CHAPMAN LAW REVIEW

Citation: Sam Mulopulos, *Digital Trade Zones: Answering Impediments to International Trade in Information*, 21 CHAP. L. REV. 443 (2018).

Digital Trade Zones: Answering Impediments to International Trade in Information

*Sam Mulopulos**

TABLE OF CONTENTS

INTRODUCTION

In an age where information has become as significant as any natural resource, data remains fiercely constrained by protectionism. Whether out of genuine, yet misunderstood, concerns for privacy and cybersecurity or because of simple, unabashed protectionist instincts, countries around the world have pursued policies designed to impede cross-border data flows, localize data, and stifle digital trade. These digital trade barriers—such as, requiring data on citizens of a country to be stored in country rather than on overseas servers—increase costs, cut against competition (especially for small Internet-based businesses), and frustrate innovation.

As countries continue to erect digital trade barriers, the value of the global information flow diminishes. While a recent report by the U.S. International Trade Commission estimates that the Internet improves the productivity of digitally intense industries by 7.8% to 10.9%,[1] barriers from the European Union ("EU") to China pose a direct challenge and potential impediment to that productivity. Data localization requirements and restrictions on cross-border data flows, perhaps more than any other digital trade barrier, impede the next generation of international trade facilitation—cloud computing. In recent years, cloud traffic has increased from 3.5 to 5.6 zettabytes[2] and will reach 10.4 zettabytes by 2019.[3] Cloud computing is particularly useful because it "provides portability" and "allows for more seamless upgrades and transitions to new or multiple devices, because content does not need to be laboriously copied from one device to another."[4]

However, the success of cloud computing, and electronic commerce at large hinges on a global distribution of servers. Lack of servers and enormous distances between them can be the cause of lethargic delivery times, which undermines international trade.[5] Therefore, restrictions on digital trade frustrate the

---

* The views expressed herein belong solely to me. I would like to thank Patrick Holvey, Al Gidari, Bill Watson, and Carolyn Iodice for their advice and wisdom.

1 Digital Trade in the U.S. and Global Economies, Part 2, Inv. No. 332-540, USITC Pub. 4485, at 65 (Aug. 2014) (Final).

2 A zettabyte is one trillion gigabytes. *See* Thomas Barnett, Jr., *The Zettabyte Era Officially Begins (How Much is That?)*, CISCO BLOG (Sept. 9, 2016), https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that [http://perma.cc/X8YT-QFDB].

3 Markham C. Erickson & Sarah K. Leggin, *Exporting Internet Law Through International Trade Agreements: Recalibrating U.S. Trade Policy in the Digital Age*, 24 CATH. U. J.L. & TECH 317, 333 (2016).

4 *Id.* at 334.

5 *See* Steven R. Swanson, *Google Set Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 715, 741 (2011).

distribution of the global network needed to make e-commerce and Internet-enabled international trade successful. Since it would be difficult for a state to block access to individual users, governments instead seek to control the flow of data higher up the chain, usually at the level of certain intermediaries like Internet Service Providers.[6] While reducing these barriers is a useful and necessary tool towards protecting free Internet-enabled commerce, it is also a traditional solution.

This article proposes an unconventional solution to the problem of digital trade restrictions: digital trade zones. Digital trade zones would be areas in which a country would forbear from jurisdiction over certain Internet and privacy laws in order to permit innovative arrangements between countries as a means of circumventing otherwise impeding digital trade restrictions. To date there has not been any discussion of creating special jurisdictions for the trade and treatment of data.[7]

This article lays a foundation for such a discussion. Part I highlights the key impediments to digital trade. Part II discusses the theoretical foundation of digital trade zones, analogizing this framework to both maritime law and Foreign Trade Zones ("FTZs") in the United States, each a key ingredient needed to make digital trade zones function. Part III anticipates successes and problems posed by digital trade zones in practice by presenting some of the potential mechanics of digital trade zones in the United States. Specifically, it proposes two types of zones—experimental zones and waystation zones—addressing, respectively, the impediments created by restrictions on cross-border data flows and data localization. Part III also contains a discussion of the ways in which digital trade zones offer answers to some common intellectual property rights violations frequently encountered in the course of trade. The Conclusion summarizes the work and proposes next steps to further the discussion.

I. IMPEDIMENTS TO DIGITAL TRADE

From galleons to gigabytes, international trade has come a long way.[8] Producers and consumers can be instantaneously connected, and the flow of information across the globe has facilitated a commercial revolution. While the world is more

---

6 *See id.* at 719.

7 A single article does discuss treating the emerging internet ecosystem broadly as a single "digital free trade zone." *See* Kristi L. Bergemann, *A Digital Free Trade Zone and Necessarily-Regulated Self-Governance for Electronic Commerce: The World Trade Organization, International Law, and Classical Liberalism in Cyberspace*, 20 JOHN MARSHALL J. COMPUTER & INFO. L. 595, 629 (2002).

8 From pieces of eight to 8-bit also hits the tone I am going for.

connected than ever, barriers to digital trade are being erected at an alarming pace. Despite the myriad of challenges facing individuals and industry engaging in e-commerce, three of the most common digital trade restrictions are data localization, restrictions on cross-border data flows, and intellectual property rights infringement.[9]

A. Data Localization

Data localization refers to mandates that require companies to engage in digital trade-related activities inside of the particular country in order to do business in that country.[10] Sometimes called "data nationalism," data localization is an extreme attempt by a government to restrict the flow of data from escaping beyond its control and its borders. Data localization can be contrasted with historical Internet border controls; while previous controls were mainly designed to keep information from entering a country, localization efforts build on this by preventing data from leaving.[11]

The most common localization efforts require that data storage facilities house data in the country or jurisdiction that originates the data.[12] For example, in 2015, Russia required that data collected by companies on Russian citizens be both processed and stored within Russia.[13] While there is still uncertainty about how the law will be implemented, the outlook for such localization requirements is not good. This is because Russia currently lacks the server capacity to shoulder the demand for data storage as required by the law.[14]

China also has localization restrictions aimed at cloud computing. Given its geographic agnosticism, cloud computing is frequently an unfortunate first casualty of data localization. In China, cloud computing is closed to foreign-invested companies and the country is presently seeking to limit foreign companies from offering cloud computing services if they are cross-border

---

9 OFFICE OF THE U.S. TRADE REPRESENTATIVE, NATIONAL TRADE ESTIMATE REPORT ON FOREIGN TRADE BARRIERS (2017) [hereinafter NATIONAL TRADE ESTIMATE REPORT] https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf [http://perma.cc/YL6U-DT56].

10 Digital Trade in the U.S. and Global Economies, Part 1, Inv. No. 332-531, USITC Pub. 4415 (July 2013) (Final).

11 Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 679 (2015).

12 *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, KEY BARRIERS TO DIGITAL TRADE (Mar. 2017), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade [http://perma.cc/BWV4-VU7A].

13 NATIONAL TRADE ESTIMATE REPORT, *supra* note 9, at 382.

14 *Id.*

services.[15] But localization is not limited to tyrannical regimes. Even Canada has caught the localization bug. British Columbia and Nova Scotia both have laws that require that personal information possessed by public institutions—such as schools, universities, or hospitals—must be stored and accessed only in Canada.[16]

Localization requirements such as these can be incredibly costly to service providers and consumers. Since, at its most extreme, localization could require a provider to construct physical data infrastructure in every jurisdiction where it does business, one can begin to imagine the expense that such requirements place on the private sector and the limitations they pose for global investment and business expansion. In Brazil, for example, a data center costs on average $60.9 million.[17] Even in the United States, construction of a data center can exceed $40 million.[18] In countries with more burdensome regulatory environments, construction costs could be even higher. For example, Chinese localization efforts could cost as much as 1.1% of the nation's gross domestic product.[19]

B. Cross-Border Data Flow Restrictions

Less extreme than data localization, restrictions on the flow of data across borders encompass a host of activities and regulations designed to impede information exchange. By limiting what types of data can be exported and how data flow restrictions can frustrate a broad range of e-commerce activities, banks may be unable to transfer data between international branches, and big data analysis may be limited by turning off the information spigot to companies that rely on cutting-edge marketing strategies.[20] Even individuals can be implicated by cross-border data flow restrictions. Consider that fifty-eight percent of eBay revenue comes from outside the United States and that Airbnb operates in more than 65,000 cities and 191 countries.[21] Consumers and companies in the United States are

---

15 *Id.* at 89.

16 *Id.* at 72.

17 Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet* (Univ. of Cal. Davis Sch. of Law, Working Paper No. 378, 2014).

18 *See id.*

19 Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, EUROPEAN CTR. FOR INT'L POL. ECON. 2 (2014).

20 *See* RACHEL G. FEFER, SHAYERAH ILIAS AKHTAR & WAYNE M. MORRISON, CONG. RES. SERV., R44565, DIGITAL TRADE AND U.S. TRADE POLICY 13 (2017).

21 Craig Smith, *70 Amazing eBay Statistics and Facts*, DMR, https://expandedramblings.com/index.php/ebay-stats/ [http://perma.cc/6UME-GT3R] (last updated Feb. 3, 2018); *About Us*, AIRBNB, https://www.airbnb.com/about/about-us [http://perma.cc/7DHL-67JP] (last visited Nov. 9, 2017).

connecting with international markets in a variety of innovative ways; they too can be entrepreneurially constrained by digital trade restrictions.

Restrictions on cross-border data flows are varied. Many are already familiar with China's Great Firewall, which blocks websites such as Twitter, Google, and Facebook.[22] In a recently issued policy, "On Cleaning up and Regulating Internet Access Services Market," China prohibits telecommunications carriers from permitting consumers access to virtual private network connections to contact data centers abroad.[23] The European Union is considering proposals on contract rules for digital content, such as streaming services and for goods sold online. Ostensibly designed to address "defective" content purchased online, it remains to be seen how this will limit the ability of U.S. providers to conduct digital business in Europe or lead to a bifurcation of service into separate geographic zones. These are just a handful of the numerous international limitations on data flows that threaten the free exchange of information throughout the world.

The numerousness of limits on cross-border data flows make the costliness of compliance with such efforts unsurprising. The Great Firewall blocks eleven of the top twenty-five global websites, and estimates place the total number of blocked sites at 3000.[24] This costs individuals and organizations countless dollars a year in lost business. Given the acceleration of cloud computing—twenty-two percent of OECD-based businesses[25] use cloud computing services—limiting the ability of the cloud to serve different populations easily is an expensive proposition.[26] Moreover, much of the value that comes from data is increasingly made by gleaning insights from data in real time.[27] Curtailing that real time analysis means placing an upper limit on a core part of data's intrinsic usefulness. Imagine a farmer relying on Internet-enabled equipment to plant crops more precisely. If that farmer is located in a country which limits his access to the cloud, the data he is simultaneously producing as he plants cannot be easily transformed from raw to useful information to make his activity more precise. Or consider the aircraft

---

22 NATIONAL TRADE ESTIMATE REPORT, *supra* note 9, at 90.

23 *Id.* at 89.

24 *Id.* at 90.

25 OECD stands for Organization for Economic Cooperation and Development.

26 *Expanding U.S. Digital Trade and Eliminating Barriers to Digital Exports: Hearing Before the Subcomm. on Trade of the H. Comm. on Ways and Means*, 114th Cong. 3 (2016) (statement of Robert D. Atkinson, President, Information Technology and Innovation Foundation) [hereinafter Atkinson Testimony].

27 *Id.* at 2.

manufacturing industry. A Boeing 737 engine produces twenty terabytes of data per hour.[28] Boeing utilizes this enormous amount of data to enhance safety and reduce flight delays. Boeing's Airplane Health Management system is used by commercial airlines that operate Boeing aircraft in real time to assess and mitigate potential aircraft problems.[29] Given that crossing borders is core to an aircraft's purpose, the success of this entire endeavor is rooted in Boeing's ability to move enormous amounts of data around the globe quickly and effortlessly. It is estimated that the Internet of Things, such as Boeing's engines, other industrial machines, and consumer electronics, will yield $11.1 trillion per year in economic impact.[30] Data flow limitations cut directly into that figure, threatening one of the largest potential additions to economic productivity in the coming years.

C. Intellectual Property Rights Infringement

Internet-enabled trade has simultaneously created new markets for intellectual property rights ("IPR") and caused a great proliferation of IPR infringement. Frequently, Internet piracy is named as a key trade barrier, including foreign countries hosting websites that post pirated content or connect people to such stolen content.[31] According to the U.S. Trade Representative, who issues lists of countries that are serial IPR violators, the countries on the "priority watch list" span the globe, including Algeria, Argentina, Chile, China, India, Indonesia, Kuwait, Russia, Thailand, Ukraine, and Venezuela.[32]

Infringement of IPR can take many forms. Often times, foreign websites will host pirated or stolen content. For example, MP3VA.com is a site based in Russia and Ukraine that sells unauthorized U.S. audio recordings.[33] The site registers more than 860,000 visits per month, with most of the visits coming

---

28 *See* John B. Maggiore, *Remote Management of Real-Time Airplane Data*, BOEING (2007), http://www.boeing.com/commercial/aeromagazine/articles/qtr_3_07/AERO_Q307_article4.pdf [http://perma.cc/T9BS-GL4Z]; Paul Mathai, *Big Data: Catalyzing Performance in Manufacturing*, WIPRO 3 (2011), https://www.wipro.com/content/dam/nexus/en/industries/process%20and-industrial-manufacturing/latest-thinking/2606-Big%20Data%20-%20Copy.pdf [http://perma.cc/KXA4-M89Y].

29 Atkinson Testimony, *supra* note 27, at 6.

30 *Id.* at 3.

31 FEFER, AKHTAR & MORRISON, *supra* note 20, at 16.

32 *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2017 SPECIAL 301 REPORT (2017) [hereinafter SPECIAL 301 REPORT] https://ustr.gov/sites/default/files/301/2017%20Special%20301% 20Report%20FINAL.PDF [http://perma.cc/LW35-7L6X].

33 *Id.*

from the United States.[34] A similar website is uploaded.net, which gives users access to different kinds of copyrighted content, such as movies, music, and books. Hosted in the Netherlands, uploaded.com uses a creative arrangement to make money whereby users receive greater compensation for the greater size of the file they pirate and load to the website.[35] Another website is taobao.com, an e-commerce platform that sells many counterfeit products. Taobao.com is one of the top websites in China.[36] Another example of IPR infringement is the theft of trade secrets. China is a repeat offender on this issue. While China has taken steps to address the theft of trade secrets, including amendments to the General Provisions of the Civil Law in March 2017 that extended civil intellectual property protection to trade secrets, there remains a long way to go.[37] This includes improving options for the use of preliminary injunctions and protections against frivolous trade secret litigation claims which can be used to gain advantage in unrelated disputes.[38]

Given the expansiveness of the Internet and the ease with which it facilitates IPR infringement, IPR infringement is exceptionally costly. Some estimate that Internet-enabled IPR infringement could be greater than the total volume of sales "through traditional channels such as street vendors and other physical markets."[39] An OECD study places trade in fake goods at $461 billion or 2.5% of global trade, and it has been noted that "the total magnitude of counterfeiting and piracy worldwide in all forms appears to be approaching, if not surpassing, the trillion dollar mark."[40]

D. Motivations to Limit Digital Trade

The motivation to limit digital trade to prevent violations of IPR may appear the most straightforward—preventing the raw profiteering from the sale of stolen goods. However, when it comes to other barriers to digital trade, the motivations are somewhat more opaque. Data flow restrictions and associated

---

34 *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2016 OUT-OF-CYCLE REVIEW OF NOTORIOUS MARKETS 9 (Dec. 2016) [hereinafter Notorious Markets] https://ustr.gov/sites/default/ files/2016-Out-of-Cycle-Review-Notorious-Markets.pdf [http://perma.cc/LMT2-RZ6K].

35 *Id.* at 14.

36 *See id.* at 12.

37 *See* SPECIAL 301 REPORT, *supra* note 32, at 30.

38 *Id.*

39 *Id.* at 13.

40 OFFICE OF THE INTELL. PROP. ENFORCEMENT COORDINATOR, U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT FY 2017–2019, at 20 (2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2016jointstrategicplan.pdf [http://perma.cc/U68K-6FUQ].

localization requirements have been enacted for a myriad of reasons by various countries.

The most common rationales respond to fears that sharing data abroad will open such data up to surveillance by foreign governments. This public motivation stems from dual desires to protect the privacy of the country's own citizens and a protectionist motivation to stimulate domestic technology and Internet companies. In the wake of the Snowden revelations, countries, including India and the EU, have pursued various efforts to guard against U.S. surveillance.[41] Brazil, Russia, India, China, and South Africa (collectively known as the "BRICS countries") have also sought to create a series of global transmission cables intended to be "a network free of U.S. eavesdropping."[42] From a civil liberties perspective, some have commented that centralizing data within certain countries only makes it easier for domestic agencies and law enforcement to spy on their own citizens by concentrating citizens' data more closely.[43] The veracity of claims that localization and data flow restrictions are primarily rooted in concern over foreign surveillance belongs in a paper all its own, and it is worth noting that some have pushed back against this notion by arguing that surveillance concerns are a veneer for what is ultimately digital protectionism against mostly American companies.[44]

Regardless of motivations, these efforts have demonstrated protectionist effects. Governments may believe that by limiting foreign competition, which is often American competition given the United States' technological and commercial dominance, a domestic technology industry may flourish. However, governments around the world have worried about the impediments this logic poses to the information economy globally. The OECD has asked countries to abstain from "barriers to the location, access and use of cross-border data facilities and functions" in order to "ensure cost effectiveness and other efficiencies."[45] In a survey of domestic companies, the Swedish National Board of Trade concluded that "trade cannot happen without data being moved from one location to another."[46]

---

41 *See* Chander & Le, *supra* note 17, at 10, 28.

42 *Id.* at 28.

43 *See id.* at 30. Chander and Le refer to this as the "Honeypot" problem. *Id.*

44 *See* Christopher Kuner, *Data Nationalism and its Discontents*, 64 EMORY L.J. ONLINE 2089, 2094–95 (2015).

45 ORG. FOR ECON. COOPERATION AND DEV., OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING 7 (Dec. 13, 2011), http://www.oecd.org/sti/ieconomy/49258588.pdf [http://perma.cc/BA4E-LLDA].

46 The National Board of Trade, *No Transfer, No Trade – the Importance of Cross-Border Data Transfer for Companies Based in Sweden*, 1 KOMMERSKOLLEGIUM 23 (2014).

II. DIGITAL TRADE ZONES IN THEORY

Digital trade zones possess two core theoretical tenets—freedom from data nationalism and existence as jurisdictions legally "outside" the territory of a country. Since digital trade zones do not presently exist, examination and understanding of these concepts is best done by analogy. The first tenet is demonstrated, in its purest form, on the high seas where nations are unable to exercise restrictions on the movement of Internet information. The second tenet is more real. FTZs in the United States offer a well-tested and successful framework to understand some of the basic mechanics of digital trade zones.

A. The High Seas

At their core, digital trade zones (just like all special jurisdictions) are areas with unique rules. While these are manmade creations, the distinction of being an original special jurisdiction belongs to the open ocean. Since there are no established digital trade zones from which to highlight, this Section returns to the sea in order to share by analogy how digital trade zones might be arranged.

1. The Precedent of Pirate Radio

In response to content restrictions imposed by the British Broadcasting Corporation, disc jockeys and music promoters started what was known as pirate radio and began to pipe rock n' roll music into Great Britain from vessels stationed in international waters.[47] These vessels, and some old naval forts located outside British territorial waters that were used for broadcasting, were usually anchored to the seafloor and supplied by tenders from the mainland.[48] In 1966, the most popular pirate broadcasters, Radio Caroline and Radio London, boasted an audience of over eight million listeners.[49] And Britain was not alone; the Netherlands had its share of pirate stations as well.[50]

At the time the pirate broadcasters were operating, controlling law was the 1958 Geneva Convention on the High

---

47 *See* Kimberley Peters, *Taking More-Than-Human Geographies to Sea: Ocean Natures and Offshore Radio Piracy*, *in* WATER WORLDS: HUMAN GEOGRAPHIES OF THE OCEAN 177, 178–80 (Jon Anderson & Kimberley Peters eds., 2014).

48 *See id.* at 182–83.

49 Horace B. Robertson, Jr., *The Suppression of Pirate Radio Broadcasting: A Test Case of the International System for Control of Activities Outside National Territory*, 45 LAW & CONTEMP. PROBS. 71, 75 (1982).

50 *See id.* at 76.

Seas.[51] This agreement did not approve or prohibit an explicit right to broadcast from the high seas.[52] In fact, the Convention only lists four core nautical freedoms: navigation, fishing, laying of pipelines and cables, and flight.[53] Some argue that so long as broadcasting or any other activity did not interfere with any of these four freedoms, it would be permissible under the Convention.[54]

Despite the apparent security offered under the Geneva Convention, pirate broadcasters were still targets of British and European authorities. To circumvent these authorities, the pirate broadcasters were known to fly a flag of convenience. These flags belonged to states that lacked the ability or will to hold pirate broadcasters accountable for their transmissions.[55] Coastal countries, like Great Britain, could not exercise authority over pirate broadcasters flying flags of convenience because only the flag state possesses sole jurisdiction over its vessels.[56] Early on, pirate radio learned the vital lesson that finding flags of convenience was necessary to avoid collapsing into the jurisdiction of the country which the pirates were attempting to avoid. Similarly, an embryonic digital trade zone—embodied in an oceangoing data center—would need to find a suitable flag of convenience to be able to exist apart from the onerous trade restrictions it seeks to evade.

In an effort to punish pirate broadcasters, the 1965 European Agreement for the Prevention of Broadcasts Transmitted from Stations Outside National Territories ("European Pirate Radio Agreement") required "that signatory flag states punish pirate broadcasters found on their own ships."[57] The European Pirate Radio Agreement did not establish a new form of jurisdiction, however. Instead, it aimed to strengthen enforcement by targeting "acts of collaboration," such as the provision or maintenance of the vessels, the provision of supplies to the broadcasters, and the provision of advertising to fund the pirate stations.[58] Even though the vessels and transmitters were themselves beyond reach of

---

51 *Id*. at 79.

52 *See id.*

53 *See* Convention on the High Seas art. 2, Apr. 29, 1958, 13 U.S.T. 2312, 450 U.N.T.S. 82 [hereinafter Convention on the High Seas].

54 *See* Robertson, *supra* note 49, at 79.

55 *See* Robert C. F. Rueland, Note, *Interference with Non-National Ships on the High Seas: Peacetime Exceptions to the Exclusivity Rule of Flag-State Jurisdiction*, 22 VAND. J. TRANSNAT'L L. 1161, 1225 (1989).

56 *See* Swanson, *supra* note 5, at 739.

57 *Id.*

58 Robertson, *supra* note 49, at 95.

European governments, the network of logistical, financial, and human support for pirate radio was not.

Pirate radio was effectively extinguished in the United Nations Convention on the Law of the Sea ("UNCLOS"). Article 109 gives states, even those who are not the flag states of a broadcasting vessel, power to arrest "any person or ship engaged in unauthorized broadcasting and seize the broadcasting apparatus."[59]

Pirate radio represents an inchoate, primitive digital trade zone. Seeking to circumvent impediments to the flow of transmitted information, individuals took to the seas. In international waters, these pirate broadcasters were able to successfully carve out space and challenge state-owned radio corporations, much in the same way digital trade zones seek to challenge the protectionist impulses of data localization and cross-border data flow restrictions, but this time with state approval.

2. The Legal Status of Oceanic Data Centers

Pirate radio offers an instructive case study about the potential, as well as the limits, of using the ocean as a means of bypassing territorial laws limiting the flow of information. However, to understand the theory that gives purpose to digital trade zones, the pirate radio analogy must be improved by considering the effect of putting servers on the seas. Can territorial restrictions on the flow of information be circumvented by placing the data on a vessel in the ocean?

For a time, Google pursued barge-based server farms that would deliver computing power throughout the world. In 2009, Google was granted a patent for a "water-based data center."[60] Using the ocean to power and cool a data center could potentially mean operating the facility much more cheaply at sea than on land. While there are doubts about the technological feasibility of such server ships, it may nonetheless be possible for a data center to maintain a degree of independence from national Internet restrictions by remaining at sea.[61]

---

59 United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]. At present, the United States has signed but not ratified UNCLOS and treats parts of the agreement as customary international law.

60 U.S. Patent No. 7,525,207 (filed Feb. 26, 2007) (issued Apr. 28, 2009).

61 *See* Tim Worstall, *Google's Offshore Data Centres Won't Be Out of the NSA's Reach, Nor the US Government's*, FORBES (Oct. 27, 2013, 9:25 AM), https://www.forbes.com/sites/timworstall/2013/10/27/googles-offshore-data-centres-wont-be-out-of-the-nsas-reach-nor-the-us-governments/#3e87c3787536 [http://perma.cc/6GGG-25VH].

Such was the case when the Swedish website, Pirate Bay, attempted to purchase an old British naval fort located outside the country's territorial waters in order to avoid law enforcement attempts to shut down the website.[62] While this attempted acquisition was for nefarious purposes, it underscores the interest in, and potential of, efforts to find places where digital restrictions do not apply. The fort, known as Sealand, had been previously used as a pirate radio base and claims a modicum of sovereignty.[63] Referred to as "a near-perfect embodiment of a data haven," Sealand has already tested its independence in cyberspace by hosting HavenCo, a provider of online gambling services.[64]

Building upon the lessons learned by pirate broadcasters and Sealanders alike, floating data centers would have to adhere to two important requirements at minimum. These vessels would have to remain on the high seas and would need to fly the flag of some nation.

UNCLOS applies several degrees of territoriality to the ocean.[65] Of these several degrees, only the final—the high seas—offers sufficient freedom from the prescriptive and enforcement jurisdiction of national governments to be of use in the intellectual development of digital trade zones. The high seas begin where a country's exclusive economic zone ends; 200 miles from the shore.[66] On the high seas, a state that is not the flag state of the vessel in question can exercise jurisdiction over a ship in international waters only in very limited circumstances such as if the ship is engaged in piracy or poses a specific threat to national security.[67] One would hope that operating a cloud computing service at an offshore data center would not fall into

---

62 *See* Jan Libbenga, *The Pirate Bay plans to buy Sealand*, THE REGISTER (Jan. 12, 2007, 2:44 PM), https://www.theregister.co.uk/2007/01/12/pirate_bay_buys_island/ [http://perma.cc/LHZ8-W3DY].

63 *See* Kevin Fayle, *Sealand Ho! Music Pirates, Data Havens, and the Future of International Copyright Law*, 28 HASTINGS INT'L & COMP. L. REV. 247, 261 (2005). Since it lacks the permanent population and capacity to pursue diplomatic relations, Sealand is unable to fully achieve sovereign recognition. *Id.* However, Sealand has been acknowledged to have a degree of sovereignty. *Id.* An English court found that Great Britain did not have jurisdiction over Sealand, and in 1978, the residents of Sealand lost the fort to German and Dutch nationals before they were able to recapture the fort in an air assault. *Id.* The Dutch and German invaders were then held as prisoners of war. *Id.*; *see also* Andrew H. E. Lyon, *The Principality of Sealand, and Its Case for Sovereign Recognition*, 29 EMORY INT'L L. REV. 637, 642–43 (2015).

64 Fayle, *supra* note 63, at 262.

65 The UN Convention on the Law of the Sea specifies these zones as internal waters, territorial seas, contiguous zones, exclusive economic zones, the continental shelf, and the high seas. Swanson, *supra* note 5, at 727–38.

66 UNCLOS, *supra* note 59, at 40.

67 *See id.* at 53–54.

these categories, though countries such as China, which have highly restrictive Internet regimes, may argue otherwise.

While the high seas offer a forum free from territorial data protectionism, a floating data center would also need, just like the pirate radio broadcasters of yore, to identify with a flag state in order to be protected against unwanted boarding and seizure. International law is explicit that a ship not flying the flag of a country is considered to be operating beyond the law.[68] The flag state, to the contrary, enjoys exclusive jurisdiction over the vessel flying its flag, thus "[h]aving a nationality actually protects the ship from other states' jurisdiction and lets the flag state exercise diplomatic protection over the vessel."[69]

Therefore, the operator of an oceangoing data center would want to select a flag state under which to operate the vessel. Options are not just limited to the United States or a company's nation of incorporation, but also a host of nations offering their flags for sale. Countries offering flags of convenience include Panama, Liberia, the Bahamas, and Bermuda.[70] Organizations usually select flags of convenience because of the light-regulatory touch and low taxes found in these nations.[71] However, in order to access markets with greater Internet regulatory schemes, especially when it comes to privacy, the operators of a floating data center may wish to choose a country that mimics the data protection regime of the jurisdiction within which they hope to conduct business. As such, operators of floating data centers may wish to affiliate with EU member states or Canada.

3. Applicability to Digital Trade Zones

The hypothetical treatment of data on the high seas offers two instructive lessons for digital trade zones. First, in order to be successful, a digital trade zone should attempt to mimic the legal conditions found on the high seas as much as possible. The digital trade zone should be a space free from territorial regulation on the flow of data; the digital trade zone should serve as a neutral zone separate and apart from domestic data restrictions. Just as it is for other special jurisdictions, extraterritoriality is important, and given the difficultly of operating data centers out in the ocean, replicating those legal conditions on land is core to the digital trade zones project. Second, digital trade zones still must be located somewhere in

68 *See* Sean Hickman, *Flagging Options for Seasteading Projects*, THE SEASTEADING INSTITUTE 3 (Mar. 2012).

69 Swanson, *supra* note 5, at 735–36.

70 Hickman, *supra* note 68, at 8.

71 *Id.* at 3.

order to benefit from a broader rule of law. This is similar to how a floating data center would need to select a flag state to avoid the predations attendant to being a stateless vessel on the high seas. Just as some flag states are more convenient for different operations, the United States likely offers the best conditions for digital trade zones, as it possesses a history of well-regarded privacy protection, a vibrant Internet industry, a strong rule of law, and a history of operating special jurisdictions. The advantages conferred on the first mover in this field would also be substantial, and policy makers may wish to work towards capturing these benefits.

B. U.S. Foreign Trade Zones

While the high seas offer an analogous way to think about the legal status of digital trade zones, FTZs in the United States offer direct insight into the mechanics of their digital trade counterparts. Created by the U.S. Congress in 1934, FTZs permit the occupants of the zone to defer customs duties and excise taxes on goods brought into the zone.[72] FTZs have proven to be successful special jurisdictions in the United States and as such offer a template from which to model their digital cousins.

1. The Purpose of Foreign Trade Zones

The purpose of FTZs is to prove an incentive for siting certain manufacturing functions within the United States. FTZs promote "importation for the purpose of conditioning or combining foreign goods with domestic products prior to exporting the finished products to foreign markets, rather than retaining them for domestic consumption."[73] At present, most activity in FTZs is manufacturing. Since their creation, the number of FTZs has proliferated. Before 1970, there were only ten cities with zones.[74] Today, there are over 200 approved zones.[75] Domestic inputs into zones account for fifty-eight percent of inputs while forty-two percent of inputs come from foreign sources.[76]

---

72 19 U.S.C. § 81c(a) (2012).

73 Barbara M. Sheppard, *Foreign Trade Zones – International Business Incentives*, 7 GA. J. INT'L. & COMP. L. 669, 670 (1977).

74 *See* John J. DaPonte, Jr., *The Foreign Trade Zones Act: Keeping Up with the Changing Times*, BUS. AM., Dec. 1997, at 22.

75 *See US Foreign Trade Zones*, EXPORT.GOV (Oct. 20, 2016), https://www.export.gov/article?id=US-Foreign-Trade-Zones [http://perma.cc/MR9K-8G4Z].

76 MARY JANE BOLLE & BROCK R. WILLIAMS, CONG. RES. SERV., R42686, U.S. FOREIGN-TRADE ZONES: BACKGROUND AND ISSUES FOR CONGRESS 7 (2013).

2. The Structure of Foreign Trade Zones

The most unique factor of FTZs is that they exist outside of U.S customs territory.[77] This allows FTZs to offer duty deferral on goods entering the zones. Customs duties are only paid when the imported goods are actually transported into U.S. customs territory.[78] In this way, FTZs represent more of a "procedure" than an actual physical demarcated place.[79] While all the zones are exempt from the same customs procedures, the zones are hardly homogenous, ranging from large, sprawling facilities to single warehouses.[80]

Applications for FTZs are reviewed by the Foreign Trade Zones Board. Located within the U.S. Department of Commerce, the Board is made up of the Secretary of Commerce and the Secretary of the Treasury.[81] The Board has an Executive Secretary to lead the daily operations.[82] The Board examines and, where appropriate, approves applications for new FTZ designations and then grants the designation to local governments or non-profit corporations, which then create and maintain the zone as a public utility.[83] Customs and Border Protection oversees all activities and collects all revenues from FTZs.[84]

3. Foreign Trade Zones Meet Digital Trade Zones

FTZs offer an established model for digital trade zones. Proposed digital trade zones in the United States would be established via federal legislation, and organizations would petition a Digital Trade Zones Board—perhaps also including the Secretary of Commerce and the Secretary of the Treasury as leaders—for inclusion in the program. Digital trade zones would be areas where instead of deferring duty collection, the United States would forbear from various Internet and privacy-related jurisdictions providing participating organizations the ability to self-regulate in ways that would satisfy the requirements of international data markets. Thus, digital trade zones would, similar to their foreign trade progenitors, be procedures rather than standard physical locations. Digital trade zones could be permitted to take a variety of forms and sizes; from the

---

77 *See* Tom W. Bell, *Special Economic Zones in the United States: From Colonial Charters, to Foreign-Trade Zones, Toward USSEZs*, 64 BUFF. L. REV. 959, 982 (2016).

78 BOLLE & WILLIAMS, *supra* note 76, at 11.

79 DaPonte, *supra* note 74, at 206.

80 Sheppard, *supra* note 73, at 670.

81 BOLLE & WILLIAMS, *supra* note 76, at 13.

82 *See* NAT'L ASS'N OF FOREIGN TRADE ZONES, THE U.S. FOREIGN TRADE ZONES PROGRAM – PROMOTING TRADE, JOB CREATION & ECONOMIC DEVELOPMENT 5 (2013).

83 *Id.*

84 *See id.*

largest of data centers to the most unusual of Internet communication arrangements.

III. DIGITAL TRADE ZONES IN PRACTICE

While there may be other applications of digital trade zones, and their enacting legislation should anticipate and encourage alternative uses, this article contemplates two practical uses. These two applications consider digital trade zones as experiments and digital trade zones as waystations. Both types of zones would adhere to the general procedures and structures in Part II. By permitting a country, in this analysis the United States, to forbear from jurisdiction over a defined area for the purposes of establishing law governing the Internet or other data uses unique to the zone, both experimental and transitory zones would be able to bypass restrictions on cross-border data flows and data localization requirements.

A. Digital Trade Zones as Experiments

Digital trade zones could also be used to detour around restrictions on cross-border data flows. This could be done by creating zones where companies could participate in different experimental arrangements designed to safeguard consumer privacy and work towards developing more beneficial arrangements for the transfer of data across borders.

Digital trade zones as experimental areas are perhaps most applicable to the relationship between the United States and the EU. In 2012, U.S. digital exports to the EU were worth $140.6 billion, representing seventy-two percent of all services exports to the EU.[85] Total U.S.–EU trade in goods and services totaled $1 trillion, and U.S. foreign direct investment in the EU amounted to $2.4 trillion—fifty-six percent of total U.S. direct investment worldwide.[86] There are several ways in which the flow of data across the Atlantic creates such exceptional value. For instance, many businesses in Europe sell products to and engage customers in the United States, European firms receive investment advice from U.S. consultancies, and companies share data internally from their international subsidiaries.[87] This is similar to how Boeing tracks engine operating data throughout

---

85 Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* 12 (Brookings Inst. Glob. Econ. & Dev., Working Paper No. 79, 2014).

86 *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RES. SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 4 (2016).

87 *See* Meltzer, *supra* note 85, at 8.

the world and shares it through its company and with commercial airlines.

1. Attempts to Preserve U.S.–EU Cross-Border Data Flows

Despite the incredible amount of data driven commerce between the United States and the EU, the EU's exceptionally rigorous data privacy requirements has been a thorn in the side of U.S.–EU trade relations when it comes to cross-border data flows. In October 1995, the EU adopted the Data Protection Directive ("DPD") to create a unified, comprehensive framework for data protection.[88] The DPD mandates that data on EU citizens can only leave the EU (and DPD's protections) if the destination jurisdiction has a sufficient data protection regime.[89] The EU assesses how adequate foreign data protections are by reviewing the circumstances governing the transfer of data.[90]

This initially posed problems for the United States, which lacks the same kind of comprehensive data protection law. Consumer privacy protection laws in the United States are "industry specific and vary by sector, with different laws governing the collection and disclosure of financial data, health-related data, student information, and motor vehicle records."[91] Some commentators have noted that, while less comprehensive on the whole, the alleged patchwork protections found in the United States form a much more nimble and flexible response to consumer privacy than the European approach, a view shared by the Department of Commerce, which maintains that "[t]he sum of the parts of U.S. privacy protection is equal to or greater than the single whole of Europe."[92]

Despite these reassurances, and in order to maintain transatlantic data flows, the U.S. and the EU agreed to the Safe Harbor Agreement in 2000.[93] The Safe Harbor Agreement was the result of negotiations between both sides in order to find an

---

88 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

89 WEISS & ARCHICK, *supra* note 86, at 2.

90 *Id.* The EU also focuses on "the nature of the data, the purpose and direction of the proposed processing operations, the countries of origin, and the final destination of the data, and that country's laws, rules, and security measures." *Id.*; *see also* Directive 95/46/EC, *supra* note 88, at arts. 25–26.

91 WEISS & ARCHICK, *supra* note 86, at 3.

92 Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

93 *See* U.S. DEP'T OF COM., U.S.-EU SAFE HARBOR FRAMEWORK; A GUIDE TO SELF-CERTIFICATION 3 (2009).

arrangement that satisfied the "adequate level of protection" for data mandated by the DPD.[94] At its peak, about 4500 U.S. companies participated in the framework established by the Safe Harbor Agreement. Participation was open to any U.S. organization that was regulated by the Federal Trade Commission and, separately, airlines, even though they are regulated by the Department of Transportation. This restriction did limit the Safe Harbor Agreement to these regulated industries and notably, it did not include U.S. financial or telecommunications companies.[95]

The serenity found under the Safe Harbor Agreement was dashed when in October 2015, the European Court of Justice struck down Safe Harbor Agreement as insufficient under the DPD.[96] First, the court found that a European Commission finding that a foreign country—the United States—had sufficient privacy protections does not supersede and reduce the powers of EU authorities to assess data privacy protections.[97] The European Court of Justice also determined that because the European Commission did not investigate "the domestic laws or international commitment of a third country prior to making a determination on the adequacy of their data privacy protection," the Commission decision adopting the Safe Harbor Agreement was invalid.[98]

The bombshell decision was followed by the U.S. and the EU scrambling to find a new mechanism to protect privacy and then facilitate transatlantic movement of data as quickly as possible. In February 2016, the U.S. and the EU announced a replacement to the Safe Harbor Agreement: the Privacy Shield Framework.[99] The Privacy Shield Framework is meant to be a more robust version of the Safe Harbor Agreement. The Privacy Shield Framework is characterized by several changes, including stronger enforcement measures administered by the Department of Commerce and the Federal Trade Commission, improved redress for citizens who believe their data has been compromised, and greater commitments by participating U.S. companies, such as more detailed notice obligations, prescriptive access rights,

---

94 WEISS & ARCHICK, *supra* note 86, at 5.

95 *Id.* at 6.

96 *See* Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's* Schrems *Decision and What it Means for Transatlantic Relations*, SETON HALL J. DIPL. & INT'L REL. (forthcoming) (manuscript at 2–3).

97 *See* Mira Burri & Rahel Schar, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479, 486 (2016).

98 WEISS & ARCHICK, *supra* note 86, at 7.

99 *Id.* at 9.

and data retention limits.[100] Currently, 2500 organizations participate in the Privacy Shield Framework.[101]

In October 2017, the European Commission released a report announcing that the Privacy Shield Framework continues to provide sufficient protection under EU law.[102] However, this positive development should not obfuscate concerns that the Privacy Shield Framework, like the Safe Harbor Agreement before it, will be eternal. Even at its inception, the EU recognized "shortcomings" with the framework,[103] and with the DPD's forthcoming replacement by the General Data Privacy Directive ("GDPD") in 2018, questions may once again arise about the survival of data flow arrangements between the U.S. and the EU.[104] The GDPD has a somewhat more expansive scope than the DPD—particularly when it comes to territoriality, data-subject rights, and personal data processing, to name a few—which may mean the currently accepted Privacy Shield Framework protections will be suddenly out of date when the GDPD comes into force next year.[105] And even without this worry, litigation relating to another tool available for U.S. business compliance with the DPD—standard contractual clauses—has been unceasing since the invalidation of the Safe Harbor Agreement. Given that this litigation, centered on the acceptability and protective adequacy of the standard contractual clauses will continue regardless of the GDPD issue, the Privacy Shield Framework will continue to face active threats and challenges for the foreseeable future.[106]

---

100 The Judicial Redress Act, 5 U.S.C. § 552a (2015), which was signed into law by President Obama in February 2016, improved transatlantic trust regarding data flows. Broadly, the Act aims to include citizens of foreign countries or organizations (like the EU), which the United States has an agreement with to promote privacy protections. Similar to the promise offered by digital trade zones, passage of the Judicial Redress Act was hailed as a turning point in U.S.–EU data relations. *See* WEISS & ARCHICK, *supra* note 86, at 10, 13.

101 *See* Press Release, U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Welcomes Release of European Commission Report on EU-U.S. Privacy Shield (Oct. 18, 2017), https://www.commerce.gov/news/press-releases/2017/10/us-secretary-commerce-wilbur-ross-welcomes-release-european-commissions [http://perma.cc/Z7NZ-PLFB].

102 *Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S. Privacy Shield*, at 2, COM (2017), 611 final (Oct. 18, 2017).

103 WEISS & ARCHICK, *supra* note 86, at 11.

104 W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 222 (2017).

105 *Id.* at 222, 225.

106 *See* Catherine Muyl, *EU Updates on Schrems II and the Privacy Shield*, SECURITY, PRIVACY AND THE LAW (Oct. 2, 2017), http://www.securityprivacyandthelaw.com/2017/10/eu-updates-on-schrems-ii-and-the-privacy-shield/ [http://perma.cc/LCU6-BC4L]. There is also litigation in France challenging the Privacy Shield Framework. *See* Les Exégètes

2. Digital Trade Zones as Experiments

The tense history, and continued fragility, of U.S.–EU data privacy agreements offers an opportunity for proposed digital trade zones to shine. While digital trade zones could be viewed as experimental zones in a variety of ways, this article focuses on one prominent way in which digital trade zones could be valuable areas of trade innovation. Currently, any data privacy arrangement between the U.S. and the EU has to be negotiated in great detail and would apply to the entirety of both jurisdictions. The stakes are also exceptionally high; a single agreement must be, at least at the time of its adoption, near perfect, or face invalidation.[107] And even where an agreement is successful at fending off legal challenges, these challenges still undermine the agreement's stability until resolution, potentially forestalling quick adoption of the framework.

Digital trade zones could be designed to permit organizations to experiment with different data privacy arrangements. The United States could forbear from standard privacy laws in specified zones. The governing principle in the zones would be a hybrid privacy regime: U.S. law contextualized by EU requirements. This would allow several places to experiment with data privacy arrangements. There are three benefits to using digital trade zones to experiment with privacy arrangements in order to circumvent impediments to the international flow of data. One way this might function would be if parties, such as the U.S. and EU, negotiated a variety of data privacy arrangements and then specified specific zones in which the arrangements would apply. Much like FTZs, these digital trade zones would be limited to the geographic area around single companies or server complexes. Interested organizations would be able to apply to the Department of Commerce to be the guinea pigs for different privacy arrangements. For participating companies, the benefits would be clear: access to European markets that would otherwise be beyond reach. Just as companies apply to participate in the FTZ program because it gives them more efficient and less costly access to difficult to source inputs, companies handling big data would be motivated to participate in a digital trade zone by the inverse: access to difficult to reach overseas markets.

Amatuers, *Privacy Shield*, LES EXÉGÈTES AMATEURS (2016), https://exegetes.eu.org/dossiers/privacyshield/index.html [http://perma.cc/W324-QP7H].

107 *See* Graham Greenleaf, *International Data Privacy Agreements after the GDPR and* Schrems, 139 PRIVACY L. & BUS. INT'L REP. 6, 8 (noting that a less than perfect Privacy Shield Framework invites litigation designed to destroy the agreement).

There are three benefits to using digital trade zones to experiment with privacy arrangements in order to circumvent impediments to the international flow of data.

First, experimental digital trade zones would reduce the currently high stakes of every data protection agreement negotiation. Since the Safe Harbor Agreement and the Privacy Shield Framework apply to the entire United States, companies do not have a choice of participating in some other arrangement. This means that the stakes are exceptionally high during a negotiation over a new arrangement or when considering updating an arrangement. If there were numerous arrangements in place, any of which could be applied for and to specific local jurisdictions, the stakes would be lower for each individual agreement. The U.S. and the EU might be more willing to experiment with different types of arrangements, perhaps even limiting the initial number of organizations which could participate during pilot programs, and would be more likely to approach agreements in an iterative process, adopting lessons learned from test agreements and adjusting to developments in U.S. and EU privacy law.

Relatedly, these zones could act as fail safes in the event certain regimes were invalidated. With lower stakes and more experimental agreements spread over different jurisdictions, the numerousness of digital trade zones would guarantee that if a single arrangement was invalidated by a U.S. or EU court, other agreements would still be in place. Indeed, if digital trade zones are permitted to "stack" agreements, conforming to the most stringent aspects of every agreement, even where one of the jurisdiction's agreements is invalidated, the jurisdiction is still able to function under other agreements. Consider the creative commons license system. Just as licensors are able to select different types of licenses that give them the desired level of attribution, commercial reuse, and derivativeness, organizations operating in a digital trade zone would be able to select the data privacy and legal arrangements that best suit their organization and the market access it hopes to achieve.[108] Modularity means longevity for transatlantic data agreements. The dispersed nature of the zones' agreement frameworks would no longer necessitate hurried negotiation for global replacements where a prior regime is withdrawn. Even without an agreement stack, there would already be other types of model agreements in place

108 *See About the Licenses*, CREATIVE COMMONS, https://creativecommons.org/licenses/ [http://perma.cc/87JF-EMJP] (last visited Nov. 10, 2017).

that the parties could draw upon to replace a failed or invalidated experimental arrangement.

Third, digital trade zones would inject market forces into a currently bulky, and non-market process. By marketizing data privacy arrangements, digital trade zones would be more responsive to consumers while giving greater choice to policy makers. Right now, consumers can only choose to do U.S.–EU business with companies complying with the Privacy Shield Framework. Consumers are not able to choose amongst companies that might protect their privacy even better under an experimental arrangement, and companies are not efficiently incentivized to offer greater or lesser, but more targeted, protections. Given the privacy concerns that form the basis of many people's desire to remain offline or minimize their online presence, this consumer choice is critical.[109] Businesses will also be interested in such a proposal because it offers a chance to improve their reputations vis a vis consumers' privacy desires, likely in a certification-style manner.[110] In this way digital trade zones can help organizations seeking to operate in Europe, while also giving consumers a voice in what types of data privacy arrangements they prefer.

B. Digital Trade Zones as Waystations

While data localization policies are difficult to surmount because the policies are designed to prohibit the international movement of data entirely, digital trade zones can still offer an answer to data localization problems when used as waystations. These types of digital trade zones would exist to hold data in transition and would be aimed at addressing localization initiatives, such as those found in Canada.

1. Data Localization in Canada

As mentioned previously, the Canadian provinces of British Columbia and Nova Scotia both have serious localization requirements for public data. Both provinces require that personal information held by a public organization, such as a university, hospital, school, or public department, be held in Canada.[111] Moreover, these public entities are prohibited from using U.S.–based services if there is the chance the data

---

109 *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards*, 25 YALE J. INT'L. L. 1, 37 (2000).

110 *See id.* at 35–36.

111 NATIONAL TRADE ESTIMATE REPORT, *supra* note 9, at 72.

covered by the laws could be "stored in or accessed from the United States."[112]

British Columbia's localization requirement comes from the Freedom of Information and Protection of Privacy Act ("FIPPA"), an act governing the protection of public information.[113] Section 30.1 of FIPPA mandates that "a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada."[114] There are three exceptions: (1) if the individual consents to their information being stored in or accessed from another jurisdiction; (2) if the data is stored in or accessed from another jurisdiction "for the purpose of disclosure allowed under this Act"; and (3) if the information was disclosed in order make a payment or resolve an issue surrounding a payment to "the government of British Columbia or a public body."[115] "Under FIPPA, a 'record' includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means."[116]

In Nova Scotia, the Personal Information International Disclosure Protection Act ("PIIDPA") forms the core of the province's localization requirement, since PIIDPA focuses on the unauthorized disclosure of information specifically beyond Canada and makes it illegal for information to be stored in, or accessed from, jurisdictions outside of Canada. There are exceptions, instances of which are detailed in a report issued by the government of Nova Scotia.[117] For example, energy officials in Nova Scotia permitted twenty-four staffers to use their government email while traveling abroad to places like the United States, Norway, and China.[118] The explanation provided for this exemption from PIIDPA is innocuous and standard: "staff may be required to monitor their email and voicemail for business continuity purposes."[119] Almost all the other entries in

---

112 *Id.*

113 OFFICE OF THE INFO. & PRIVACY COMMISSIONER FOR B.C., GUIDE TO ACCESS AND PRIVACY PROTECTION UNDER FIPPA 3 (Oct. 2015) [hereinafter FIPPA GUIDE].

114 Freedom of Information and Protection of Privacy Act, 165 R.S.B.C. § 30.1 (1996).

115 165 R.S.B.C. §§ 30.1, 33.1(1).

116 FIPPA GUIDE, *supra* note 113, at 7.

117 *See* Ian Wallace, *Privacy: what laws apply in Atlantic Canada?*, STEWART MCKELVEY, http://www.smss.com/abcnewsletter/AEC/2014_Summer/A1.html [http://perma.cc/ML8K-MGG8] (last visited Nov. 9, 2017).

118 N.S. DEP'T OF JUSTICE, PERSONAL INFORMATION INTERNATIONAL DISCLOSURE PROTECTION ACT: 2014 ANNUAL REPORT 12 (July 2015).

119 *Id.*

the report detail similar situations of staff bringing laptops and phones outside of Canada on official or personal trips.[120]

2. Digital Trade Zones as Waystations

In this conception of digital trade zones, waystations are locations where data is transitory. Information will flow through the zone but not be accessed there. Data may be stored there as long as necessary until it is repatriated back to the jurisdiction with the localization requirement. The waystation model would work by creating space where organizations would be permitted to add additional privacy and cybersecurity protections to meet the protection thresholds necessary to handle the data coming out of a localized jurisdiction. However, the waystation would not be physically located in that jurisdiction and may even be situated in a foreign country.

In the case of Canada, the United States could create digital trade zones that exist as spaces outside of U.S. jurisdiction for the purposes of privacy laws, similar to how FTZs exist "outside" the U.S. for the purposes of duty collection on initial imports. In these zones, organizations would be able to build and operate servers to handle public data from British Columbia or Nova Scotia. Since the zones would be outside the jurisdiction of the United States for the purposes of privacy law, the zones would be able to be sealed from intrusion by host jurisdiction surveillance agencies. Title II of the Electronic Communications Privacy Act, also known as the Stored Communications Act ("SCA"), would not apply. Law enforcement would not be able to use a warrant issued under the SCA to access data stored outside the United States.[121] The individual whose data is being stored remains inviolate because the organization storing the individual's information is merely a "caretaker."[122] The right to the data remains with the individual, in this case in Canada, and the server itself remains in the digital trade zone thus technically outside the borders of the United States. With ensured privacy protection from the United States, organizations operating in the zone would still need to certify to the relevant province that they had met the necessary privacy and cyber protection to handle the province's public data. Furthermore, the data would not be able to be accessed in these zones. It would simply be stored there

120 *See generally id.*

121 *In re* Matter of Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 201 (2d. Cir. 2016).

122 Andrew J. Pecoraro, *Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act*, 51 CREIGHTON L. REV. 75, 95 (2017).

until the data was requested back in Canada, at which point it would be transmitted back to the originating province.

The benefit of the waystation model is that it may be easier, more cost-effective, and less burdensome to construct, maintain, and operate a collection of servers in jurisdictions that are not subject to the localization requirement. In the U.S.–Canada example, it may be easier to build and operate servers in the United States, or another country, than it is in Nova Scotia.

For example, in Toronto it costs $1580 per square meter to build a high-tech factory, the closest type of structure to a data center mentioned in a recent report on comparative construction costs.[123] Presumably it may be even more expensive to do such construction in places outside of Canada's largest city, such as Nova Scotia. While all U.S. cities in the report were listed as having higher construction costs than Toronto, numerous other cities did have lower costs, potentially making them ripe candidates for using digital trade zones as waystations. Some notable cities where construction costs are lower than Toronto include Seoul, Singapore, and Brisbane.[124] However, data centers are different from generic high-tech factories, and so these general numbers might not encompass the exact cost of construction for such a specialized facility. In the United States, it costs on average $43 million to build a data center.[125] Costs are even higher in Brazil ($60.9 million) and Chile ($51.2 million).[126] Directly comparable data was not available for Canada. However, data center construction costs in Brazil and Chile were higher than the United States, even though construction of high-tech factories in both of those countries were considerably cheaper than such construction in the United States.[127] This suggests that there is something intrinsic about the construction of *data centers* that makes such construction cheaper in the United States than abroad. To the extent that such construction is cheaper in the United States rather than British Columbia or Nova Scotia, digital trade zones can serve as a way to promote the domestic construction industry, while also

123 TURNER & TOWNSEND, INTERNATIONAL CONSTRUCTION MARKET SURVEY 2016, at 26 (2016) (comparing construction costs on numerous global cities—Toronto was the only Canadian city included and U.S. cities covered by the report were New York City, Houston, San Francisco, and Seattle).

124 *See id.* at 13.

125 Chander & Le, *supra* note 17, at 36.

126 *Id.*

127 *See* TURNER & TOWNSEND, *supra* note 123, at 24, 28, 78. Construction costs for a high-tech factory was $1300 in Brazil and $3500 in Chile. *Id.* at 24, 28. Comparatively, according to the report, the city with the lowest cost of construction of a high-tech factory was Houston at $4272. *Id.* at 78.

bringing U.S. organizations in closer proximity to Canadian information markets.

Construction is not the only driving cost of data centers. Data centers are exceptionally energy intensive,[128] with energy costs accounting for three-quarters of a data center's cost of operation.[129] In Canada, data centers use approximately one percent of the entirety of the country's energy consumption.[130] And, since Canada actually has more expensive electricity than the United States, small businesses pay, on average, eight percent more and industrial businesses pay thirty percent more per kilowatt hour than their southern neighbors.[131] Cheap electricity in the United States may be a reason why businesses would want to site their data centers in the United States rather than in Canada. While Canada has 164 data centers, the costs of operating those centers can be reduced by siting those centers in the U.S., or by contracting with U.S.–based centers to handle provincial public information.[132] Waystation digital trade zones would help enable this cross-border data storing to be realized.

C. Digital Trade Zones and Intellectual Property Rights

The practical proposals of digital trade zones as experiments and waystations only addresses two of the three main types of digital trade barriers. Digital trade zones could also help advance national interests in protecting intellectual property. While the potential for digital trade zones to seriously mitigate intellectual property rights infringement is reserved for future works, it is worthwhile to mention one particular way that digital trade zones guard against intellectual property rights infringement, even only examining the simple applications presented in the present work.

The Trade Related Intellectual Property ("TRIPS") Agreement, which was created along with the World Trade Organization ("WTO") at the Uruguay Round, requires participating states to establish minimum intellectual property rights standards.[133] However, some view the TRIPS Agreement

---

128 Swanson, *supra* note 5, at 715.

129 Chander & Le, *supra* note 17, at 37.

130 *Data Centres*, NAT. RESOURCES CAN., https://www.nrcan.gc.ca/energy/products/categories/data-centres/13741 [http://perma.cc/4HZKLFQA] (last modified Jan. 19, 2018).

131 *See* Gerry Angevine & Kenneth P. Green, *Paying More for Power: Electricity Costs in the US and Canada*, FRASER INST. iii (May 2014), https://www.fraserinstitute.org/sites/default/files/paying-more-for-power-rev.pdf [http://perma.cc/M59X-8EJ4].

132 *Colocation Canada*, DATA CTR. MAP, http://www.datacentermap.com/canada/ [http://perma.cc/22JL-RGUS] (last visited Nov. 7, 2017).

133 *See* Rachel Brewster, *The Surprising Benefits to Developing Countries of Linking International Trade and Intellectual Property*, 12 CHI. J. INT'L L. 1, 2 (2011).

minimum standards as insufficient. For example, the TRIPS Agreement requires that countries make available "enforcement procedures" against intellectual property rights violations.[134] This language stops short of any "affirmative obligation to stop acts of infringement."[135] This suggests that digital trade zones may be able to fill gaps in the TRIPS Agreement by denying violators an opportunity to purloin intellectual property.

One example from a country mentioned in this article is Canada. Canada remains on the U.S. Trade Representative's Special 301 Watch List for a variety of reasons.[136] Canada does not give customs officials authority to "detain, seize, and destroy pirated and counterfeit goods."[137] Presumably, this limitation could be extended to goods in digital form, although there remains a debate about the proper classification of e-products under the WTO.[138] As digitally neutral territory that retain (or even improve upon) the intellectual property rights regimes of their host country, digital trade zones offer safe havens for digital content to be stored without fear of piracy. While the data may be subject to piracy if it moves across borders and outside the digital trade zone, digital trade zones can offer intellectual property protection for the data they hold.

CONCLUSION

In a world with non-tariff restrictions on trade, there is a truism that speaks to those who desire to negotiate around these restrictions: to play the game, participants must give something up. That is, to engage in commerce across borders, participants—whether they be countries or organizations—must be prepared to find some compromise. In the context of digital trade zones this thinking also holds true. Countries seeking to expand their digital markets might forbear from some jurisdiction over their territory, internet laws, and surveillance authority in order to promote the creation of digital trade zones and the proliferation of e-commerce by domestic organizations. Countries seeking to protect their domestic technology sectors should also be

---

134 Agreement Trade-Related Aspects of Intellectual Property Rights art. 41, Apr. 15, 1994, 1869 U.N.T.S 299.

135 Brewster, *supra* note 133, at 22.

136 Special 301 Report, *supra* note 32, at 62.

137 *Id.*

138 *See* Sam Fleuter, *The Role of Digital Products under the WTO: A New Framework for GATT and GATS Classification*, 17 CHI. J. INT'L L. 153, 158–59 (2016). For the domestic version of the debate over the classification of digital goods, see *ClearCorrect Operating, LLC v. International Trade Commission*, 810 F.3d 1283, 1289–99 (Fed. Cir. 2015), finding that the International Trade Commission lacks authority to exclude patent infringing digital goods under Section 337 of the Tariff Act of 1930. *See also* Sapna Kumar, *Regulating Digital Trade*, 67 FLA. L. REV. 1909, 1924–25 (2015).

prepared to give up some of the artificial advantage created by protectionist policies. Privacy remains protected at the level required by the home jurisdiction and data-based commerce flows more easily in a trusted environment in the host jurisdiction.

This article has provided some initial thoughts to start a conversation on digital trade zones; many additional inquiries on this topic and opportunities for exploration yet exist. A further investigation of the ways in which digital trade zones could protect intellectual property rights, especially as data flows through jurisdictions that do not contain digital trade zones, is vital. It would also be worthwhile to consider what digital trade zones might look like in other, non-common law countries. This article proposed a particular conception of digital trade zones based off of international maritime law blended with the procedures of FTZs in the United States. Given the expansiveness of special jurisdictions throughout the world, what other types of special jurisdictions could serve as models to improve the usefulness of digital trade zones or tailor them to even more specific applications of situations? And is there a different base framework better suited to the general foundation of the digital trade zone?

While digital trade zones may never be deployed in the real world, the underlying principles which would motivate their consideration and adoption is worth noting. The forbearance of jurisdiction that would be required to occur in digital trade zones represents an inherently pro-commerce approach. Where governments can be persuaded to forbear from protectionist policies generally, and limit other impeding regulations in certain narrow cases or jurisdictions, private industry, organizations, and entrepreneurs can leverage this freedom to create value for the communities in which they are based.