contract law, damages are controlled by terms in the contract.[98] In recent years, cloud based service providers have themselves become owners of undersea cable infrastructure.[99] Facebook recently joined a consortium building a new

96. ROBERT L. DUNN, RECOVERY OF DAMAGES FOR LOST PROFITS § 3.6 (6th ed. 2005). Future scholarship may want to begin to broach the topic of when information becomes property or if the loss of access to data can ever be considered a property loss. However, this article assumes that for now at least, a loss of access to data is not damage to property.

97. *Id.* at § 3.8. Even if a court did allow companies to recover from cable owners, there would still be the issue of whether the economic loss in question was too tenuously removed from the damage to the cable. In *Kinsman Transit Company v. City of Buffalo*, a ship belonging to the Kinsman Transit Company became unmoored and crashed into and destroyed a bridge. Kinsman Transit Co. v. City of Buffalo, 388 F.2d 821, 822 (2d Cir. 1968). The two plaintiffs in the case brought suit against the transit company and the city of Buffalo to recover for economic loss. *Id.* at 824. Plaintiff A brought suit because as a result of the bridge being unavailable, it was unable to transport its wheat and had to purchase replacement wheat to fulfill a contract. *Id.* at 823. Plaintiff B sought to recover the costs of equipment it was forced to rent to unload its cargo from a ship that was blocked by ice due to the accident. *Id.* The court in both cases found that the damage to the plaintiffs was too 'remote' or 'indirect' a consequence of the defendants' negligence and denied their requests for recovery. *Id.* at 824. It is likely in the case of cable damage and subsequent loss of data that the economic damage would be considered even more tenuous.

98. DAVID W. TOLLEN, THE TECH CONTRACTS HANDBOOK 108 (2010). Tollen gives a good and relevant example to illustrate how this works: "Imagine the provider supplies defective software. The software malfunctions, and as a result, the recipient loses a million dollars. Imagine also that the limitation of liability clause caps the provider's liability at $50,000. The result: the provider is liable for *one twentieth* of the recipient's loss. Even if everyone agrees the malfunction was the provider's fault, the provider owes $50K, and that's all." *Id.*

99. Robert McMillan, *Facebook Mimics Google with Underwater Cable to Asia*, WIRED (Jul. 5, 2012), http://www.wired.com/wiredenterprise/2012/facebook-submarine/.

undersea cable in Asia.[100] In doing so, it follows in the footsteps of Google which helped pay for an undersea cable connecting Japan to the United States.[101] Thus it is possible, depending on the contract terms, that consumers could recover from cloud providers who are also cable owners (like Google) that they are in contract with, if the cable breach leads to downtime in the cloud data storage service. However, here the largest obstacle is the contract itself. Consumers who use Google Docs to store their work documents must sign an agreement that absolves Google of any liability for economic harm to the consumer.[102] This provision would likely absolve Google of having to pay a consumer for the loss they experience should a cable be breached.[103] The only exception would be if a court found the contract to be unconscionable or opposed to public policy.[104] But this would be unlikely to occur.[105] In contracts, as in torts, it is unlikely that a user would be able to recover for economic harms suffered even if those harms rose into the billions of dollars.

III. HOW TO PROTECT VULNERABLE INFRASTRUCTURE AND PROVIDE RECOURSE FOR CABLE BREAKS: POSSIBLE BUT PROBLEMATIC SOLUTIONS

Part II demonstrated not only that the physical infrastructure of undersea cables is vulnerable to intentional disruptions, but also how difficult it would be for those affected by a disruption to recover for any economic loss they experience as a result of losing access to their data. With cloud computing on the rise, it has never been more critical to ensure the safety of the world's undersea cables. Should a breakage occur, cloud computing customers will need to have some recourse to recover for their economic loss. This Part explores and critiques possible

100. *Id.*

101. *Id.*

102. Andrew Couts, *Upload at Your Own Risk: Most Cloud Storage Services Offer No Data Guarantee,* DIGITAL TRENDS (Jan. 30, 2012), http://www.digitaltrends.com/computing/upload-at-your-own-risk-most-cloud-storage-services-offer-no-data-guarantee/.

103. *Id.*

104. TOLLEN, *supra* note 98, at 111.

105. *See generally* Melissa T. Lonegrass, *Finding Room for Fairness in Formalism – The Sliding Scale Approach to Unconscionability*, 44 LOY. U. CHI. L.J. 1, 1-5 (2012) (discussing how the area of unconscionability in boilerplate contracts is evolving). However, it is hard to imagine judges voiding contracts and thus opening up companies to huge amounts of liability, especially when the user is a company that could have stored its data elsewhere.

but problematic solutions to the structural and liability issues raised in the previous sections. Part IV then advocates for a proposal incorporating data redundancy, government subsidized insurance, and shifted liability aimed specifically at safeguarding access to the cloud.

Possible Solution A: Increase Security and International Preparedness

Most of the solutions that have been put forward by scholars focus on the structural security issues alone and what governments must do to secure this vital infrastructure. Douglas Burnett argues that governments should follow the lead of Australia and Singapore and coordinate a single point of contact for undersea cable issues.[106] He suggests that the U.S. Navy should reach out to naval allies such as Canada and France as well as to cable industry representatives and together develop cable-protection strategies that enable the navy to respond quickly to pirate and terrorist attacks.[107] Commander Michael Matis of the U.S. Navy recommends creating a new international cable construction regulatory regime that would promote greater international cooperation and information sharing.[108] As part of that effort, he urges the United States to immediately ratify UNCLOS and encourages UNCLOS members to collectively update their legislation to protect cables and make it an international crime to tamper with them.[109] These scholars understand that any action to increase the safety of undersea cables must be international. Models have shown that a cable break off the coasts of Marseille could have detrimental effects on data flow in and out of India.[110] In other words, merely increasing security in one's own waters will not be sufficient. Any security strategy must be global in scope.

Even if both of the above plans are implemented, however, this will likely still not solve the problem of structural security. Autonomous undersea vehicles are now commercially available and can easily dive to the depths where undersea cables are left unprotected and render them inoperable by cutting them or laying explosives.[111] Unlike in aviation, undersea vehicles are very hard to find due to low light underwater and

106. Burnett, *Cable Vision*, *supra* note 18, at 70-71.

107. *Id.*

108. MATIS, *supra* note 13, at 18.

109. *Id.* at 15-18.

110. Crain, *supra* note 31, at 46-47.

111. *See* MATIS, *supra* note 13, at 12; Laurence R. Wrathall, Comment, *The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward*, 12 SAN DIEGO INT'L L.J. 223, 237-38 (2010).

thus low visibility.[112] Radars can scan thousands of square miles of air space but there is no equivalent system underwater.[113] Even with unprecedented cooperation amongst naval forces, it is virtually impossible to completely police the thousands of miles of undersea cable infrastructure.[114] Therefore, while a ratification of UNCLOS or increased international cooperation will likely be helpful and increase global preparedness, it will not be enough to prevent many attacks.

Possible Solution B: Keep All Data Within a Country

One solution is to simply do away with the need for undersea cables altogether when it comes to data storage in the cloud. Some cloud storage providers such as Google have allowed customers to pay a premium and specify where their data is to be kept.[115] In Google's contract with the City of Los Angeles, Google guaranteed that the city's data would remain within the contiguous forty-eight states.[116] While this solution does eliminate the reliance on undersea cables for data storage, it is problematic. Firstly, the ability of customers to choose where their data is stored may not be available to smaller customers with limited bargaining power.[117] More importantly, in today's global economy, having data servers limited to the United States is unrealistic. Many companies, large and small, have customers or offices all around the world. No matter where their data servers are located, undersea cables will have to be relied upon because some customers will not be located in the same country as the data server. Having data stored in servers in every country where a company operates or has customers rather than in several strategic servers in a few countries is economically inefficient. While this solution may work for some customers like the City of Los Angeles, it is not a viable solution for most.

---

112. Wrathall, *supra* note 111, at 234.

113. *Id.* at 234-35. Wrathall explains that underwater concealment maximizes the impact that a small number of operatives can have, allowing them to place explosives in multiple locations over an extended time frame and later conduct a coordinated simultaneous strike. *Id.*

114. *See id*.

115. Schoorl, *supra* note 10, at 636.

116. Patrick Thibodeau, *Microsoft's Cloud-Enabled Office 2010 Set to Join Battle with Google*, COMPUTERWORLD (Apr. 8, 2010), http://www.computerworld.com/s/article/9175019/Microsoft_s_cloud_enabled_Office_2010_set_to_join_battle_with_Google.

117. Schoorl, *supra* note 10, at 637.

Possible Solution C: Creation of a Fund for Data Disruption Victims or a Subsidized Insurance Plan

Part II explained that the current U.S. legal framework is unlikely to provide recourse for cloud computing users in the event that there is a breach of undersea cables and they lose access to their data. As we rely more and more on undersea cables to form the backbone of our businesses and economy, the amount of possible economic losses that users could face begins to reach catastrophic levels. Often in cases of catastrophes, like floods, the BP oil spill and the terrorist attacks of September 11th, a fund is created whereby parties who have suffered a loss due to the event can recover, even if their damages are purely economic in nature. For example, the BP oil spill was the worst oil spill in U.S. history.[118] The spill had a huge effect not only on the wildlife in the Gulf of Mexico and local fishermen, but on the communities surrounding the gulf as well. In New Orleans, there was a twenty-eight percent drop in tourism even though the city was 150 miles away from the spill.[119] The economic effects of the oil spill rippled far beyond the accident site. As a result, BP created a fund of over twenty billion dollars to compensate those affected.[120] The fund allowed claimants to recover for purely economic damages.[121] In this case, it was BP, the negligent party, who contributed to the huge recovery fund.

In the case of the BP oil spill, the tortfeasor had immense funds at its disposal and was easily identifiable as the responsible party. BP caused the spill and BP provided the funds to compensate the victims.[122] In situations involving natural disasters or terrorist attacks, however, it is often the government, the insurer, or if all else fails, the victim, who

118. *See* Linda S. Mullenix, *Prometheus Unbound: The Gulf Coast Claims Facility as a Means for Resolving Mass Tort Claims--A Fund Too Far*, 71 LA. L. REV. 819, 819 (2011).

119. Allan Kaner et al., *Mass Torts Litigation Forum: The Deepwater Horizon Gulf Oil Spill*, AMERICAN BAR ASSOCIATION 5 (2010), http://www.kslaw.com/Library/publication/ABAMassTortsLitigationForum-Reigle-August-2010.pdf.

120. *White House: BP Will Pay $20B Into Gulf Spill Fund*, NPR (Jun. 16, 2010, 3:24 PM), http://www.npr.org/templates/story/story.php?storyId=127879786 [hereinafter *White House*].

121. UNITED STATES COAST GUARD, NATIONAL POLLUTION FUNDS, OIL SPILL CLAIMS CENTER, http://www.uscg.mil/npfc/claims/#types_of_claims (last visited Dec. 3, 2012) (a valid claim includes loss of profit and earning capacity).

122. *White House*, *supra* note 120.

bears the burden of the catastrophe.[123] The larger and more frequent the catastrophe, the more likely that private insurance companies will refuse to offer insurance to cover it.[124] Thus if the government does not step in, victims are left on the hook for any damage. Sometimes this takes the shape of a fund like the BP oil spill fund, except that the funds are provided by the government. In the case of the September 11th Victim Compensation Fund, the funds were provided by the government (and therefore U.S. taxpayers).[125] Other times, government aid for victims comes in the form of insurance. Before 1968, property owners were forced to assume the risk of flood damage.[126] Flooding was considered so high-risk that private insurance companies refused to cover flood damage.[127] In this case, instead of creating a fund that would dole out money for individual claims, the government enacted the National Flood Insurance Act, which subsidized insurance plans managed by private insurers.[128] Property owners were required to purchase insurance ex-ante, unlike in the September 11th Victim Compensation Fund, where no ex-ante action was necessary for recovery.[129]

It is possible that users who suffer economic loss due to an undersea cable breach could recover either via a fund like the BP fund or through a subsidized insurance program like the National Flood Insurance Act. Neither solution would be perfect. In the case of a fund, who would pay for the potentially enormous damages? Is the situation of a massive undersea cable breach more akin to an oil spill where the cable owner (and any of their insurers) would be held responsible for contributing to the fund, or would the government be responsible as it was for the September 11th Victim Compensation Fund? In the case of a terrorist or pirate attack on undersea cables, the responsible terrorists and pirates are obviously at fault, and so one would think the government should be responsible for any compensation payouts just as in the September 11th Fund. On the other hand, it could be argued that the cable companies were negligent in not taking adequate precautions to secure their cables

123. Robert J. Rhee, *Catastrophic Risk and Governance After Hurricane Katrina: A Postscript to Terrorism Risk in a Post-9/11 Economy*, 38 ARIZ. ST. L.J. 581, 597-98 (2006).

124. Judith Kildow & Jason Scorse, *End Federal Flood Insurance*, N.Y. TIMES (Nov. 28, 2012), http://www.nytimes.com/2012/11/29/opinion/end-federal-flood-insurance.html?_r=0.

125. SEPTEMBER 11TH VICTIM COMPENSATION FUND OF 2001, http://www.justice.gov/archive/victimcompensation/ (last visited Dec. 4, 2012).

126. Rhee, *supra* note 123, at 599.

127. *Id.* at 598.

128. *Id.* at 599.

129. *Id.* at 599-600.

against such outside attacks and in failing to provide sufficient alternate cables.[130] So perhaps the cable companies should be at least partially responsible for the funds.

The problem with requiring cable companies to pay a large part of a recovery fund is the likelihood of breaches – either accidental or from deliberate attack. Undersea cable infrastructure will remain vulnerable even with the increased security measures suggested above in Proposal A.[131] Cable breaches are much more likely to occur than oil spills or terrorist attacks.[132] Requiring cable companies to pay billions of dollars in damages to third parties for an event that is likely not preventable by them could bankrupt smaller cable owners. It could also deter companies like Google from becoming cable owners and opening themselves up to this kind of liability. Likewise, it would be hard for these companies to find willing insurers to cover this kind of likely liability.

It is hard to argue, given the initiation of the breakages by terrorists or natural disasters, that cable companies should be forced to pay damages similar to that of the BP oil spill, which was caused by the negligence of BP's own agents. As a result, it is most likely that the burden would fall on the government if a potential fund were to be created. This would put taxpayers on the hook for a huge bill. Such legislation to compensate victims for attacks that occur halfway around the world for damages merely economic in nature may not be perceived as fair and thus may not be politically viable.[133] Therefore, the ability of the government to create this kind of fund is unclear.

As for insurance, like with flooding, private insurance companies may not be willing to insure either users or cable owners, given how likely a simultaneous breach is to occur and how catastrophic the damages could be. Thus a government-subsidized model would make sense. In fact, similar models have been suggested for terrorist attacks in the past in which the government would handle the extreme range of potential liability so that private insurers could offer consumers terrorism insurance.[134] However, these models have been criticized for being

130. After all, these attacks are foreseeable. Cable owners should be prepared for both accidental and intentional breaches.

131. *See supra* Part III.A.

132. *See* discussion *supra* Part II.B.

133. In discussing a possible catastrophe pool created by tax dollars to compensate victims of terrorist attacks and Katrina-like catastrophes, Robert J. Rhee argues that taxpayers in average homes in Cleveland may resent having to fund the lifestyle of a taxpayer in Miami and may perceive this to be unfair. Rhee, *supra* note 123, at 611-12.

134. *Id.* at 601.

unsustainable.[135] With subsidized insurance, policyholders pay premiums that represent a mere percentage of the true actuarial risk.[136] Thus the program is designed to be a loss-making program and is sustainable only through continued government funding. [137] As a result, the popularity and political viability of this plan is also unclear. Would taxpayers support continually subsidizing the economic losses of others no matter how large? How much economic damage would taxpayers be willing to shoulder?

IV. PROPOSED MOVE TOWARD A HOLISTIC SOLUTION: INCREASE REDUNDANCY AND SHIFT LIABILITY

What the above proposed solutions show is that there is no "silver bullet" solution to undersea cable security and liability for cable breaches. Merely increasing international cooperation and maritime security, for example, will not be sufficient to prevent all attacks. Nor will this increase in security do anything to compensate victims who lose access to their data for a prolonged period of time. Likewise, a solution focused entirely on increasing liability does little to improve the physical security of the infrastructure itself. Therefore, any solution going forward must be holistic. It must consider both ex-ante security measures and ex-post liability. This article proposes a solution meant to address both of these issues in the context of cloud computing - to ensure that access to data remains safe and that victims can recover in the event of a data breach. In doing so, this article draws from scholarship on cybersecurity as well as public information on the government-subsidized insurance programs mentioned above. It also shifts the focus on undersea cable liability away from the cable owner to the cloud data storage providers and their insurers.

While the security of undersea cables is a specific problem having to do with a particular piece of telecommunications infrastructure, undersea cables are in fact just one part of a larger mesh that makes up the Internet. A potential breach of cables is thus an issue of cybersecurity. While many proposals to increase and improve cybersecurity, such as building firewalls or repelling hackers,[138] are inapplicable to undersea

135. *Id.* at 599.

136. *Id.*

137. *Id.* at 599.

138. *See generally* UNITED STATES COMPUTER EMERGENCY READINESS TEAM, RECOMMENDED PRACTICES, https://www.us-cert.gov/control_systems/practices/-Recommended_Practices.html (last visited Dec. 4, 2012).

cables due to their focus on software, other cybersecurity solutions that incorporate infrastructure can be applied. One solution is the idea of *redundancy*.[139] While it may be efficient to have a single point of access to one's data, this approach creates the possibility of losing access to all that data if that single point of access is destroyed.[140] It is therefore better to be redundant and inefficient: having information stored in multiple locations and having multiple points of access to that data.[141] Professor Derek Bambauer argues that inefficiency creates resiliency.[142] Bambauer suggests that multiple data storage facilities and modes of access can not only improve a user's chance of being able to access their data but can also deter intentional attacks.[143] The less chance an attack has to actually cause damage through data disruption, the less it will be an attractive plan to an attacker.[144] It is useful to think of a resilient Internet as a hydra.[145] Cut off multiple heads and the creature still survives because each head is redundant. Therefore the incentive to cut off just a few heads is reduced. Security is increased not through additional patrols or naval exercises but by simply making the target less attractive to potential attackers.[146]

To increase cybersecurity in general, Bambauer proposes establishing information storage legislation that would require an organization to maintain separate and redundant information in a way that ensures that if it loses its primary source of data, it is able to restore regular functionality within a day.[147] His proposal involves penalties and

---

139. *See generally* Bambauer, *supra* note 12.

140. Bambauer, *supra* note 12, at 637; *see also* SYMFORM, REDUNDANT DATA STORAGE, http://www.symform.com/join-the-revolution/how-symform-works/data-redundancy/ (last visited, Dec. 4, 2012) (pointing to Symform's redundant cloud storage as what sets it apart from its competitors and allows for greater guarantees of data safety).

141. Bambauer, *supra* note 12, at 637.

142. *Id.* at 638.

143. *Id.*

144. *Id.*

145. *Id.*

146. An argument can be made that in the case of piracy, increased redundancy will be ineffective. A more redundant system does not remove the attractiveness of a cable if the purpose is to sell its components on the black market or for scrap. *See* Burnett, *Cable Vision*, *supra* note 18, at 69. Also, Bambauer's proposal assumes terrorists will act rationally. Terrorists may still attack cable infrastructure as a symbolic gesture even if the impact on the flow of data is minimal.

147. Bambauer, *supra* note 12, at 645. Bambauer looks at record keeping rules like the Securities and Exchange requirement that accounting firms keep records related to auditing and financial statements reviews for seven years after such reviews are concluded. *Id*. These existing requirements suggest that private incentives for

sanctions for non-compliance as a way to enforce the legislation.[148] There are several issues that Bambauer himself raises about his proposal.[149] Bambauer acknowledges that establishing these requirements through public law is challenging.[150] Government mandates risk being extremely expensive and poorly tailored, and the speed of the legislative process increases the likelihood that mandates will become rapidly obsolete.[151] However, he argues that despite these problems with legislation, relying on the private sector to develop best practices may lead to insufficient precautions.[152] Bambauer does not resolve the specifics of his proposed legislation. He does not address the scope of information that different organizations would be required to store redundantly or the level and speed of functionality restoration that would avoid triggering penalties. Although he acknowledges that various industries would have to be treated differently,[153] he does not delve into those differences.

This article proposes creating a new kind of government-subsidized insurance and certification plan, based on the idea of redundancy advocated by Bambauer, as a way to protect undersea cables and their users. Briefly, this article proposes that the government offer subsidized insurance to cloud data providers who meet certain set redundancy requirements. Those data providers who met the requirements would be government certified, and consumers would be encouraged to utilize these certified services. Consumers would be allowed to recover from these certified companies, who would be backed by government insurance, for economic damages due to loss of data access. While this insurance is envisioned to be available to U.S. consumers, the model itself could be followed in other countries.

Firstly, the U.S. government should work with private cable operators[154] and data storage providers to create a set of guidelines for

---

information storage are frequently inadequate, at least in comparison to larger societal interest in that information. *Id.* at 641.

148. *Id.* at 647-48.

149. *Id.* at 667-69.

150. *Id.* at 642.

151. *Id.*

152. *Id.*

153. *Id.* at 643.

154. By having the government work with private companies, this plan hopes to avoid the problems highlighted by Bambauer of either obsolete legislation or insufficient precautions. *See* Bambauer, *supra* note 12 and accompanying text.

optimal redundancy.[155] This is not simply a matter of determining the minimum number of data center locations that a company like Google or Amazon must have. The coalition should look at models of the effects of potential undersea cable breaches to determine strategic placements of data servers around the world, and to ensure that if a group of cables are cut multiple data centers are still accessible. They should consider expanding the use of domestic data centers as well.[156] This coalition should also look at the larger Internet infrastructure as a whole. It should explore whether new technologies such as long-range WiFi[157] could reduce reliance on undersea cables by rerouting data in the event of a breach. Both locations and technology should be diversified.

Once these guidelines are established, compliant companies would be eligible to receive government-subsidized data disruption insurance. Unlike flood insurance, which puts the burden on consumers to purchase ex-ante insurance, the burden would be on the data storage companies themselves to pay for the insurance. Once they had purchased this insurance, these companies would be certified as "recommended and insured cloud storage providers."[158] Users who chose to use these recommended providers would be able to recover for economic loss in the event of a cable breach leading to loss of data access. Government funds would be available to insurance companies of certified data providers in the event of terrorist attacks, natural disasters, and other catastrophic data disruptions.[159] However, more standard data disruptions, such as those caused by computer viruses or human error (by

155. A question that would have to be resolved is which executive agency would spearhead this effort. The Federal Communications Commission would be an obvious choice, given its regulation of other communications industries like terrestrial cable companies and its experience working with private companies like AT & T. However, it is possible that the Department of Homeland Security or the Department of Defense could assume this task.

156. *See supra* Part III.B.

157. *See generally* Chris Burns, *WiFi 802.22 Technology Promises Wireless Data Over 60 Miles: Say Goodbye to Data Plans,* SLASHGEAR (July 29, 2011), http://www.slashgear.com/wifi-802-22-technology-promises-wireless-data-over-60-miles-say-goodbye-to-data-plans-29168407/.

158. The certification would be subject to ongoing audits. The standard for adequate redundancy is likely to change over time as new technology is developed, and this system should be prepared for that.

159. This proposal does not intend to change the fact that cable owners must handle all repairs, and does not require their insurers to shoulder repair costs in cases of terrorist or pirate attacks. It may be advisable to establish a rule forcing cable owners who do not adequately protect their cables to pay fines that would be funneled into the proposed insurance fund. What adequate precautions entail would have to be determined.

a data storage provider's employees), would be covered by the data providers and their insurance companies.[160] In other words, government funds would be available in cases of large-scale disruptions outside of a data storage company's control.[161]

Several issues are raised by this particular proposal. The first issue is whether the private sector would be willing to participate in such a plan. For private insurance companies, they would be able to offer comprehensive data disruption insurance without worrying about being liable for billions of dollars in economic losses in the event of a terrorist attack or undersea landslide. Therefore, it is likely that private insurance companies would support this proposed arrangement. However, data storage providers would be required to spend a great deal of money on increasing their redundancy and would also have to pay insurance fees. Furthermore, they would now be liable for the acts of third parties on infrastructure like undersea cables that do not even belong to them. For them, it would not seem like an attractive plan.

But two factors could be emphasized that would make data storage provider participation more likely. First the government would pay for the damage caused by third parties. Second, the hope is that the certification would encourage users to utilize certified data storage providers as "safer" options. Consumers who value the security of their data and access to that data would likely migrate to these certified services.[162] In this regard the challenge would be publicizing and raising awareness about the certification, such that consumer demand for certified data storage makes the certification process sufficiently attractive to data storage providers.

The second issue raised by this article's proposed holistic solution is sustainability. As discussed above, one of the main criticisms of the government-subsidized flood insurance program is that floods continue to occur and thus the government has to pay out a never-ending supply of

160. Whether or not companies should be allowed to continue to limit this liability will have to be resolved.

161. This article does not address whether government insurance would cover disruptions due to electricity loss. Attacks on the power grid are also a large concern in cybersecurity and cloud computing. These issues, however, are beyond the scope of this article.

162. Many companies have been skittish about moving their data to the cloud, but a certification could help alleviate their fears. Arik Hesseldahl, *Businesses Confront the Cloud Security Threat*, BLOOMBERG BUSINESSWEEK (June 17, 2010), http://www.businessweek.com/stories/2010-06-17/businesses-confront-the-cloud-security-threatbusinessweek-business-news-stock-market-and-financial-advice.

funds.[163] In the case of data disruption, the insurance would be given out only to those companies who met the agreed upon redundancy requirements. As a result, only the most extreme terrorist attacks or natural disasters would lead to losses. A breach of a few cables would be covered due to redundancy and users would not experience a loss of access to their data. Therefore, the amount of times the government would actually have to pay out money to cover data disruptions would likely be limited. Granted, the payouts in those infrequent cases could be costly, potentially reaching into the billions of dollars depending on the industries affected. However, as more technology is developed to create new modes of access, such as through long-range WiFi or increased satellite capacity, the risks of such catastrophic failure should decrease even further.

Perhaps the largest problem with this proposal is the effect on smaller cloud data storage providers who lack the funds to reach the required redundancy. This problem would be especially acute if the government decided to go one step further and require that any cloud storage provider, no matter how small, would be liable for the economic damages of its customers resulting from loss of access to data. As a result, data storage companies would risk having to pay for all potential damages unless they complied with the redundancy requirements and purchased the subsidized insurance plan. While this further step by the government would increase consumer security, the measure could crush smaller data storage providers who are unable to build out sufficient infrastructure to comply with the redundancy requirement. As a result, cloud data storage would begin to be consolidated into the hands of fewer and more powerful players.[164]

This consolidation may not be a bad thing. By having such stringent requirements, the cloud computing system would begin to closely resemble a U.S. utility system. Smaller companies could "interconnect" with larger storage providers like Google or Amazon to ensure coverage by the government-subsidized insurance. The larger companies like Google would be more heavily regulated but could also benefit from greater market share and the interconnection fees from smaller companies. This article does not endorse such a dramatic change, but the government should at least consider whether protecting consumers and

163. *See* discussion *supra* Part III.C.

164. Matthew Mitchell, *The Pathology of Privilege: The Economic Consequences of Government Favoritism*, MERCATUS RESEARCH (July 8, 2012), http://mercatus.org/publication/pathology-privilege-economic-consequences-government-favoritism (discussing the issues of monopoly, antitrust, and abuse of power that are raised by such consolidation).

the economy warrant more extreme measures. Even under the less extreme plan proposed in this article, the government will have to consider whether the protection of consumer access to data should be placed above the interests of smaller cloud storage providers.

V. CONCLUSION

Just as it is impossible to fully prevent cyber-attacks,[165] it is impossible to prevent attacks on the vast web of undersea cables. Retaliation and other reactive measures for these attacks would not do anything to remedy the situation.[166] As a result, successful cybersecurity, including undersea cable security, must focus on ex-ante redundancy. This article has proposed a plan to encourage cloud data providers to increase redundancy and has also provided a mechanism by which consumers could be protected from economic loss stemming from disruptions to their data access.

If this plan were to be implemented, there would likely be a shift of consumers toward certified data storage providers. As a result, more consumers would be relying on highly redundant systems to access their data. Terrorists looking to attack Internet infrastructure would find that attacking cables would have far less of an effect as the data flowing through the disrupted cables would simply be rerouted through alternate cables and technologies. The target would be less attractive and thus more secure. This article argues that the best way to increase the security of undersea cables is to rely on them less.

It is important to remember, however, that the economies of the world are increasingly intertwined. As a result, while this proposal is targeted at the U.S. government and legal system, it is imperative that other nations also consider not only increasing security of cables in their waters, but also providing recourse for their own citizens in the event of data disruptions. If companies in India or China suffer data disruptions and lack any recourse or compensation, those effects will be felt globally. If countries protect their consumers from cyber-attacks, whether they are attacks on undersea cables or computer viruses, data around the world will be safer and the global economy will grow more resilient.

---

165. Bambauer, *supra* note 12, at 673.

166. *Id*.