SEAFARING DATA HAVENS: GOOGLE'S PATENTED PIRATE SHIP

Jeffrey D. Kramer[*]

TABLE OF CONTENTS

I. Introduction 360
II. Background 360
A. Google's Floating Data Centers 361
B. Law of the Sea 361
C. Regulation of Data 362
1. Internet Traffic v. Traditional Forms of Trading 362
2. Evolution of International Data Regulation 363
III. Analysis 364
A. Data v. Traditional Objects 365
B. Examples of Contemporary "Data Havens" 366
1. Sealand & HavenCo, A Failed Extra-Jurisdictional Data Haven 366
2. OIS, an example of a Nationally-Based Data Haven 368
3. Other Data Safe Havens 369
C. Google's Floating Server: Effects of Mobility 369
1. Nationally-Based Data Havens 370
2. Non-National Data Havens 370
3. Mobile Data Havens Could Avoid Jurisdictional Regulation 371
D. Extra-Jurisdictional Regulation and International Law 371
1. Presumption Against Extraterritoriality 372
2. Offsetting Principles 373
E. Practical considerations 374
1. Political and Macroeconomic Pressures 375
2. Financial Connectedness 375
3. Applicability of the Law of the Sea 376
IV. Recommendations 378
A. Assert Control Through Existing Means 378
1. Political and Economic Pressures 378
2. Nations of Citizenship of Offenders 379
3. Financial Ties 379
4. Utilize the "In Touch with the Shore" Exception 380
B. Looking forward: Regulating Data in Space 380
1. Freedoms 381
2. Restraints 381
V. Conclusion 382

[*] J.D. Candidate 2011, Univ. of Ill.; Int'l Rel. B.S. 2002, Grinnell College.

"Where there is a sea, there are pirates."[1]

I. INTRODUCTION

In August 2008, Google was issued a U.S. patent for a floating data center designed to self-sustainably operate in the offshore oceans.[2] Such seafaring data centers, by being literally off-shore, will differ from traditional "offshore" data centers in that they can exist outside of *any* nation's jurisdictions. This freedom may remove them from the practical bounds of any extant set of laws regulating data privacy and security. The ability of seafaring data havens to escape to international waters could therefore allow them to serve as pirate havens for those seeking to avoid intellectual property regulation.

This Note considers the extent to which contemporary laws, conventions, and *realpolitik* forces are capable of controlling such oceangoing data havens. Part II lays the background by addressing the nature of data and of information transactions, and how regulators have modified the traditional methods of trade regulation to account for this new medium. Part III of this Note then analyzes the current situation and some potential tools for preventing such data piracy. This analysis describes some contemporary data havens and how their fixed geographic characteristics have limited their owners' and clients' autonomy, causing them to founder; limitation which Google's oceangoing data haven might avoid by navigating around current national and international jurisdictional limitations. Part III also analyzes the relevant legal concepts and reviews some practical political and economic instruments which regulators might use to counter this possibility. In Part IV, this Note then recommends regulatory solutions drawn from both the realms of law and economics in light of the practical obstacles and opportunities facing data-minded entrepreneurs, and suggests for consideration a future data regulation frontier.

II. BACKGROUND

In August of 2008, a patent was issued to Google for a floating data center.[3] The first and second sections in this Part describe the concept embodied by the patent and what new opportunities it creates in light of the modern Law of the Sea.[4] The third section recapitulates the evolution of intellectual property regulation and its applicability to these uniquely mobile

1. Greek proverb.

2. Water-Based Data Center, U.S. Patent No. 20,080,209,234 (filed Feb. 26, 2007).

3. *Id.*; *see generally* Ashlee Vance, *Google's Search Goes Out to Sea*, N. Y. TIMES BITS BLOG (Sept. 7, 2008, 9:59 PM), http://bits.blogs.nytimes.com/2008/09/07/googles-search-goes-out-to-sea/ (providing a description of Google's patent filing).

4. *See* United Nations Convention of the Law of the Sea, Nov. 16 1994, 1833 U.N.T.S. 31363 [hereinafter UNCLOS] (creating and codifying the modern Law of the Sea).

data havens.

A. Google's Floating Data Centers

Google's patent describes an oceangoing ship or barge which would be anchored off the coast,[5] at a distance that Google speculated might be seven miles.[6] What made the idea unique and thus patentable is that the boats would draw energy directly from the movement of the ocean waves while also drawing cooler ocean water up from below the thermocline.[7] Doing so would provide the power and cooling necessary to operate a computer data center, thereby, eliminating the need to physically connect to a large power source with long and sensitive wiring.[8] This would free such data centers from the need to be tethered to shore and would allow them to relocate or roam the seas at their owner's whim.

B. Law of the Sea

The modern law of the sea is codified by the Third United Nations Convention on the Law of the Sea (UNCLOS), which came into effect in 1994.[9] Among its various provisions, it significantly redefined the rights that nations have to the waters around them.[10] UNCLOS established "territorial sea" as extending twelve nautical miles[11] beyond a nation's shores and internal waters.[12] Within their territorial sea, governments of nations can create and enforce laws on all matters.[13] Extending beyond the territorial sea for another twenty-four nautical miles is the "contiguous zone," in which UNCLOS permits nations to enforce their tax, customs, sanitary, and immigration laws.[14] Land and seabed beyond this, up to a distance of 200 nautical miles from shore, constitute a nation's "Exclusive Economic Zone," (EEZ) within which the nation retains rights to economic resources such as minerals, oil reserves, and fish.[15] Past the EEZ lie "international waters," the high seas of old, which are open to all nations and to which no nation may claim sovereign

5. *Id.*

6. *See* Murad Ahmed, *Google search finds seafaring solution*, THE TIMES ONLINE (Sept. 15, 2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4753389.ece (stating that Google is considering deploying the barges up to seven miles offshore).

7. *See generally* '234 Patent (indicating that Google's patent claims include that the boats would draw energy directly from the movement of waves and draw ocean water up from below the thermocline).

8. *Id.*

9. UNCLOS, *supra* note 4.

10. *See, e.g.*, *id.* (establishing, inter alia, exclusive economic zones for coastal waters).

11. One nautical mile equals 1.151 U.S. customary miles, or 1.852 kilometers.

12. UNCLOS, *supra* note 4, at 400; *see supra* Part II (discussing this history and implications of this boundary).

13. UNCLOS, *supra* note 4, at 400–07. If infringements of a nation's territorial sea rights occur, the nation may exercise control over boats outside the zone if necessary to punish or prevent infringement of those rights. *Id.* at art. 25.

14. *Id.* at 409. *See generally* 14 U.S.C. § 89(a) (2006) (codifying law enforcement upon the high seas and waters in the United States).

15. UNCLOS, *supra* note 4, at pt. 5.

dominion.[16]

C. Regulation of Data

Informational property is data, which—in contrast with tangible goods—is by its nature non-rivalrous.[17] More than one person can therefore simultaneously possess and utilize this information.[18] Though data is not consumed by its usage and repeated utilization does not exhaust the resource itself,[19] because data is duplicable and transmittable, it is capable of being acquired and used by many parties who have not paid for the right to do so. Data-specific regulation is thereby needed to control the flow and usage of informational property; this subsection describes the reasons for and results of such regulation.

1. Internet Traffic v. Traditional Forms of Trading

Unlike the discrete and controllable pathways on which traditional goods flow, the internet does not have a corporeal being[20] whose traffic is amenable to regulation at a tollgate. Data transfers, unlike shipments of physical objects, travel along the myriad connections making up the internet, ignoring geography and thus ignoring national boundaries.[21] Unlike the marketplaces and storefronts through which physical goods are acquired, the location of the internet is impossible to pin down. As the Canadian academic and internet regulatory authority put it, "not only is there perhaps 'no there,' [regarding the internet, but] the 'there' is everywhere where there is an Internet access."[22] This ephemeral nature means that the ultimate recipient of data from the internet has knowledge of neither whence the data originated nor where the data was stored during its travels.[23]

Given the decentralized and fluid nature of the internet, once connectivity of any sort is allowed, there are no options available to a jurisdiction or even a nation to limit transmission of data.[24] The sole exception may be the

16. Convention on the High Seas, Apr. 29, 1958, 450 U.N.T.S. 11, T.I.A.S. No. 5200 (entered into force Sept. 30, 1962); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 511 (1987). A nation retains rights to resources on or under the continental shelf but not to waters and surface above it. UNCLOS, *supra* note 4, at arts. 77–81.

17. Eli M. Salzberger, The Law and Economics Analysis of Intellectual Property: Paradigmatic Shift From Incentives to Traditional Property, § 2.1.1 (Mar. 2, 2010) (unpublished article) (on file with author).

18. *Id*.

19. *Id*.

20. Dan L. Burk, *Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks*, 68 TUL. L. REV. 1, 8-10 (1993).

21. *Id*.

22. Samuel O. Manteaw, *Entering the Digital Marketplace: E-Commerce and Jurisdiction in Ghana*, 16 TRANSNAT'L LAW. 345, 373 (2003) (quoting Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1346 (2001)).

23. Trevor A. Dennis, *The Principality of Sealand: Nation Building by Individuals*, 10 TULSA J. COMP. & INT'L L. 261, 294–95 (2002) (updating Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA J.L & TECH. 3 pt. 3 (1997)).

24. Warren Chik, *U.S. Jurisdictional Rules of Adjudication over Business conducted via the Internet—*

draconian step of halting internet usage entirely, and limiting users to only the resources on a single self-contained network.[25] Therefore, in a liberal society, any internet user can freely transfer files to any other user of the internet, regardless of location.

The data transmitted on the internet not only represents private intellectual property, but can also contain representations that are themselves property.[26] The electronic nature of this information makes it easy to copy and transmit.[27] As such, creators and owners of copyrighted, patented, or otherwise sensitive data have an interest in protecting their investments. Data owners thus fear the consequences of the free flow of information.

2. Evolution of International Data Regulation

a. The Berne Convention and Intellectual Property

That intellectual piracy will result from the unregulated flow of information has been recognized for over a century.[28] As long ago as 1886, European nations formed the International Union for the Protection of Literary and Artistic Works, codified in the "Berne Convention."[29] The Berne Convention thereafter became the foundation of modern international intellectual property law, which is currently administered by the World Intellectual Property Organization (WIPO), founded in 1967 for that very purpose.[30] WIPO has since been ratified by over 180 nations,[31] a testament to the global awareness of intellectual property's significance.

b. TRIPS, WIPO Copyright Treaty, and Information Technology

In more recent decades, the rise of information technology created a need for a new agreement capable of handling the ease and anonymity of electronic

---

Guidelines and a Checklist for the E-commerce Merchant, 10 TUL. J. INT'L & COMP. L. 243, 300 (2002) (describing the "necessity of an international uniform approach to the jurisdictional question").

25. *See, e.g.*, *Developments in the Law - The Law of Cyberspace*, 112 HARV. L.R. 1577, 1683–84 (1999) (discussing China's and Germany's differing attempts to suppress 'objectionable' internet content and describing China's unusually extreme exercise of control over its data network that includes attempts to block every electronic communication portal between its citizenry and the rest of the globe).

26. F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CAL. L. REV. 1, 7–13 (2004) (explaining virtual worlds and discussing the nature of their "property," and describing the two philosophies of dealing with emergent internet laws).

27. *See* Eli M. Salzberger, The Law and Economics Analysis of Intellectual Property: Paradigmatic Shift from Incentives to Traditional Property, 1–2 (Mar. 2, 2010) (unpublished article, on file with author) (recognizing the "huge increase in informational goods and intellectual creations" that came with the Internet and the prevalence of copying using computers).

28. *See* Berne Convention for the Protection of Literary and Artistic Works, July 14, 1967, 828 U.N.T.S. 221, 223 [hereinafter Berne Convention] (recognizing a "desire to protect . . . the rights of authors in their literary and artistic works" in a treaty originating in 1886).

29. *Id.*

30. *What is WIPO?*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/about-wipo/en/what_is_wipo.html (last visited Sept 28, 2010).

31. *See Member States*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/members/en/ (last visited Sept. 28, 2010) (listing "184 current Member States").

data transfers.[32] The member states of WIPO therefore drafted the World Intellectual Property Organization Copyright Treaty (WIPO Copyright Treaty) in 1996.[33] The founding nations of the Global Agreement on Tariffs and Trade (GATT) also acted to stem digital piracy during that period by drafting the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS protocol) and requiring its adoption before nations could join the WTO.[34] The TRIPS protocol expanded upon the Berne Convention's intellectual property protections to explicitly include databases, along with other budding tools of information technology.[35]

c. Jurisprudential Regulation of the Internet

Courts, including those of the United States, initially struggled to translate the traditional jurisdictional approach to the internet,[36] and have modified the traditional approaches regarding non-resident defendant personal jurisdiction to apply to the internet and its content. In the United States for instance, courts first consider what the venue's "long-arm statutes" allow, and then whether the exercise of jurisdiction would violate the defendant's constitutional due process rights.[37] The courts then consider where the effects of the activity will be felt[38] and where the activity falls on a sliding scale between aggressively reaching out to do commercial business and relatively passive websites.[39] Despite this workable standard for defining jurisdiction over internet-related activities, ocean-going data centers can elude the reach of national jurisdictions by placing themselves beyond nations' physical boundaries.[40] This troubling possibility is explored in the following Part of this Note.

III. ANALYSIS

The prospect that offshore data havens will undermine regulatory regimes is of such concern that, even a decade ago, the European Council outlawed "transborder flows of personally identifiable data" between the European

32. WIPO Copyright Treaty preamble, Dec. 20, 1996, 2186 U.N.T.S. 38542, *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

33. *Id.*

34. Agreement On Trade-Related Aspects of Intellectual Property Rights (TRIPS) preamble, Apr. 15, 1994, 33 I.L.M. 1197, 1869 U.N.T.S. 299.

35. Article 10 of TRIPS reads, "1. Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971). 2. Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such." *Id.* at 1201.

36. *See* Cameron Hutchison & Moin A. Yahya, *Infringement & the International Reach of U.S. Patent Law*, 17 FED. CIR. B.J. 241, 241–42 (2008) (discussing territorial jurisprudence of patents, TRIPS, and the Patent Act § 271(a)).

37. *See* World Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 289–90 (1980) (noting that the proper approach to testing personal jurisdiction involves both statutory and constitutional standards).

38. Pavlovich v. Superior Court, 58 P.3d 2, 7–8 (Cal. 2002).

39. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1125–27 (W.D. Pa. 1997).

40. *See infra* Part III (discussing problems posed by offshore data centers).

Union and jurisdictions having "inadequate" data protection standards.[41] The potential for wily entrepreneurs to misuse such transborder informational flows has again been increased by the capacities of Google's ocean-going data center.[42] The unique capacity of this type of vessel to avoid traditional intellectual property regulation raises challenges and opportunities fundamentally different from those of attempted data havens to date.

The following analysis describes first how data's ethereal and non-material nature makes it so fundamentally different from traditional objects of trade. Data's resulting potential for unauthorized copying and usage has required the creation of a separate governing regime, as discussed above.[43] The analysis then describes several recently attempted circumvention of this regulation by intended data havens based in countries amenable to unregulated data storage, and demonstrates that these have so far been only moderately successful, due to *realpolitik* limitations inherent in nationhood.[44] Thirdly, this analysis discusses the particular regulatory difficulties created by an extra-jurisdictional data haven which could result from Google's patent, since current data protection solutions are inapplicable to the kind of extra-jurisdictional data havens that floating data centers will allow. International law also offers a pair of alternate control mechanisms, presented in the fourth section of this analysis, but even their applicability to pirate data havens is arguable.

The dilemma of how to regulate such an extra-jurisdictional data haven is the animating force of this Note. After considering the uncertainty surrounding regulation of mobile seafaring data havens, and the factors which make it difficult for land-based data centers to operate with impunity, the fifth section of the analysis suggests several economic and political means of curtailing rogue data centers' activities. These dynamics frame this Note's subsequent recommendations for other tools that regulators might utilize to inhibit the unrestrained flow and storage of information on mobile data havens.

A. Data v. Traditional Objects

The body of law regulating the use of data is fundamentally different than traditional property regulation due to the privacy considerations inherent in the former that are absent for chattel, real property, contract rights, and other customary forms of property.[45] Though electronic data is physically carried

41. *E.g.*, information entered by an online purchaser, customer databases, and government tax rolls. Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 751–52 (1999) (reviewing PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998)).

42. *See supra* Part II.A. (describing the vessel and its operation).

43. *See supra* Part II.C.1–2 (discussing this difference and the resultant data regulation systems).

44. *See supra* Part II.C. (describing several such attempts and their results).

45. *E.g.*, Viktor Mayer-Schönberger, *The Share of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 608 (2003) (describing "cyber" law as a field distinct from the standard law regarding physical transactions, and analyzing various legal paradigms and their application to cyberlaw); *see supra* Part II.C. (addressing differences between traditional trade and the internet).

and stored inside of wires, circuits, transistors, and recording media, the value of data lies neither in its electrons and bytes nor its means of transmission or storage, but instead in the ideas and information that the data represents.[46]

As industry and society increasingly amass and rely on privately owned data, lawyers need to become familiar with data privacy laws and their practical application, as ever more clients engage in international transportation of data.[47] The importance of protecting data was recognized as long as 120 years ago, when the Berne Convention was first negotiated.[48] Data, like other forms of assets, has since come to be governed by numerous modern statutes, treaties, opinions and customs, with regimes differing across various jurisdictions.[49] Attempts to avoid these regulations have naturally been made, and are discussed below.

B. Examples of Contemporary "Data Havens"

As regulatory advances limited the activities that are permissible, people who benefit from those activities are driven to greater and greater lengths to circumvent the rules. The prohibition movement in the United States, for example, failed to do away with alcoholic consumption, instead resulting in communities of underground speakeasies.[50] The current attempts to regulate the internet will likewise drive up the value of any remaining confidentially operating data havens.[51]

The following sections describe several of the well-known attempted data havens to date and the reasons for their inability to provide the un-regulated environment their users desired. These examples illustrate the limitations inherent in stationary computing centers; limitations which mobile data havens may be able to avoid.

1. Sealand & HavenCo, A Failed Extra-Jurisdictional Data Haven

The notion of safe-havens for data arose even before the nature of the World Wide Web had even solidified.[52] Perhaps the most popularized

46. *Supra* Part II.C.

47. *See generally* Samuelson, *supra* note 41, at 753 (describing the rising trend of trans-border data flow, and need for lawyers to keep up with the scholarship on it).

48. As evidenced by the Berne Convention, which came into force in 1886. Berne Convention, *supra* note 29.

49. *See supra* Part II.C.

50. *See, e.g.*, Bernard Isaac Weinstein Baskin, *Historical Heist: an Economic Argument Against Embargoing Chinese Cultural Property*, 8 WASH. U. GLOB.STUD. L. REV. 107, 132–33 (2009) (describing how Prohibition in the United States had little effect on alcohol production, as an analogy for how a ban on trading in Chinese cultural artifacts would drive up their price and therefore increase incentives for looters to acquire them).

51. *Cf. id.* (giving two parallel cases of such regulatory efforts having no – or the opposite of the intended – limiting effect).

52. *Compare Bahamas Wants Business Data*, Transnat'l Data & Comm. Rep., Mar. 1986, at 8 (describing offshore "data free zone"), *with* Scott Ruthfield, *The Internet's History and Development: From Wartime Tool to the Fish-Cam* (1995), http://www.acm.org/crossroads/xrds2-1/inet-history.html (recapping the timeline of modern internet's evolution).

example of its attempted execution was the short-lived data haven knows as HavenCo, and the micronation of Sealand on which it was hosted, the history and failure of which the following sub-subsections briefly review.

a. The Principality of Sealand

In 1965, Paddy Roy Bates occupied and moved his family into an abandoned British naval fortification left standing seven nautical miles off of England's southeastern coast.[53] Bates was soon brought before a British court for firing warning shots against the British naval vessel that had attempted to evict him.[54] At the time, the United Kingdom still recognized the 3-nautical-mile boundary, so the British courts found that they lacked jurisdiction over the installation.[55] The charges were dropped and Bates proceeded to establish a small *de facto* country, complete with a national anthem and flag, coinage and stamps, and passports.[56]

In 1978, a brief skirmish ended with Bates detaining several "prisoners of war" who had entered the installation without permission and who had held Bates' son hostage.[57] Germany subsequently sent a diplomat to negotiate the captives' release, having had their request for help rebuffed by the British, and thereby, provided arguable *de facto* recognition of Sealand's sovereignty.[58] This sovereignty made Sealand valuable to others who, like Bates, were attempting to avoid national regulation; their resulting data haven is the subject of the next two sub-subsections.

b. HavenCo

In the late 1990s, Ryan Lackey, an American information technology entrepreneur, created a company to take advantage of Sealand's unique physical security and lenient oversight.[59] To this end Lackey, in consultation with Bates, created a British company named HavenCo.[60] Lackey billed HavenCo as the world's most sophisticated data haven[61] and as a "free-market" location capable of thoroughly protecting its clients' data.[62] With an eye towards fast and ultra-secure data storage, high-tech servers were installed

53. Dennis, *supra* note 23, at 263–64 (2002) (citing in part Sealandgov.org, *The Principality of Sealand*, http://www.sealandgov.org/history.html (last visited Sept. 28, 2010)).

54. Frank B. Arenas, *Cyberspace Jurisdiction and the Implications of Sealand*, 99 IOWA L. REV. 1165, 1168 (2003).

55. Jeremy N. Geltzer, *The New Pirates of the Caribbean: How Data Havens can Provide Safe Harbors on the Internet Beyond Governmental Reach*, 10 SW. J. L. & TRADE AM. 433, 434 (2004).

56. Arenas, *supra* note 54, at 1168–69.

57. *Id.* at 1169.

58. *Id.*

59. Matthew Conroy, *Sealand – The Next New Haven?*, 27 SUFFOLK TRANSNAT'L L. REV. 127, 137–39 (2003); Declan McCullagh, *A Data Sanctuary Is Born*, WIRED NEWS (June 4, 2000), http://www.wired.com/news/business/0,1367,36749,00.html.

60. Conroy, *supra* note 59, at 137–38.

61. *Id.*

62. *Id.* at 138 (quoting *Data Center Services*, HAVENCO (Sept. 28, 2010, 6:59 PM), http://web.archive.org/web/20080822054338/http://www.havenco.com/index.html (accessed by searching for http://www.havenco.com/index.html in the Internet Archive Index)).

in the fortification that constituted Sealand and usage regulations were drawn up in an only modestly limiting way.[63] Clients were solicited and engaged with promises of confidential and untouchable data storage.[64] In short, Lackey established HavenCo specifically and openly in order to attempt to utilize Sealand's "sovereignty" to create an essentially non-national and extra-jurisdiction data haven, free from all agencies' regulatory clutches.[65]

c. Failure of HavenCo

As HavenCo was setting up shop on Sealand,[66] the United Kingdom passed the Regulation of Investigatory Powers Act (RIPA).[67] This act, passed in 2000, granted the U.K. government numerous powers enabling the interception, monitoring, and controlling of electronic communications within and passing through the United Kingdom.[68] Through these powers, RIPA effectively authorized the British government to monitor all internet traffic flowing into or through the UK.[69] Since all of Sealand's data connections ran through mainland England, the RIPA essentially permitted the United Kingdom, should it desire, to force Sealand into compliance with domestic and international intellectual property protection agreements.[70]

Despite Sealand's claims of sovereignty, this prospect undermined HavenCo's entire *raison d'être*. Predictably, HavenCo thereafter did not fare well. Its listed clients were few and decreasing by 2003, and in 2008, HavenCo's website quietly ceased to function.[71] HavenCo's apparent demise[72] illustrates the problem inherent in operating a data haven that must rely on a single nearby nation for its internet connectivity.

2. OIS, an example of a Nationally-Based Data Haven

Another approach is to situate the data haven in a country which itself has weaker intellectual property protections. An example of this is Offshore Information Services (OIS), an Anguillan internet service provider operated by

63. Amounting to little more than a requirement not to promote terrorism. *Acceptable Use Policy*, HAVENCO (Sept. 28, 2010, 6:46 PM), http://web.archive.org/web/20061031084159/ http://www.havenco.com/legal/aup.html (accessed by searching for http://www.havenco.com/legal/aup.html in the Internet Archive Index).

64. *Id.*

65. S*upra* notes 54–59.

66. Dennis, *supra* note 23, at 270 (stating that HavenCo started setting up in Sealand in 1999).

67. Regulation of Investigatory Powers Act (RIPA), 2000, c. 23, §§ 6–11 (Eng.), *available at* http://www.legislation.gov.uk/ukpga/2000/23/contents.

68. *Id.*

69. *Id.* §5.

70. *See* Conroy, *supra* note 59, at 140 (stating that RIPA allows the U.K. government to "intercept, monitor and control" electronic communications passing through the country).

71. *HavenCo "Data Center" Offline?*, SECURITY AND THE NET, (Nov. 18, 2008), http://securityandthe.net/2008/11/18/havenco-data-center-offline (reporting that the www.havenco.com sites remain dark, and that inaccurate current status are shown on HavenCo's pages).

72. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD, 65–66, 85 (2006).

Vince Cate, an American computer scientist.[73] OIS allows users to not only connect to the internet but also to rent space on OIS's own internal servers for hosting data and web sites.[74]

In addition to being an income tax haven for foreigners, Anguilla is not a signatory to the Berne Convention and so has no direct international obligation to prevent data piracy,[75] making it an ideal place for a data haven. Mr. Cate boasts that "[t]hanks to Anguilla's strict secrecy laws, we can offer 100 percent privacy-protected access."[76] OIS thus positions itself as an internet data haven by using Anguilla's strict privacy laws and lackadaisical intellectual property laws to put its customers' data beyond foreign governments' reach.[77]

3. Other Data Safe Havens

Others have since followed OIS' example. Another Anguillan company, IsleByte, similarly attempted to attract data storage customers by advertising its host nation's favorable tax laws and lax web regulation,[78] but closed when Anguilla was unable to provide the stronger assurances demanded by its operators.[79] Analogous attempts have been made in various countries without extradition treaties with the United States, including Antigua, Belize, Costa Rica, Curacao, Dominican Republic, Grenada, and Lichtenstein.[80] By utilizing nations with convenient laws, such data havens can avoid the regulation that defeated HavenCo but still cannot entirely achieve freedom to operate with permanent impunity, as the next section of this Note explains.

C. Google's Floating Server: Effects of Mobility

Google's patent for a floating and mobile data center foreshadows a pirate data haven that is fundamentally different from those attempted to date because it permits its operator to avoid most of the regulation and pressures that can be brought to bear on traditional immobile data centers. The following two sub-subsections illustrate how such a seafaring data center might avoid the reach of nation's jurisdictions.

---

73. Josh McHugh, *Going offshore on the Internet*, FORBES.COM (Sept. 8, 1997), http://www.forbes.com/forbes/1997/0908/6005179a.html; OFFSHORE INFORMATION SERVICES LTD., http://online.offshore.com.ai (last visited Sept. 28, 2010).

74. McHugh, *supra* note 73.

75. *Contracting Parties*, WORLD INTELLECTUAL PROPERTY ORGANIZATION-ADMINISTERED TREATIES, http://www.wipo.int/treaties/en/ShowResults.jsp?treaty_id=15 (last visited Sept. 28, 2010).

76. Steve G. Steinberg, *Offshore Data Haven*, WIRED, May 1996, at 40.

77. *Id.*; Press Release, Offshore Information Services Ltd., New Internet Privacy Provider (Feb. 8, 1996), *available at* http://offshore.ai/press.960208.html (last visited Sept. 28, 2010).

78. Geltzer, *supra* note 55 at 448–49 (describing the IsleByte company). IsleByte is also no longer functioning; their webpage (http://islebyte.com) no longer exists, and IslyByte founder Sean Hastings' resume lists his involvement as ending in 1999. Sean Hastings, *Resume*, http://www.seanhastings.com/resume.txt (last visited Sept. 28, 2010).

79. John Markoff, *Rebel Outpost on the Fringes of Cyberspace*, N.Y. TIMES, JUNE 4, 2000, at 14, *available at* http://partners.nytimes.com/library/tech/00/06/biztech/articles/04have.html (last visited September 28, 2010).

80. John Edmund Hogan, *World Wide Wager: The Feasibility of Internet Gambling Regulation*, 8 SETON HALL CONST. L.J. 815, 847 (1998) (cited by Conroy, *supra* note 59 at 127–28)).

1. Nationally-Based Data Havens

Traditional data havens are not as untouchable as their owners may claim, as their users may desire, or as they were originally feared to be by intellectual property owners.[81] IsleByte and OIS, for example, were not able to remove themselves entirely from regulatory reach, despite being based in countries which are non-signatories to the Berne Convention, and which have the kind of loose data regulation and lack of extradition treaties that appeal to those who may wish to avoid regulation.[82]

Merely by being land-based, terrestrial data havens encounter practical limitations. Not only are they subject to the laws of their physical host, but host countries can be subjected to *de facto* influence. This can be blatant, by having their national data infrastructures physically stifled, as the U.S. did to Iran in 1996,[83] or covertly, as their government can be politically pressured or even replaced, as the U.S. did in Grenada in 1983.[84] More subtle—yet equally effective—economic and political pressures can also be applied by willful world powers to encourage smaller nations to do their bidding.[85]

Concerned nations also have more palatable and straightforward regulatory powers that they can use to reach foreign wrongdoing, although these are limited. Initially, obtaining jurisdiction over foreign actions or assets is difficult because there are many different agencies involved on both sides of the border.[86] Additionally, a court in a given country only has power over an individual once that individual's assets become reachable within that country; for most users of a data haven in a remote and tiny state, this is unlikely ever to occur.[87] To avoid these gaps in jurisdiction, international conventions and bodies such as the WIPO, UNCITRAL, and the WTO are created to place *ex ante* transactional limitations on nations' behaviors regarding intellectual property.

2. Non-National Data Havens

An ocean-going data center would avoid many of the limitations to which nationally-located havens are subject. International treaties, for example,

---

81. Geltzer, *supra* note 55, at 452; *see supra* Part III.B. (describing several failed attempts).

82. *See supra* Part III.B.2–3.

83. Declan McCullagh, *HavenCo: Come to Data*, WIRED (June 5, 2000), http://www.wired.com/politics/law/news/2000/06/36756. In 1996, the United States shut down Iran's Internet access at Austria's Vienna University, through which it was routed at the time. *Id.*

84. This kind of overreaching has prompted backlash against the United States, and today is perhaps less common, but still not impossible. McCullagh, *supra* note 83.

85. *See infra* Part III.E. (exploring in depth how this potential has tremendous power in some relationships and should not be underrated).

86. Burk, *supra* note 20, at 60–62 (discussing the complications and limitations of enforcing IP and patent rights in foreign jurisdictions).

87. Because most people do not own assets in the foreign jurisdictions through which their internet transactions occur, there is little danger of material loss. "So as long as you keep yourself, and your assets, out of [e.g.] Latvia, you don't really have to worry about the ever-present, but entirely theoretical, problem of being hauled into a . . . Latvian courtroom." David G. Post, *Governing Cyberspace: Law*, 24 SANTA CLARA COMPUTER & HIGH TECH L.J. 883, 893 (2008).

traditionally affect only nations. National laws like RIPA, which authorized Britain to reach out to Sealand and the abortive HavenCo, are only applicable to havens within reach of that nation's jurisdiction.[88] This naturally creates motivations for countries to expand their jurisdictions and therefore their physical control; a desire which treaties like the Third United Nations Convention on the Law of the Sea (UNCLOS) helped fulfill.[89]

In the decades since Sealand's 'founding,' UNCLOS came into force and extended the definition of Territorial Waters to include area within twelve nautical miles of a nations' coastline, thereby, subsuming the geography of Sealand back into the jurisdiction of the United Kingdom.[90] This returned to Britain control over the territory upon which Sealand existed, and therefore control over activities carried out thereon.[91] This application of UNCLOS-based jurisdiction illustrates another advantage of floating data centers: they are not limited to being planted near shore or even on the continental shelf.[92] Mobile data havens could thereby avoid this form of jurisdictional regulation.

3. Mobile Data Havens Could Avoid Jurisdictional Regulation

In general, U.S. Courts have held that "different results should not be reached simply because business is conducted over the Internet" even if the source of the electronic data is outside of the end user's or the court's jurisdiction.[93] Conducting electronic commerce with residents of a jurisdiction constitutes availment of that government's benefits and so empowers its courts to reach beyond their customary jurisdictions to grasp accused offenders in other regions.[94] As such, traditional data protection laws would seem to apply even to data havens. However, *mobile* data havens have the ability to place themselves physically and permanently beyond a nation's boundaries. In this manner, a mobile data haven makes moot the question of whether a particular court can acquire power over it using traditional notions of jurisdiction since it can exist outside of all governments' legal borders.[95]

D. Extra-Jurisdictional Regulation and International Law

Normally, when objectionable activity by data centers or their users encroaches on protected data, e.g. patents, liability for such infringement is

88. Regulation of Investigatory Powers Act (RIPA), 2000, c. 23, §§ 6–11 (Eng.), *available at* http://www.legislation.gov.uk/ukpga/2000/23/contents.

89. UNCLOS, *supra* note 4; *see supra* Part II.C. (explaining the expansion codified in UNCLOS).

90. UNCLOS, *supra* note 4. UNCLOS came into force in 1994. *Id.*

91. *Id.*

92. This note does not explore the question of whether standing upon, or being grounded in, the continental shelf makes all platform-based data centers susceptible to regulation under the claim that they are extensions of the sea floor and therefore fall within nation's exclusive economic zone rights or continental shelf rights.

93. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119, 1124 (W.D. Pa. 1997).

94. *Id.* at 1126.

95. By definition, *e.g.* "1. A government's general power to exercise authority over all persons and things within its territory." BLACK'S LAW DICTIONARY 707 (8th abg. ed. 2005); *see* Ruhrgas AG v. Marathon Oil Co., 526 U.S. 574, 583 (describing the types of and constraints on domestic jurisdiction generally).

imposed by the government controlling the center's physical jurisdiction.[96] The standard solution for data centers in other countries and for cross-border patent protection has been to induce the host nation to enforce the data owner's rights.[97] Mobile data havens, however, are able to move into and out of—or even remain beyond—a nation's jurisdiction, and so the standard solution becomes inapplicable.[98] Absence evidence of purposeful availment, traditional legal mechanisms for regulating extra-jurisdictional data centers fail.[99]

This Section instead explores the customary international law concepts related to acquiring jurisdiction over a vessel in international waters; first, the general judicial presumption which prohibits such meddling, and second, two principles which have the potential to create exceptions.

1. Presumption Against Extraterritoriality

The "presumption against extraterritoriality" stems from the assumption that, as Chief Justice Rehnquist put it, when Congress legislates it is "primarily concerned with domestic conditions."[100] Today this doctrine is a historic and powerful admonition that legislation is meant to apply only within the territorial jurisdiction of the United States unless the legislature has manifested a contrary intent.[101] This intent clause of the presumption has mired the doctrine in ambiguity and inconsistency in the U.S. as courts struggle over what evidence of legislative intent is sufficient to rebut the presumption against extraterritoriality, and whether the presumption is to be applied uniformly to all statutes.[102]

a. Legislative Intent

In declining to enforce a statute extraterritorially, Rehnquist wrote in *Aramco* that statutes could overcome the presumption against extraterritoriality only through a "clear statement" in the statute itself indicating congressional intent to apply the statute abroad.[103] The issue of whether Congress has

96. *See* Burk, *supra* note 20, at 66 (noting that "when such activity by data service providers or subscribers knowingly encroaches on the patent, imposition of liability for direct infringement and inducement would be appropriate."). *See also* Ted L. Field, *The "Planes, Trains, and Automobiles" Defense to Patent Infringement for Today's Global Economy: Section 272 of the Patent Act*, 12 B.U. J. SCI. & TECH. L. 26, 29 n7 (2006) (discussing the enforcement of patent rights internationally).

97. Eric W. Guttag, *When Offshore Activities Become Infringing: Applying § 271 to Technologies that "Straddle" Territorial Borders*, 14 RICH. J.L. & TECH. 1, ¶¶ 52–75 (2007) (discussing the evolution of border-straddling patents).

98. Burk, *supra* note 20.

99. *Id*.

100. EEOC v. Arabian Am. Oil Co. (*Aramco*), 499 U.S. 244, 248 (1991) (quoting Foley Bros. v. Filardo, 336 U.S. 281, 285 (1940)).

101. James E. Ward, *"Is That Your Final Answer?" The Patchwork Jurisprudence Surrounding the Presumption Against Extraterritoriality*, 70 U. CIN. L. REV. 715, 715 (2002) (citing *Aramco*, 499 U.S. at 248 (1991)).

102. *See id.* at 716 (stating that the lower courts use diverse approaches to the issue).

103. *See id.* at 723–25 (discussing the history of the standards needed for setting up extraterritorial jurisdiction).

intentionally exercised its authority to enforce laws beyond the national boundaries is therefore one of statutory interpretation; courts should therefore look to the text for the operation of the statute.[104] Whether the intellectual property statutes governing mobile data havens will pass or fail this test remains to be seen, however the presumption initially stands against them.

b. International Law

The presumption against extraterritoriality also specifies that the court "look to the operation of the statute to determine whether the exercise of extraterritorial jurisdiction complies with principles of international law."[105] In the instant case, the self-executing UNCLOS treaty also seems to deprive U.S. of extraterritorial jurisdiction[106] with its declarations about the inviolability of the high seas.[107] Though the U.S. Congress has withheld its approval, UNCLOS nonetheless received enough endorsements to execute,[108] and has now risen to a level of acceptance such that it is considered a part of customary international law. Both congressional intent and international law therefore seem to prevent interference with an oceangoing data haven in international waters.

2. Offsetting Principles

Two countervailing principles support the ability of the United States to extend its jurisdiction to such vessels: the Passive Personality Principle and the Protective Principle.

a. Passive Personality Principle

This controversial principle represents the idea that all crimes against a citizen are automatically within the jurisdiction of the victim's country of citizenship.[109] This notion is opposed by most countries and was also disfavored by the United States until the 1970s, when the U.S. adopted it in defense of its measures to curb terrorism.[110] This principle has since been officially recognized in the U.S., where a "special maritime and territorial jurisdiction" has been created that includes "[a]ny place outside the jurisdiction of any nation with respect to an offense by or against a national of the United

104. *E.g.*, United States v. Neil, 312 F.3d 419, 421 (9th Cir. 2002) (giving explanation of statutory interpretation).

105. *Id.*

106. United States. v. Postal, 589 F.2d 862, 875–76 (5th Cir. 1979). "Self- executing" is a somewhat circular test inserted by the *Postal* court. *Id.*

107. *See Oceans and Law of the Sea*, UNITED NATIONS: DIV. FOR OCEAN AFFAIRS & THE LAW OF THE SEA, http://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm (last visited Sept. 28, 2010) (providing a list of the UNCLOS signatories).

108. *Id.*

109. BOLESLAW ADAM BOCZEK, INTERNATIONAL LAW: A DICTIONARY 79 (2005).

110. *E.g.*, *id.* at 79–80 (describing this adoption, which provided jurisdiction under which the U.S. could try terrorism suspects for crimes that would otherwise have had no connection to American courts).

States."[111] Since infringement of U.S. intellectual property rights will by definition harm the right's owner, the Passive Personality Principle effectively brings all such infringement within the "special maritime and territorial jurisdiction of the United States."[112]

c. Protective Principle

The Protective Principle, which receives broader support on the international stage, justifies the exercise of jurisdiction by courts over foreign entities' conduct when it is both domestically criminal and harmful to national interests, particularly national security interests.[113] This principle is used in the U.S. to prosecute national security offences, currency offences, desecration of flags, economic crimes, forgery or fraud regarding official documents, and immigration and political offences.[114] Under international law the Protective Principle is applicable in situations involving a potentially adverse effect on either the sovereign's security or governmental functions.[115] Since protecting personal property rights is a function of government, the Protective Principle is arguably applicable to oceangoing data havens.

However, U.S. courts only allow a statute to override international law if the legislature has expressed the clear intent to supersede it.[116] Given that neither the statutory authority for customs enforcement nor the wording of the "special maritime jurisdiction" statute specifically extends U.S. jurisdiction over a foreign vessel outside of the EEZ, boarding a vessel in international waters cannot be justified merely on proof of activities which may violate U.S. law in another location.[117] To utilize the Protective Principle to intrude on a vessel in international waters, even one containing a data haven, would therefore require a showing of more than just possession of illegally obtained and transported property. Since the Passive Personality Principle is also uncertain to be strong enough to overcome the presumption against extraterritoriality, the next section address several more practical methods for gaining control over an illicit data haven.

E. Practical considerations

There are several practical impediments that attach, in varying degrees, to

111. Special Maritime and Territorial Jurisdiction of the United States, 18 U.S.C. § 7(7) (2006).

112. *Id.*

113. *E.g.*, Brian L. Porto, Annotation, *EXTRATERRITORIAL CRIMINAL JURISDICTION OF FEDERAL COURTS*, 1 A.L.R. Fed.2d 415, IV § 27–28 (2005) (discussing whether jurisdiction exists over offenses committed outside the United States under the protective principle of international law).

114. *See id.* (discussing cases that deal with national security offences, currency offences, desecration of flags, economic crimes, forgery or fraud regarding official documents, and immigration and political offences).

115. United States v. James-Robinson, 515 F. Supp. 1340, 1345 (S.D. Fla. 1981).

116. *Id.* at 1343 (citing Murray v. The Schooner Charming Betsey, 6 U.S. (2 Cranch) 64, (1804)); RESTATEMENT (SECOND) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 3(2).

117. Possession of and conspiracy to import marijuana into the United States, for instance, is not alone sufficient to trigger the expanded "special maritime and territorial jurisdiction of the United States." United States v. Cadena, 585 F.2d 1252, 1258–59 (5th Cir. 1978).

all data storage operations. While a mobile sea-going data haven could avoid some of these consequences, this section discusses the political, financial, and treaty difficulties that would unavoidably be faced by any such attempt to be completely free from influence.

1. Political and Macroeconomic Pressures

Countries, by their nature, have international political and economic relations and dependencies that make them susceptible to political and economic pressures. Even the venerable Swiss banking system, long renowned for uncompromising anonymity and discretion, has recently yielded to public and political pressures to disclose client details.[118] This capitulation serves as an example of how strong such pressures can be; if even the institutions of famously neutral Switzerland can be made to acquiesce, albeit only for suspected terrorist financiers or tax evaders, it is unlikely that many other nations could resist the pressures to surrender the secrets of suspected criminals.[119] Firms seeking to establish a data haven will be hard pressed to find a country, particularly a small and far-flung one of the type likely to have abstained from intellectual property conventions, which could withstand such pressures.[120] Avoiding national ties would help a data haven maintain its autonomy, and an untethered haven may therefore be able to avoid this consideration entirely.[121] However, economics are an issue not only for countries, since even pirate data havens will have operating expenses requiring financing.

2. Financial Connectedness

When offshore (i.e. foreign) data havens began arising, major nations' financial regulators noticed and began considering the problem.[122] Michael D. Mann, formerly a director of the Securities and Exchange Commission's international enforcement, commented on a flaw in the data haven model, noting that even markets in cyberspace must connect with the material world's conventional economy; "[y]ou can have all the secrecy and protection in the world as long as you don't need to write a check or wire a dollar."[123] Since even extra-jurisdictional data havens have financial connections, their real-world monetary transactions serve to bring otherwise isolated entities within range of government regulation.[124] To the extent that financial movements are

118. *E.g.*, Hasnain Kazim, *Tax Havens Give In to EU Pressure*, SPIEGEL ONLINE INT'L (Mar. 13, 2009), http://www.spiegel.de/international/business/0,1518,613252,00.html (noting that even Switzerland has loosened some of its bank secrecy laws).

119. *Id.*

120. As IsleBytes discovered, not even Anguilla provide sufficient assurances to satisfy their need for autonomy and security. Markoff, *supra* note 79, at 14.

121. Communications between ship and shore are addressed *infra* Part III.E.3.a.

122. Markoff, *supra* note 79, at 14.

123. *Id.*

124. *Id.*

traceable, political pressures can be applied to the financing countries,[125] and might even bring the offending party within a court's jurisdiction.[126]

3. Applicability of the Law of the Sea

Although the Law of the Sea does grant to nations regulatory powers and maritime rights, this jurisdiction is bounded both geographically and in scope.[127] These limitations allow offshore data havens – particularly mobile data havens – to potentially elude government control. This Section describes these gaps and points to a possible workaround for regulators seeking to prevent the uninhibited transfer of protected data.

a. Limited Applicability to Data Centers

When UNCLOS came into effect in 1994, it redefined and harmonized the rights of nations to the waters surrounding them.[128] Defining territorial waters to extend out to twelve nautical miles gave Britain nominal control over Sealand,[129] though the actual measure of control granted by RIPA and UNCLOS has yet to be given a thorough legal testing. These new laws should at least limited the ability of would-be nation founders to claim islets or vestigial structures as their private fiefdoms, since these too would now be subject to the same limitations.[130]

Mobile data centers floating near shore would likewise be encumbered by the regulatory authority granted to signatory nations by UNCLOS.[131] However, since within their contiguous zone states' enforcement powers are restricted to immigration, revenue, customs and sanitary regulation,[132] a state has—at best—limited rights to proscribe data-bearing and data-transmitting boats. Moreover, in the portion of their Exclusive Economic Zone that is beyond the twenty-four mile contiguous zone, states' control is even more circumscribed; control is granted only over natural resources below the surface, and then only to natural resources like fish, minerals, and oil.[133]

Rights to energy generated by wave motion and thermal differences are

125. *See supra* Part III.F.1.

126. *C.f.* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 472–79 (1985) (clarifying the purposeful availment test).

127. *Supra* Part II.B.

128. UNCLOS, *supra* note 4. *See generally* The United Nations: Division for Ocean Affairs and the Law of the Seas, *The United Nations Convention on the Law of the Sea (A Historical Perspective)*, http://www.un.org/Depts/los/convention_agreements/convention_historical_perspective.htm (last visited Sept. 28, 2010) (describing the key provisions of UNCLOS).

129. *See* Dennis, *supra* note 23, at 266-67 (explaining that Sealand is located seven miles off the coast of Britain, which placed it outside the old three-mile limit of Britain's territorial waters and therefore prevented British courts from exercising jurisdiction over it in 1968, prior to the adoption of UNCLOS).

130. *See generally supra* Part II.B. and accompanying notes (explaining the expansion of nations' power over territorial waters). Territorial waters include natural and man-made islets alike. *Id.*

131. *Id.*; UNCLOS, *supra* note 4.

132. UNCLOS, *supra* note 4, at art. 33, ¶ 1.

133. *See supra* Part II.B and accompanying footnotes (describing the rights of states in the different distances from shore).

protected within the EEZ, and so a data haven thusly powered within this zone would fall under the theoretical treaty jurisdiction of nearby signatories (which the U.S. is not).[134] Pirate data havens moored beyond a signatory's EEZ or powered by other means, however, would remain unrestrained.

b. "In Touch with the Shore" Exception

A possible exception to a ship's autonomy arises if its communications with shore violate local national laws. Though little-used, there exists a historic "in touch with the shore" exception designed to catch ships that would otherwise retreat to safety across the territorial waters boundary.[135] This authority, at least arguably under the laws of the United States, potentially grants authority to exercise control for the purpose of preventing violations of the nation's right to regulate its territorial and contiguous zones.[136] This power is restricted to national defense, to the specific interests of enforcement of customs and safety regulations or to another concerns agreed upon by treaty.[137]

Because a data center is useless if users are unable to connect to it, its value depends upon contact with the outside world, which consists (at least at present) almost entirely of nations. The back-and-forth communication implicit in the operation of such a data center could bring the data center within a nation's authority under the "in touch with the shore" exception, if asserted.[138] To achieve high bandwidth connections with users, a mobile data center is likely to connect to local terrestrial networks with electronic or optic cables to the nearest shore, making obvious their communication link.[139] Transmissions directly to satellites might overcome the necessity of a direct connection to shore without sacrificing privacy, but would then open the door for regulation through the owner of the satellites.[140] Therefore, unless and until clients no longer have need of land-based communication—perhaps through private satellite networks that are beyond government regulation—the "in touch with the shore" exception[141] could suffice to gain jurisdiction over even mobile seagoing data havens.

134. *See* UNCLOS, *supra* note 4, at art. 56, ¶ 1 (granting sovereign rights for "exploitation and . . . production of energy from the water, currents and winds").

135. 48 CJS *Int'l L.* § 14 (2009) (explaining that "a state may exercise authority to prevent violation or evasion of its revenue, customs, immigration, or sanitary laws . . . by ships hovering off the territorial limit, or in touch with the shore."). For an application of this exception, *see* U.S. v. Louisiana (The Louisiana Boundary Case), 394 U.S. 11, 22 (1969) (stating the assertion of jurisdiction over a vessel was proper, despite its distance from shore, to prevent it from violating national laws enforceable within the boundary).

136. 48 CJS *Int'l L.* § 14 (2009).

137. *Id.*

138. *Id.*

139. Broadcast connections to shore would be vulnerable to interception by a well- placed antenna, and to signal leakage, both of which a client seeking high security would find unacceptable.

140. Similarly to the regulation of other physical assets. *See supra* Part III.C.1. (discussing this influence).

141. 48 CJS *Int'l L.* § 14 (2010).

IV. RECOMMENDATIONS

The ability of mobile data havens to avoid regulation[142] should concern intellectual property and data regulators.[143] Based on the history presented and the analysis conducted in this Note, regulators should implement anti-piracy measures wherever possible. The following sections therefore recommend that regulators: utilize their own governments' clout to leverage political and economic pressure against countries harboring or supporting data havens; appeal to offenders' nations of citizenship to discipline them; obtain jurisdiction over firms and persons in violation of national laws through their financial arrangements; revitalize and expand the "in touch with the shore" exception to reach vessels through their communications; and utilize the principles of international law when they are applicable. Additionally, far-sighted regulators should also consider the next frontier of data storage and transmission, and establish principles for controlling the flow of data between satellites and elsewhere in space.

A. Assert Control Through Existing Means

Despite the ability of Google's conceptualized oceangoing data storage vessels to avoid current informational regulation, pragmatic forces are available that can limit even a mobile data center's practical ability to function. Four such approaches are suggested in the following subsections.

1. Political and Economic Pressures

Ports of call offer opportunities for regulators to take advantage of vessels' needs to refuel and resupply to assert their authority. This opportunity stems from the physical requirement for reaching a dock: that the vessel must enter a nation's Territorial and perhaps Internal Waters, over which that nation's government has dominion.[144] Therefore, governments seeking to pressure patent infringers can do so by regulating the problem vessels if they utilize that government's ports. An influential and motivated nation, *e.g.* the United States in relation to its Caribbean neighbors, can also reach out to vicariously limit a vessel's ability to dock at foreign ports by applying political or economic pressure on the those ports' governments.[145]

Limiting the ability of vessels to dock at foreign ports does require *ex ante* knowledge of where a vessel will be docking. It also requires the political will to pressure the nations being visited. By cooperating, the regulatory agencies of the world's largest nations might be able to overcome the latter

142. *See supra* Part III.C.

143. *See supra* Parts I and III.E.

144. UNCLOS, *supra* note 4, at art. 2(1) (explaining that "[t]he sovereignty of a coastal State extends beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea"). The same requirement would apply to service and supply vessels which attempted to act as intermediaries. *Id.*

145. *See supra* Part III.E. regarding the applicability of this option.

hurdle by jointly imposing an embargo on their trading partners which permit passage and safe harbor to data havens found to be enabling illegal or piratical uses of data. As regulators seek to cast a broader net, proportionately more political capital will need to be expended.

Even were there general willingness to attempt to deprive a suspect vessel of all potential ports of call, such an effort may still be imperfect. Consider the yet-intractable problem of piracy off of the Somali coast, which has not been deterred despite the large human and economic costs[146] and despite the coordinated efforts of European Union, NATO, Russia, China, the United States, the African Union, and others.[147] An oceangoing data center such as Google envisions may not be able to cross the high seas, but it would by design be able to relocate, and so be able to travel to and from lawless areas of the world. The inability of the developed world's navies to prevent simple piracy in the Indian Ocean, and of such sophisticated nations as the United States to close its own borders against the flow of illegal drugs,[148] bodes ill for any attempt at a universal solution.

2. Nations of Citizenship of Offenders

If an operator of the offending data center is a citizen of the regulator's country, then regulators may be able to acquire jurisdiction over the operator through that relationship. If the operator is a citizen of a friendly or receptive nation, their government may be convinced to do the same. This secondary enforcement will suffer under the same encumbrances as would any attempt to coordinate a world-wide ban on admitting oceangoing data havens to nations' ports. Even if jurisdiction can be established or foreign cooperation can be induced, parties plaintiff and regulators still bear the burdens of serving notice upon and acquiring physical control over a transient person or vessel.

3. Financial Ties

Regulators should continue to pressure financial centers to ensure the legality of their clients' activities and to verify or at least report suspected breaches. If the nations through which extra-jurisdictional data centers finances are routed can be determined, then these economic points of contact can be used to limit the freedom and profitability of illicit data havens.[149] This could be done directly by freezing or seizing assets suspected of being used in

146. *E.g.*, Stephen Askins, *Piracy: A Review of 2009*, INCE & CO SHIPPING E-BRIEF, Feb. 2010, at 14–16, http://www.incelaw.com/whatwedo/shipping/article/shipping-e-brief-february-2010/Piracy-a-review-of-2009.

147. Jacquelyn Porth, *International Navies Coordinate to Deter Somali Pirates*, AMERICA.GOV (Feb. 19. 2010), http://www.america.gov/st/peacesecenglish/2010/February/20100219174011SJhtroP0.8000299.html.

148. *See, e.g.*, Drug Policy Educational Group, *No Data on Effectiveness*, DRUG POLICY NEWS, Spring/Summer 2001, at 5 (detailing the problems inherent in stopping the drug trade). *See also* Brian Doherty, *The International War on Drugs Hits Close to Home*, REASON.COM (Mar. 4, 2009), http://reason.com/archives/2009/03/04/the-international-war-on-drugs (describing the failure of the "War on Drugs" to eradicate either production or importation of marijuana and cocaine).

149. *See supra* Part III.E.1–2; Markoff, *supra* note 79, *attributed to* Michael Mann, former Director of International Enforcement for the SEC.

the furtherance of intellectual property theft or illegal redistribution.

Even if the financial assets themselves turn out to be unreachable, regulators should nevertheless strive—within the boundaries of the law—to uncover and track the transactions of their targets. Should such transactions take place within the regulators' own nation, or within an ally's, then the transactions alone might suffice to establish personal jurisdiction over the transgressor. This could then enable the full utilization of the judicial system against them.

This approach has the advantage of being effective against all profitable data havens, given their need to purchase fuel and supplies and their owners' interconnections to the global financial market. This approach is also is limited by the same functional obstacles as have been discussed in the previous two subsections, namely regulatory willpower and foreign governmental cooperation. For any of these three practical forms of control to be realized, the government's leaders will have to make a bona fide commitment to and investment in their success.

4. Utilize the "In Touch with the Shore" Exception

The "in touch with the shore" exception to the UNCLOS boundaries could provide a justification for intercepting ocean-going vessels exchanging prohibited communication with a nation's data infrastructure.[150] This device has seldom been used, most recently four decades ago.[151] Nonetheless, since a data center is only useful when it can be reached by electronic communications, regulators concerned with off-shore data havens should strive to confirm the validity and import of this exception through publications or test cases extending it to cover the type of pass-through communication likely between an oceangoing data center and their shores,[152] to make it easier for prosecutors to pass the threshold questions for federal extraterritorial criminal jurisdiction.[153]

B. Looking forward: Regulating Data in Space

Direct links between an oceangoing data haven and the terrestrial networks that stand upon a nation's shore might be avoided by utilizing

150. *See supra* Part III.C.3.b.

151. The most recent case is *U.S. v. Louisiana* (Texas Boundary Case), 394 U.S. 1 (1969).

152. In which the purpose of communication is not to share information between the vessel and the receiver on shore, but for the receiver to act as a mere relay into conventional data networks.

153. *Compare* U.S. v. Georgescu, 723 F. Supp. 912, 912 (E.D.N.Y. 1989) (holding that federal jurisdiction existed when a Romanian national flying into New York City from Denmark was indicted for committing a criminal sexual act while within the special aircraft jurisdiction of the United States), *and* U.S. v. Pizzarusso, 388 F.2d 8, 10 (2d Cir. 1968) (holding that a false statement under oath while applying for a visa, regarding places of residence and arrested record, created jurisdiction because of adverse effect on governmental function of border control), *with* U.S. v. James-Robinson, 515 F. Supp. 1340, 1346 (S.D. Fla. 1981) (holding that possession of and conspiracy to smuggle marijuana into a third country did not create federal jurisdiction because the border security of the United States was not endangered).

satellite communication, but satellites themselves are still owed by entities which can be regulated. Regulating the data transmitted through communication satellites would be analogous to regulation of the satellites themselves. To confront these difficulties, far-sighted regulators should also consider the next frontier of data storage and transmission, and should proactively establish the regulatory foundations for controlling the flow of data to and from satellites in outer space.

1. Freedoms

Since the abridgement of the vaulted *ad coelum* doctrine[154] in the early twentieth century,[155] maritime law has been used as a template for the regulation of outer space.[156] The governing treaty for outer space, analogous to the role of UNCLOS to international waters, is the Outer Space Treaty.[157] The Outer Space Treaty declares that the "exploration and use of outer space . . . shall be the province of all mankind"[158] and that outer space "is not subject to national appropriation by claim of sovereignty."[159]

Regulators should prepare to analogize this freedom from appropriation of outer space to the freedom from restraint upon the high seas. Just as there are situations enabling the United States to extend jurisdiction to vessels in international waters, regulators should push for the Protective Principle of international law to be extended to the heavenly context.

2. Restraints

Notwithstanding these liberties, State parties to the Outer Space Treaty are obligated to authorize and supervise the activities of non-governmental entities.[160] This oversight requirement for commercial activity is intended to prevent negligent or malicious acts by private citizens, by encouraging signatory nations to ensure the safety of their citizens' technology, lest the nation itself be penalized in accordance with the Outer Space Treaty.[161]

---

154. *Cujus est solum, ejus est usque ad coelum*, "whoever has the land possesses all the space upwards indefinitely." 2 WILLIAM BLACKSTONE, COMMENTARIES *18.

155. The doctrine of *ad coelum* was not negated in the United States until 1946. U.S. v. Causby, 328 U.S. 256, 261 (1946).

156. *E.g.*, Dan L. Burk, *Protection of Trade Secrets in Outer Space Activity: A Study in Federal Preemption*, 23 SETON HALL L. REV. 560, 574 n.93 (1993) (noting one analogy between outer space and the high seas as being outer space law").

157. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty), Oct. 10, 1996, 18 U.S.T. 2410, 610 U.N.T.S. 8843, *summarized at* United Nations Office for Outer Space Affairs, *Outer Space Treaty*, [hereinafter Outer Space Treaty], http://www.unoosa.org/oosa/SpaceLaw/outerspt.html, (last visited Sept. 28, 2010).

158. Outer Space Treaty, *supra* note 157, art. I.

159. *Id.*, art. II.

160. "The activities of non-governmental entities in outer space . . . shall require authorization and continuing supervision by the appropriate State Party to the Treaty". *Id.* at art. VI (2).

161. Major Ronald L. Spencer, Jr., *State Supervision of Space Activity*, 63 A.F.L. REV. 75, 82 (2009). This is based on the currently realistic assumption that all spaceflight is sponsored by governments or conducted by nationally registered entities. *Id.*

Remedies for harm are expounded in the Liability Convention,[162] which explicitly holds the launching state liable for damages caused by its space objects.[163] Though these provisions were intended to address physical damage to terrestrial and airborne objects,[164] they may be extensible to intellectual property transgressions causing monetary harm.

Regulators should seek systems capable of tracking the passage of data to and amongst communications networks, so that any economic harm caused by the misuse of that data can be recognized and attributed to a specific communications satellite, allowing that satellite's operator to be held liable—just as they are for physical damages.[165] Though costly, such a system would prompt communication satellite operators to limit their liability by curtailing the illicit uses of their equipment. Even then, this incentive will only motivate the satellite system owners if liability can be imposed on the operator as well as on the user. Prompt adoption of such systems will help steer the development of space-based communications and storage towards a model where regulators will have the willing assistance of the facility owners in preventing illicit uses of their systems.

V. CONCLUSION

The ocean-going computing center patented by Google raises the possibility of mobile data havens operating beyond traditional jurisdictions and regulations. Current regulatory tools can only tangentially affect this capability, so the ability to limit piratical data havens potential to violate intellectual property and data privacy laws will depend largely on the ability of governments to induce compliance from complicit nations. Political, economic and financial pressure may all be useful in this attempt. The principles allowing exceptions from the presumption against extraterritoriality should be the basis for law enforcement efforts to control seafaring data havens. Regulators should also plan for the governing of satellite and space-based communication systems, lest data pirates are able undercut intellectual property rights and escape regulation in the heavens as well as on the seas.

162. Convention on International Liability for Damage Caused by Space Objects (Space Liability Convention), G.A. Res. 2777(XXVI), U.N. GOAR, 26th Sess., Annex., II, (Sep. 1, 1972).

163. Major Arie J. Schaap, *Cyber Warface Operations: Development and Use Under International Law*, 64 A.F.L. REV. 121, 161 (2009) (citing *id.*).

164. *Id.*

165. Commercial Space Launch Act of 1984, 49 U.S.C. § 70112(a). The U.S. 'requires commercial operators to indemnify it for the first $500 million of 'damage to other parties. *Id*.