William & Mary Business Law Review

Volume *10 (2018-2019)*
Issue 1

Article 7

November 2018

Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data

Victoria Conrad

DIGITAL GOLD: CYBERSECURITY REGULATIONS AND ESTABLISHING THE FREE TRADE OF BIG DATA

VICTORIA CONRAD*

ABSTRACT

Data is everywhere. With more than ten billion Internet-enabled devices worldwide, each day individuals create a flood of information that is transferred onto the Internet as big data. Businesses that have the resources to capture and utilize data can better understand their consumers, allowing for reinforcement of customer relationship management, improvements to the management of operational risk, and enhancement of overall firm performance. However, big data's advantages come with high costs. The cost of organization and storage coupled with the fact that no legal principle allows for any sort of property rights in big data creates a "digital divide" between data giants, like Facebook and Google, and smaller businesses. What's more, because each country sets different cybersecurity standards, start-up costs and expenses are cutting many businesses out of the digital market. This Note will first discuss the basics of big data and then argue that policymakers need to promote the free trade of data as a commodity with independent property rights. This Note will then discuss the obstacles to the free trade of data regarding privacy rights and the diversity of international cybersecurity regulations. Finally, this Note will propose the need for a multilateral convention on cybersecurity that will promote a centralized regulatory approach.

---

* JD Candidate William & Mary Law School, Class of 2019; BS Political Science, University of Maryland, College Park, Class of 2016. The author would like to thank the editorial board and staff of the *William & Mary Business Law Review* for their help throughout the editing process. She also would like to express gratitude to her parents, Chris and Joanne Conrad, for their continuing support throughout her entire education.

TABLE OF CONTENTS

INTRODUCTION

The world runs on oil, or at least it did.[1] The United States' development into the great industrial power of the twentieth century was built on the exploitation of oil.[2] However, "'black gold' is no longer the world's most valuable resource—it has been surpassed by data."[3] The five most valuable companies in the world, "Technologic Giants"—Apple, Amazon, Facebook, Microsoft, and Alphabet (Google)—have commodified data to take over their sectors.[4] Yet, these Giants are not the only companies benefitting from data usage.[5] Across industries, "companies are ramping up their attention" to big data.[6] "[B]illions of connected devices—smartphones, cars, tablets, household and industrial products, and business process machines—that together have the potential to transform how companies deliver innovation, create differentiated customer experiences, and optimize global operations."[7]

But as this new frontier opens for businesses, data's containment, regulation, and protection are falling behind.[8] "With more than [ten] billion [I]nternet-enabled devices worldwide … [the] increasing surface area leaves us vulnerable to attack."[9] Big data may be the next "gold rush," but it involves many costs, benefits, and externalities that have yet to be addressed.[10]

---

[1] MICHAEL MANDELBAUM, THE ROAD TO GLOBAL PROSPERITY 18 (Simon & Schuster, 1st ed. 2014).

[2] *Petroleum Resources*, SUNY SUFFOLK, http://www2.sunysuffolk.edu/westn/oil.html [https://perma.cc/7JGX-RELG].

[3] Ramona Pringle, *'Data is the New Oil': Your Personal Information is Now the World's Most Valuable Commodity*, CBC NEWS (Aug. 25, 2017, 5:00 AM), http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677 [https://perma.cc/QEZ2-ZY49].

[4] *Id.*

[5] *See id.*

[6] Paul Brody & Veena Pureswaran, *The Next Digital Gold Rush: How the Internet of Things Will Create Liquid Transparent Markets*, 43 STRATEGY & LEADERSHIP 36, 36 (2015).

[7] *Id.*

[8] Michael Mattioli, *Disclosing Big Data*, 99 MINN. L. REV. 535, 583 (2014).

[9] Kate Edgar, *Data is the New Global Commodity*, MEDIUM (July 29, 2016), https://medium.com/global-intersection/data-is-the-new-global-commodity-38b8d7e43ebf [https://perma.cc/6P6J-ZEU3].

[10] Brody & Pureswaran, *supra* note 6.

Part I of this Note will give a background on big data, the benefits it offers, as well as the barriers that prevent new companies from accessing large-scale data use. Because big data has created such an opportunity for economic advancements, Part II of this Note will argue that policymakers need to promote the free trade of data as a commodity with independent property rights. Part III will discuss the obstacles the free trade of data faces regarding privacy rights and international cybersecurity regulations. Finally, Part IV will propose the need for a multilateral convention to promote the international data exchange and create a more centralized system of cybersecurity.

I. BACKGROUND

"Big data is just what it sounds like ... massive amounts of information generated and gathered by modern technology."[11] Big data contains traditional scientific information, such as DNA evidence, genome mapping, chemical screening, climate data, and population analysis.[12] However, new analytical technology has transformed data collection, enabling researchers to gather less-traditional information.[13] Each day, individuals "generate an avalanche of [data] each day, in tweets and posts, in web browser histories and credit card purchases, in GPS-marked cellphone calls, in fitness trackers, and ATM transactions."[14] For the first time, scientists have the resources to capture and analyze a person's digital existence.[15]

Big data has become synonymous with business intelligence, analytics, and data mining.[16] With 2.5 quintillion bytes of data

---

[11] Alvin Powell, *Big Data, Massive Potential*, HARV. GAZETTE (Oct. 13, 2015), https://news.harvard.edu/gazette/story/2015/10/big-data-massive-potential/ [https://perma.cc/QJ6Q-BVJ6].

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition and Productivity*, MCKINSEY GLOB. INST. 1 (2011), https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf [https://perma.cc/3FWU-Z5DB].

[16] M. Moorthy et al., *An Analysis for Big Data and its Technologies*, 4 INT'L J. OF COMPUT. SCI. ENG'G & TECH. 412, 412 (2014).

created every day,[17] "[b]ig data presents concepts, methods, technologies, IT architectures and tools available to the exponentially increasing volumes of diverse information ... improv[ing] the inventiveness and competitiveness of enterprises."[18] Businesses able to harness big data have virtually shifted intelligence strategies "from reporting and decision support to prediction and next-move decision making."[19] The adoption of big data analytical tools and infrastructure includes the use of transaction history, social media, mobile devices, and automatic identification technologies to process and create a better understanding of the industry and its consumers.[20] Firms that can incorporate these strategies are able to better reinforce customer relationship management, improve the management of operational risk, and enhance operational efficiency and overall firm performance.[21] McKinsey Global Institute estimates that a retailer embracing big data can potentially increase its operating margin by more than sixty percent.[22] Furthermore, McKinsey estimates the potential annual consumer surplus from using services enabled by personal-location data can allow consumers to capture $600 billion in economic surplus.[23]

Data is now everywhere—in every sector, in every economy, in every organization and user of data—the public sector included.[24] Many believe that the use of big data in healthcare allows for personalization and the collection of real-time lifestyle data that tracks specific activities within specific areas.[25] For example, Google

---

[17] Ralph Jacobson, *2.5 Quintillion Bytes of Data Created Every Day. How Does CPG & Retail Manage It?*, IBM (Apr. 24, 2013), https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/ [https://perma.cc/45X8-83Q4].

[18] Moorthy et al., *supra* note 16.

[19] *Id.*

[20] Samuel Fosso Wamba et al., *Big Data Analytics and Firm Performance: Effects of Dynamic Capabilities*, 70 J. BUS. RES. 356, 356 (2017).

[21] *Id.* (citing Kiron D., *Organization Alignment is the Key to Big Data Success*, MIT SLOAN MGMT. REV. 54 (2013)).

[22] Manyika et al., *supra* note 15, at 2.

[23] *Id.* at vii.

[24] *Id.* at 2.

[25] David B. Nash, *Harnessing the Power of Big Data in Healthcare*, 7 AM. HEALTH & DRUG BENEFITS 69, 70 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4049118/pdf/ahdb-07-069.pdf [https://perma.cc/Z97P-AZMA].

employs an automated method for analyzing influenza-related web searches to track epidemics, which currently aids the work of the Center for Disease Control.[26] McKinsey estimates that, if U.S. health care could use big data to drive efficiency and quality, the potential value from the use of big data could be more than $300 billion every year.[27]

Although the private and public sectors have recognized the value big data can bring to the global economy, full-scale integration still presents obstacles.[28] The relative term "big data" describes "a situation where the high volume, velocity, and variety of data exceed[s] an organization's [preexisting] storage or comput[ing] capacity for accurate and timely decision making."[29] Researchers appropriately explain that the Internet is "like a data-driven Niagara Falls, surging with an endless, churning, unstoppable flood of bits and bytes," and it only keeps getting larger and faster.[30] CISCO forecasted that "global Internet traffic in 2021 will be equivalent to 127 times the volume of the entire global Internet in 2005."[31]

Data traffic is also not created in a uniform manner.[32] Each data source a business receives data from collects the information into a different form or type, all of which must be filtered through one infrastructure to be of any value.[33] "Trying to pinpoint and analyze a particular piece of information from the Web is like trying to pick out a specific drop of water as it rushes over the falls."[34]

---

[26] Elliot Naidus & Leo Anthony Celi, *Big Data in Healthcare: Are We Close to It?*, 28 REVISTA BRASILEIRA DE TERAPIA INTENSIVA 8, 9 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4828085/pdf/rbti-28-01-0008.pdf [https://perma.cc/2HPE-MYNB].

[27] Manyika et al., *supra* note 15, at 2.

[28] Moorthy et al., *supra* note 16.

[29] *Id.*

[30] David Hunt, *Big Data Challenges: Volume, Variety, Velocity & Veracity*, N.C. ST. U. RESULTS, 1, 2 (2014), https://research.ncsu.edu/results/2014/12/big-data-challenges-volume-variety-velocity-veracity/ [https://perma.cc/62H2-CXBG].

[31] *CISCO Visual Networking Index: Forecast and Methodology 2016–2021*, CISCO (2017), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html [https://perma.cc/R7GC-UCQA].

[32] *See* Hunt, *supra* note 30.

[33] *Id.* at 3.

[34] *Id.* at 2.

The technology requirements to gather, organize, and store vast amounts of data is just not available for businesses wishing to utilize big data.[35] "The reality is that traditional database approaches do not scale or write data fast enough to keep up with the speed of creation."[36] Additionally, data warehouses are effective at organizing data, but a high cost exists for the hardware to scale out as the volume grows.[37] It seems, in the case of big data, quantity does have its own quality.[38]

In the private sector, the abundance of data created a "digital divide" between the Technologic Giants and smaller companies.[39] The Giants maintain colossal infrastructures able to collect and organize data in massive quantities.[40] The information collected then allows the companies access to better information to improve their products, which then attracts more users and generates even more data.[41] The data divide has a monopolistic effect on each company's market.[42] For example, "Amazon now captures 46 [percent] of online shopping" in America,[43] while Google and Facebook "accounted for about 99 [percent] of the $2.9 billion" growth in digital advertising in 2016.[44]

Furthermore, the Technologic Giants' monopoly on data literally protects themselves.[45] Within the tech industry, competition

---

[35] John Bantleman, *The Big Cost of Big Data*, FORBES (Apr. 16, 2012, 1:21 AM), https://www.forbes.com/sites/ciocentral/2012/04/16/the-big-cost-of-big-data/#2728e8195a3b [https://perma.cc/JAY7-ZT7M].

[36] *Id.*

[37] *Id.*

[38] *The world's most valuable resource is no longer oil, but data*, ECONOMIST (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [https://perma.cc/HB4P-AXFG].

[39] Hwa-Jong Kim et al., *The Open Data Interface (ODI) Framework for Public Utilization of Big Data*, *in* DATA ANALYTICS 2012 94 (Sandjai Bhulai et al. eds., 2012) [https://perma.cc/Q8TC-UFLX].

[40] *The world's most valuable resource is no longer oil, but data*, *supra* note 38.

[41] Kim et al., *supra* note 39; *The world's most valuable resource is no longer oil, but data*, *supra* note 38.

[42] Kim et al., *supra* note 39.

[43] Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 712 (2017).

[44] Matthew Ingram, *How Google and Facebook Have Taken Over the Digital Ad Industry*, FORTUNE (Jan. 4, 2017), http://fortune.com/2017/01/04/google-facebook-ad-industry/ [https://perma.cc/73ZW-LESM].

[45] *The world's most valuable resource is no longer oil, but data*, *supra* note 38.

arises when incumbents are blindsided by an innovative startup or a technological shift.[46] However, the monopoly on data within the market allows for surveillance systems to span the entire economy.[47] The Giants can see when a new competitor enters the market, allowing them to copy it or acquire it through a "shoot-out acquisition" before the competitor becomes a threat.[48] By creating early warning systems and further enhancing the digital divide, the Technologic Giants can stifle competition.[49]

Firms wanting to access big data also face obstacles from the decentralized nature of cybersecurity laws.[50] "[D]ivergent regulatory approaches ... result in uneven levels of protection between jurisdictions."[51] Cross-border flows of data are then subjected to more legal control to prevent laws of more protective regimes from being circumvented and the privacy rights of companies eroded.[52] The World Trade Organization (WTO) acknowledges the important aspects of data defense and privacy protection.[53] Article XIV of the WTO's General Agreement on Trade in Services (GATS) permits trade restrictions that are necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[54]

If regulations on data go too far, these restrictions can hinder competition and innovation in the digital market.[55] Diversity in regulation requires firms to adjust their infrastructure to meet each nation's policies.[56] But without any harmonization of laws and regimes, the friction between international data exchanges can severely limit a business's ability to enter certain markets.[57]

---

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] U.N. Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 2 UNCTD /WEB/DTL/STICT/2016/1/iPub (2016).

[51] *Id.*

[52] U.N. Conference on Trade and Development, *supra* note 50.

[53] General Agreement on Trade in Services art. XIV(c)(ii), Apr. 15, 1994, 1869 U.N.T.S. 183 (1994).

[54] *Id.*

[55] U.N. Conference on Trade and Development, *supra* note 50, at 3.

[56] *See id.* at 50.

[57] *Id.* at 3.

II. PROPERTY RIGHTS AND THE FREE TRADE OF DATA

To maximize the economic and social benefits big data offers, policymakers must recognize organized data as a good and apply free trade policies to the digital exchange.[58] However, within the United States, underdeveloped intellectual property rights and privacy issues have caused policymakers at both the federal and state levels to hesitate in classifying big data as a commodity.[59]

A. Current U.S. Federal and State Law Cannot Establish Property Rights

Data is a raw material of production.[60] "Big data is some of the most granulated data ever available, generated from moment to moment from every device ... connected to the [I]nternet."[61] The challenge for businesses is not gathering the data, but organizing the data and using it to target consumers in a personalized way.[62] Businesses need analytical software to convert the large and intricate data sets into utilizable information.[63] Businesses use analytic software to build models based on available data and then run situations, repeating the value of data points and monitoring how different situations impact results.[64] "Current computing power can run millions of these simulations, thereby iterating all the possible variables until it finds a pattern, correlation, or insight" on proper business strategy.[65]

Even though a business's complex analytical infrastructure creates value out of raw data, the federal intellectual property

---

[58] *The world's most valuable resource is no longer oil, but data*, *supra* note 38.

[59] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1170 (2000).

[60] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 240, 240 (2013).

[61] Shelly Blake-Plock, *Where's The Value In Big Data?*, FORBES (Apr. 14, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/04/14/wheres-the-value-in-big-data/#19b054ec30da [https://perma.cc/A74V-DXRQ].

[62] *Id.*

[63] *See* Kim et al., *supra* note 39, at 96.

[64] Fred Greguras, *Legal Issues in Big Data: 2017*, ROYSE LAW FIRM (July 3, 2017, 8:06 PM), http://rroyselaw.com/technology-transactions/agtech/legal-issues-big-data-2017/ [https://perma.cc/MJ5H-UFAK].

[65] *Id.*

system is not well-equipped to deal with ownership of big data or the subsequent infrastructures created.[66] Data and infrastructures are not creative expressions that qualify for copyright (i.e., books, paintings, sculptures).[67] Not only is current copyright law inefficient for big data ownership, but also 17 U.S.C. § 102(b) codified an express limitation on copyright protection of ideas and facts.[68] Since big data is fundamentally factual information and data infrastructures usually involve combining algorithms that are classified as ideas, this limitation bars copyrighting big data.[69]

When considering federal patent law, the Supreme Court's decision in *Alice Corp. v. CLS Bank International* effectively eliminated the patentability of analytical software.[70] The Court in *Alice* held that, to be patent eligible, computer innovations must incorporate "an inventive concept" beyond computer application of an abstract idea.[71] Since businesses frequently rely on computer execution of series of routine algorithms to process big data, the use of a computer in a "particular technological environment" was not enough to transform an algorithm into an innovative concept.[72] Moreover, patentability of data and the technological infrastructures would be difficult to formally define to the Patent and Trademark Office, since both are subject to constant change and innovation.[73] When a company gathers new data, the infrastructure creates new results and the product itself changes, making the patent invalid.[74]

Turning to state law, scholars have argued that trade secrecy law may allow companies to maintain property rights in big data.[75]

---

[66] BRADEN R. ALLENBY ET AL., INFORMATION SYSTEMS AND THE ENVIRONMENT 6 (2001) (ebook).

[67] *Id.*

[68] 17 U.S.C. § 102(b) (2012).

[69] Mattioli, *supra* note 8, at 553–54.

[70] Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347, 2354 (2014).

[71] *Id.* (quoting that courts "must distinguish between patents that claim the building blocks of human ingenuity and those that integrate the building blocks into something more, … thereby transforming them into a patent-eligible invention").

[72] 134 S. Ct at 2358; *see* 35 U.S.C. § 112 (2012).

[73] Mattioli, *supra* note 8, at 554.

[74] *Id.* at 554–55, 561.

[75] *Id.* at 551–53.

"The Uniform Trade Secrets Act (UTSA), which most states have adopted, defines trade secrets as [']information['] that is (i) valuable, and (ii) reasonably protected."[76] "Vendors of information-based products have long secured exclusivity in their processes and knowhow through the law of trade secrets."[77] "The definition of [']information['] under the UTSA is expansive, covering technical and non-technical information, including methods, knowhow, and even ideas."[78] For example, Google's well-known "PageRank" algorithm and the algorithms high-speed electronic trading firms are two examples of data analytics software that have been recognized trade secrets.[79]

However, the secrecy requirement is difficult to meet for data and infrastructures that are shared and marketed, which is a large part of the digital trade.[80] Google and Facebook, in particular, have used personal data as a new source of economic value.[81] Once processed and classified, they provide relevant information for companies about consumer's interests and activities, which allows those companies to retarget these individuals for advertisement purposes.[82] Retargeted advertising is Google and Facebook's core business.[83] Both companies constantly track information about their users only to then disclose this data to companies willing to pay a per-advertisement rate.[84]

If the goal is to expand the free trade of big data domestically and internationally, creating property rights based on trade

---

[76] *Id.* at 550.

[77] *Id.*

[78] *Id.* (citing Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 76 (1999) ("Trade secret law ... extends to technical and non-technical information, expression, ideas, and facts, embracing such things as customer and supplier lists, financial information, methods of doing business, future marketing, sales and product plans and even employee names, job responsibilities and phone numbers.")).

[79] *See* VAN LINDBERG, INTELLECTUAL PROPERTY AND OPEN SOURCE: A PRACTICAL GUIDE TO PROTECTING CODE 130–31 (Andy Oram, ed., 2008) (discussing Google's use of trade secrecy).

[80] Mattioli, *supra* note 8, at 583.

[81] Asunción Esteve, *The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA*, 7 INT'L DATA PRIV. L. 36, 36 (2017).

[82] *Id.*

[83] *Id.* at 40.

[84] *Id.*

secret law would be counterintuitive.[85] "[T]rade secret law would slow the pace of ... innovation" in the data industry and limit trade in the digital market.[86] Any business that decided to enter the digital market would forfeit the property rights it had within the data the business collected and organized.[87] While the Technologic Giants, with their constant influx of data, have maximized their profits without private ownership of data, new companies would be pushed out once their property rights were quashed.[88]

Since neither federal nor state intellectual property law provides a legal method to establish property rights in data, policymakers and companies have sought to create a *sui generis* statutory regime of legal protection for organized data.[89] By creating a statutory regime that recognizes big data as a legal good, policymakers could finally address the privacy issues of big data as well as apply free trade principles to the digital market.[90]

B. A Statutory Regime Recognizing Data as a Commodity Would Allow Policymakers to Address Privacy Issues as well as Apply Free Trade Policies

Privacy of personal data is an important issue that underpins trust in the digital trade.[91] The data overflow presents concerns for privacy rights that, when left unaddressed, dampen the data economy and innovation.[92] A statutory regime would offer policymakers the chance to find "a balance between the beneficial uses of data and individual privacy," as well as apply free trade principles to the digital market.[93]

Omer Tene and Jules Polonetsky discuss privacy concerns in the digital age in the article *Big Data for All: Privacy and User Control in the Age of Analytics*.[94] Tene and Polonetsky assert that

---

[85] *See* Mattioli, *supra* note 8, at 551.

[86] *Id.*

[87] *Id.* at 538.

[88] *See* Kim et al., *supra* note 39, at 94 (discussing how the Technologic Giants maintain their monopoly on data through the digital divide).

[89] *See* Mattioli, *supra* note 8, at 580.

[90] *See id.* at 583.

[91] Tene & Polonetsky, s*upra* note 60, at 239.

[92] *Id.*

[93] *See id.; see also* Mattioli, *supra* note 8, at 583.

[94] Tene & Polonetsky, *supra* note 60, at 239, 251.

"the accumulation of personal data has an incremental adverse effects [sic] on privacy"[95] Researchers can draw different conclusions from an individual's online activity, and once data is linked to an identified individual, it becomes difficult to disentangle.[96] "Once any piece of data has been linked to a person's *real* identity any association between this data and a *virtual* identity breaks anonymity of the latter."[97] Tene and Polonetsky warn that "this incremental effect will lead to a 'database of ruin,' chewing away at an individual's privacy until his or her profile is completely exposed."[98]

Tene and Polonetsky concede that opening up an individual's virtual profile gives businesses predictive analysis that can be beneficial in numerous areas of society including healthcare, law enforcement, and national security.[99] However, "[p]redictive analysis is particularly problematic when based on sensitive categories ... such as ... race, [gender] or sexuality."[100] "This type of activity, while clearly unconstitutional under existing U.S. law, is not so far-fetched in other parts of the world."[101]

A statutory scheme that regulates data as a commodity exchanged between not only business-to-business but also consumer-to-business could allow the digital market to expand while also addressing privacy issues.[102] Tene and Polonetsky claim that open access between individuals and businesses offers a solution to privacy issues as the big data market expands.[103] The three components come together to promote transparency between individual users and the companies that want their data.[104] The call for

---

[95] *Id.* at 251.

[96] *Id.*

[97] *Id.* (quoting Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 IEEE SYMP. ON SECURITY & PRIVACY 119).

[98] *Id.* at 251–52.

[99] *Id.* at 253.

[100] *Id.* at 253–54 ("It is one thing to recommend for a customer books, music or movies she might be interested in based on her previous purchases; it is quite another thing to identify when she is pregnant before her closest family knows."). *Id.*

[101] *Id.* at 254.

[102] *See id.* at 263 (discussing that a framework for big data must balance with a privacy framework to allow individuals their privacy rights while also creating additional opportunity for efficient value creation and innovation in the digital market).

[103] *Id.*

[104] *See id.*

transparency is not new, but Tene and Polonetsky emphasize individuals' access to data in a usable format, which can create value to individuals and ensure better protection of privacy rights.[105] A statutory framework formally recognizing a transaction between individuals and businesses where an individual's personal data is exchanged for goods and services could address privacy issues, promote transparency, and still allow the digital market to expand under free trade.[106]

This Note emphasizes, however, that a statutory framework should still limit property rights in raw data. Raw data "should be regarded as neither an exclusive asset of individuals ... nor exclusively the property of businesses."[107] As discussed previously, data is a raw material of production.[108] Businesses create value in big data once the analytical infrastructure compiles, organizes, and stores the data.[109] Establishing property rights in raw data could eviscerate the competitive advantage companies gain when investing significant resources to organize and share data in commercially valuable ways, thereby stifling innovation within the digital market.[110] Recognizing the rights of individuals to access their data balances their right to privacy, invites scrutiny into businesses' data practices, and exposes potential misuses in data prior to a business ever establishing property rights within the data in which they invest.[111]

III. CHALLENGES TO THE FREE TRADE OF DATA: CYBERSECURITY THREATS AND REGULATIONS

The conventional idea is that private and public data infrastructures are susceptible to catastrophic cyberattacks that could leave consumers, enterprises and governments vulnerable.[112] As

---

[105] *Id.* at 268.

[106] *See id.*

[107] *Id.* at 269.

[108] *See supra* notes 60–69 and accompanying text.

[109] *Id.*

[110] Tene & Polonetsky, *supra* note 60, at 269.

[111] *Id.* at 268.

[112] Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. L. REV. 1503, 1503 (2013).

an increasing portion of the world embraces the digital era, cyberattacks "can now affect critical infrastructure, turn smartphones into monitoring devices, and put the safety of healthcare patients at risk."[113] To protect consumer data and private infrastructures, over fifty governments worldwide have developed cybersecurity strategies and regulations.[114] These government policies range from strong government control over both domestic and international flows of data to and from their borders, to voluntary regulations that promote coordination between the government and private companies.[115] This Section will first give a brief history of cyber threats and then discuss how cybersecurity regulations in the United States, the European Union and China have advanced to address future cyberattacks.

A. The History of Cybersecurity Threats

Breaches of data and information have existed as long as companies have stored digital information.[116] Public awareness of large-scale data breaches parallels the growth of computer access in the 1980s and 1990s.[117] As technology grows, governments and businesses store more information digitally, increasing efficiency but exposing more information to possible cyberattacks.[118] Since 2005, "the advancement of technology and proliferation of electronic data throughout the world," has made "data breaches a top concern for both enterprises and consumers."[119]

---

[113] *2017 Emerging Cyber Threats, Trends & Technologies Report*, GA. TECH. INST. FOR INFO. SEC. & PRIV. 1 (2017), http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf [https://perma.cc/ET2J-XWSF].

[114] Allan A. Friedman, *Cybersecurity and Trade: National Policies, Global and Local Consequences*, BROOKINGS 1 (2013), https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf [https://perma.cc/MCV6-C5LE].

[115] *See, e.g., id.*; *Overview of China's Cybersecurity Law*, KPMG 6–7 (2017), https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf [https://perma.cc/8BPK-CVFU].

[116] Nathan Lord, *The History of Data Breaches*, DIGI. GUARDIAN (July 27, 2017), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/3TG9-6B3M].

[117] *Id.*

[118] *See id.*

[119] *Id.*

The first major cybersecurity threat the world faced was the emergence of malicious software.[120] In 1988, the first Internet worm, the Morris worm, infected ten percent of the Internet.[121] This worm's "self-replication flooded many networks with an overload of traffic ... temporarily [disabling] approximately six thousand computers, including machines at NASA, some major universities, and several military bases."[122] However, system administrators were soon able to detect the worm and run a defense program.[123]

> Ultimately, the worm was a victim of its own success. The Morris worm was poor at determining whether or not a system was already infected, targets were soon infected with multiple copies of the worm running simultaneously. As copies scanned for new targets, the resulting exponential increase in the load on individual computers and network connections tipped off system administrators.[124]

The Morris worm was a landmark event in cybersecurity, leading to public awareness of "the potential that such attacks held for mass electronic destruction."[125]

The pace and magnitude of cyberattacks have increased since the foundations of cyber breaches in the 1990s.[126] Between 2005 and 2015, the Privacy Rights Clearinghouse reported more than 4,500 data breaches, resulting in more than 816 million individual records breached.[127] "In actuality, the numbers are [probably] much higher, as the total number of records breached reported by the Privacy Rights Clearinghouse includes breach reports for which the number of records breached is unknown."[128] "Additionally, the Privacy Rights Clearinghouse is not a comprehensive

---

[120] *See* Stephen Cass, *Anatomy of Malice*, IEEE SPECTRUM (2001), https://spectrum.ieee.org/telecom/internet/anatomy-of-malice [https://perma.cc/TE9Z-XLTT].

[121] *Id.*

[122] *The Social Impact of Viruses*, STAN. (Nov. 27, 2017), http://cs.stanford.edu/people/eroberts/cs201/projects/2000-01/viruses/social.html# [https://perma.cc/R4VB-9XUP].

[123] *See* Cass, *supra* note 120.

[124] *Id.*

[125] *The Social Impact of Viruses*, *supra* note 122.

[126] *See* Lord, *supra* note 116.

[127] *Id.*

[128] *Id.*

compilation of all breach data, so the actual ... [cumulative harm from data breaches] is likely substantially higher."[129]

The prime example of this is the financial and insurance data breaches that occurred in recent years.[130] For example, in 2013, the largest bank in the United States, JP Morgan & Chase (JP Morgan), reported that private information from seventy-six million households and eight million small businesses was exposed in a monumental cyberattack.[131] JP Morgan, on the other hand, "was seen as one of the best at security."[132] Financial institutions store "everything from social security numbers to detailed records of past spending."[133] As a result, financial institutions invest heavily in their cybersecurity programs.[134] JP Morgan currently spends $500 million per year on cybersecurity alone to protect its data infrastructure and the sensitive information it stores.[135] Thus, what was most alarming about the JP Morgan breach was how prepared the company was and how little difference it made.[136]

The JP Morgan breach indicated that cyberattacks may be an unavoidable consequence of collecting and storing this much sensitive information:[137] "[a]s innovative uses of the Internet by business and government organizations increases, so do the number

---

[129] *Id.*

[130] *See, e.g.*, Lorenzo Ligato, *The 9 Biggest Data Breaches Of All Time*, HUFFINGTON POST (Aug. 21, 2015), https://www.huffingtonpost.com/entry/biggest-worst-data-breaches-hacks_us_55d4b5a5e4b07addcb44fd9e [https://perma.cc/NAH9-QAD8].

[131] Jake Swearingen, *Why the JP Morgan Data Breach Is Like No Other*, ATLANTIC (Oct. 3, 2014), https://www.theatlantic.com/business/archive/2014/10/why-the-jp-morgan-data-breach-is-like-no-other/381098/ [https://perma.cc/9SEU-BKZU] ("Previous data breaches had been confined to retail companies (Target, Home Depot, etc.), where brands [were] required to meet basic security protocols and not much else.").

[132] *Id.*

[133] *Id.*

[134] Steve Morgan, *Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity*, FORBES (Jan. 30, 2016, 9:02 AM), https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#19621a025991 [https://perma.cc/7BJD-973U].

[135] *Id.*

[136] *See id.*

[137] Warren W. Fisher et al., *The Unavoidable Risk of Cloud Computing*, 1 J. BUS. ISSUES 1, 1 (2009), http://www.jrhasselback.com/Journal/JBI2009-1.pdf#page=5 [https://perma.cc/5SFQ-ZMGF].

of threats to information system security."[138] Even with current technology, many scholars suggest that large-scale information collection creates "risk[s] [that] cannot completely be avoided."[139]

When considering future cyberattacks, policymakers and scholars warn that attacks will shift from data and information theft to cyberterrorism.[140] As the digital revolution spreads and captures more sectors, technology that is fundamental to society—such as power grids, water service, or air traffic control—could be at risk.[141] Cyber threats are always evolving.[142] However, as the number, severity, and sophistication of attacks progresses so does the development of better action to protect businesses and individuals.[143]

B. Major Cybersecurity Actions in the United States, the European Union, and China

"Cybercrimes are borderless crimes where the repercussions and consequences are endless."[144] A cybersecurity regulation involves directives to protect information technology and computer systems with the purpose of enforcing safety mandates on companies and organizations to protect their infrastructure and data from cyberattacks.[145] As cyberattacks become more and more common, countries are beginning to take part in both private and public cyber-safety actions.[146] Many countries established their own

---

[138] *Id.*

[139] *Id.*

[140] *But see* James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CTR. FOR STRATEGIC & INT'L STUD. (2002), https://www.steptoe.com/publications/231a.pdf [https://perma.cc/XYU4-ADB5].

[141] *Id.*

[142] *Id.*

[143] *See* JOHN ARQUILLA & DAVID RONFELDT, NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY 283 (John Arquilla & David Ronfeldt eds., 2001).

[144] Charletta E. Anderson-Fortson, *Cyber Security and the Need for International Governance*, NAT'L L. REV. (2016), https://www.natlawreview.com/article/cyber-security-and-need-international-governance [https://perma.cc/D3QS-X77E].

[145] *See* Cybersecurity Act of 2015, Pub. L. No. 114-113, § 102(4), 129 Stat. 2242, 2936 (2015).

[146] *Global Cybersecurity Index (GCI) 2017*, INT'L TELECOMM. UNION iii, 1 (2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [https://perma.cc/945K-VZP8].

cybersecurity regulations with unique standards and approaches to digital safety.[147]

1. The United States

The role of the federal government in cybersecurity involves coordinating with private entities to secure both federal and nonfederal systems.[148] On December 18, 2015, President Obama signed the Cybersecurity Act of 2015 (the Cyber Act) into law.[149] The Cyber Act is landmark legislation that established the first broad mechanism under which the federal government, specifically the Department of Homeland Security, can begin standardizing cybersecurity.[150]

> The Act ... establishes a mechanism for cybersecurity information sharing among the private-sector and federal government entities. It also provides safe harbors from liability for private entities that share cybersecurity information in accordance with certain procedures, and it authorizes various entities, including [many] outside the federal government, to monitor certain information systems and operate defense measures for cybersecurity purposes. The Act also contains provisions designed to bolster cybersecurity protections at federal agencies, assess the federal government's cybersecurity workforce, and implement a range of measures intended to improve the cybersecurity preparedness of critical information systems and networks.[151]

The Cyber Act also requires that nonfederal entities review information that will be shared or utilized by those entities

---

[147] *See id.*

[148] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, CONG. RES. SERV. 1, 15 (2014), https://fas.org/sgp/crs/natsec/R42114.pdf [https://perma.cc/9UQS-263H].

[149] Keith M. Gerver, *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing*, NAT'L L. REV. 1 (2016), https://www.natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information [https://perma.cc/V4JT-FP3W].

[150] *What You Need to Know About the Cybersecurity Act of* 2015, LATHAM & WATKINS 1, (Feb. 18, 2016), https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015 [https://perma.cc/ZV3J-SWAA].

[151] *The Cybersecurity Act of 2015*, SULLIVAN & CROMWELL 1 (Dec. 22, 2015), https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf [https://perma.cc/ZZW2-6TEF].

to remove any information that the entities "know[] at the time of sharing" to be personally identified information not directly related to cybersecurity.[152]

Instead of a hardline regulatory approach, President Obama claimed the "only ... way to defend America from these cyber threats ... is through government and industry working together, sharing appropriate information as true partners."[153] The framework is designed to help businesses decide how to create new cybersecurity systems and implement new cybersecurity techniques as compared with prominent techniques used within the same industry.[154]

In May 2017, President Trump signed Executive Order 13800, entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which largely builds off the Obama Administration's cybersecurity policies.[155] The executive order draws directly on the Cyber Act's policy aim of producing a plan "to address the risk of multiple simultaneous cyber incidents affecting critical infrastructure,"[156] and applying standards for risk management set in the National Institute of Standards and Technology's framework for protecting critical infrastructures.[157]

Trump's executive order made key additions to U.S. cybersecurity policy, including directly assigning accountability to the heads of executive departments and agencies "for managing cybersecurity risk to their enterprises."[158] However, the executive order also reasserts that "because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, ... cybersecurity risks [constitute] ... an executive branch

---

[152] Cybersecurity Act of 2015, *supra* note 145, at § 103(b)(1)(E)(i).

[153] Katie Zezima, *Obama signs executive order on sharing cybersecurity threat information*, WASH. POST (Feb. 12, 2015), https://www.washingtonpost.com/news/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/?utm_term=.17d2e9d08c3b [https://perma.cc/QGS7-LBFC].

[154] *Id.*

[155] Exec. Order No. 13800, 82 Fed. Reg. 22,391 (May 16, 2017).

[156] Cybersecurity Act of 2015, *supra* note 145, at § 208; *see also id.* § 2(b) (following the Cybersecurity Act of 2015's goal of establishing a plan to protect and support critical infrastructure, but also specifically assigning agency heads to meet and collaborate proactive defense strategies).

[157] Exec. Order No. 13800 § 1(c)(i–ii) (May 11, 2017).

[158] *Id.* § 1(a).

enterprise," and will be addressed through the full power of the executive, not merely the federal agencies.[159] Another key element of the executive order is the "market transparency" provision.[160] This provision aims to "promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities" in both the public and private sectors.[161]

Trump's executive order is far from a comprehensive regulation—"[t]he final order goes ... much [more] ... [in-]depth on policy goals" as opposed to addressing how to actually meet them.[162] The only true action the executive order implements in the present is evaluating federal agencies' current cybersecurity practices and requiring the initial steps to coordinate policies between the Department of Homeland Security, Department of Justice, and Department of Commerce.[163] The current actions being taken appear to be merely precursors to eventually creating a broader cybersecurity policy.[164] But for now, the federal approach to cybersecurity is no more than far-reaching policy goals coupled with a framework to eventually create a centralized cybersecurity regulation in the future.[165]

On the state level, at least forty-two states have introduced more than 240 cybersecurity-related bills or resolutions.[166] According to the National Conference of State Legislatures, the key areas of state legislative activity include "[i]mproving government security practices ... commissions, task forces[,] and studies [on cyber security] ... [f]unding for cybersecurity programs and initiatives ... [t]argeting computer crimes ... [r]estricting public disclosure of sensitive security information [and] ... [p]romoting workforce, training, [and] economic development."[167]

---

[159] *Id.*

[160] *Id.* § 2(c).

[161] *Id.*

[162] *But see* Sean Gallagher, *Something about Trump cybersecurity executive order seems awfully familiar*, ARS TECHNICA (May 18, 2017), https://arstechnica.com/tech-policy/2017/05/the-text-and-subtext-of-trumps-cyber-executive-order/ [https://perma.cc/LV8J-ZBR8].

[163] *See id.*

[164] *See id.*

[165] *See id.*

[166] *Cybersecurity Legislation 2017*, NAT'L CONF. OF STATE LEGIS. (Dec. 29, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx [https://perma.cc/82R6-4TWU].

[167] *Id.*

While some of these actions have been performed at the federal level, "[s]tate regulation of cybersecurity [generally] stand[s] apart from federal standards."[168] First, state laws are able to focus more on consumer protection as opposed to the defense of large-scale infrastructure.[169] Second, state statutes often include a reasonableness standard for the data security efforts of entities that manage personal information.[170] In 2002, Minnesota enacted a cybersecurity statute requiring internet service providers to take "reasonable steps to maintain the security and privacy of a consumer's personally identifiable information."[171] Since then "thirteen other states have issued broader data security mandates generally requiring any entity ... that manages 'personal information' to employ reasonable data security practices."[172]

Although these commonalities may suggest that there is a harmonized approach to cybersecurity across US states, this is far from the case.[173] "Each state statute [usually] applies ... [different standards of safety] to different categories of data."[174] Moreover, the term "reasonable data security" allows for a range of interpretations within different state legislatures and state judicial systems.[175] This sort of flexibility has caused states to diverge from any sort of common regulatory approach.[176] For example, the California Attorney General released the California Data Breach Report in 2016, which referenced specific standards for defining "reasonableness," providing that, "the failure to implement all the [Center for Internet Security's Critical Security] controls that apply to an organization's environmental constitutes a lack of reasonable security" under California's cybersecurity statute.[177]

---

[168] David Forscey et al., *Cybersecurity Is The Next Frontier Of State Regulation*, LAW360 (May 11, 2017, 1:26 PM), https://www.law360.com/articles/922786/cybersecurity-is-the-next-frontier-of-state-regulation [http://perma.cc/A59M-GW54].

[169] *Id.*

[170] *Id.*

[171] MINN. STAT. ANN. § 325M.05 (West 2002).

[172] Forscey et al., *supra* note 168.

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] *Id.*

[177] *California Attorney General Releases Report Defining "Reasonable" Data Security*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SECURITY L. BLOG (Feb. 19, 2016) (citing California Data Breach Report 2012–2015), https://www

California's working definition of "reasonable" data security differs significantly from many other states like Minnesota's that requires "reasonable steps to maintain the security and privacy," which is a far more vague and open to a wide variety of interpretations.[178]

These diverging standards can impose significant burdens on companies, especially small businesses, that actively use and store data.[179] Based on the variations in each state, businesses will have to comply with dozens of different cybersecurity standards to enter different markets within the United States.[180] Additionally, businesses must consider the costs of fitting into these regulations and the risk of potential legal exposure under each state law against the potential profits.[181] Without a more unified standard, many businesses are kept out of digital markets within different states.[182]

2. The European Union

On April 14, 2016, the EU Parliament approved the General Data Protection Regulation (GDPR).[183] The GDPR was designed to "harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."[184] Since the European Commission first proposed a unified approach to cybersecurity, the legislation has attracted attention from the international community.[185] "[Enterprises] across the EU and beyond have been frustrated by the increasing lack of [harmonization] across the Member States, despite data flowing increasingly without

---

.huntonprivacyblog.com/2016/02/19/california-attorney-general-releases-report-defining-reasonable-data-security/ [https://perma.cc/3PTH-6TFC].

[178] MINN. STAT. ANN. § 325M.05 (West 2002).

[179] Forscey et al., *supra* note 168.

[180] *See id.*

[181] *See id.*

[182] *See id.*

[183] THE EU GENERAL DATA PROTECTION REGULATION (Dec. 1, 2017), https://www.eugdpr.org [https://perma.cc/GX6E-HQV2].

[184] *Id.*

[185] *The EU General Data Protection Regulation*, ALLEN & OVERY (2017), http://www.allenovery.com/publications/en-gb/data-protection/Pages/default.aspx [https://perma.cc/6DAR-KJ98].

boundaries."[186] The EU institutions have since risen to the task: the adoption of the GDPR was a milestone in data protection law.[187]

The GDPR updates the EU's 1995 Data Protection Directive 95/46/EC.[188] Although the key principles of data privacy established in the previous directive remain, the GDPR made many changes to the regulatory policy.[189] The biggest change to the regulatory landscape comes with the extended jurisdiction of the GDPR, applying "to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location."[190] The previous territorial applicability under the directive referred to data process "in context of [the activities] of an establishment," as opposed to the "data subjects."[191] The GDPR makes its application very clear: "it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not."[192] In addition, the GDPR will also have extraterritorial applicability to data controllers or processors that are not even established in the EU where the activities relate to: "offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU."[193] Also, to represent their interest in data sharing within member states and facilitate smoother compliance, "[n]on-E[U] businesses processing the data of EU citizens will also have to appoint a representative in the EU."[194]

The GDPR also established new penalties for organizations in breach.[195] As a maximum penalty, organizations in breach

---

[186] *Id.*

[187] *Id.*

[188] *An Overview of the Main Changes Under the GDPR and How They Differ from the Previous Directive*, THE EU GEN. DATA PROTECTION REG. (Dec. 1, 2017) [hereinafter EUGDPR], https://www.eugdpr.org/the-regulation.html [https://perma.cc/R89B-3CC4].

[189] *Id.*

[190] *Id.*

[191] Council Directive 95/46/EC, art. 4, 1995 O.J. (L 266) [https://perma.cc/L3PH-PKHU]; *id.*

[192] EUGDPR, *supra* note 188.

[193] *Id.*

[194] *See id.*

[195] *Id.*

of the GDPR "can be fined up to four percent of annual global turnover or €20 Million (whichever is greater)."[196] There is a "tiered approach to fines" under the GDPR based on the seriousness of the infringement.[197] Additionally, based on the GDPR's extraterritorial jurisdiction, rules apply to all controllers and processors that deal in EU citizens personal data, meaning cloud storage and processing will no longer be exempt from the EU's regulatory enforcement and penalties.[198]

Finally, the GDPR expanded "data subject" rights, which provides individuals a wide array of rights that can be enforced against any organizations processing personal data.[199] At its core, data subject rights enforce the GDPR's "privacy by design" concept.[200] Privacy by design calls for "the inclusion of data protection from the onset of the designing of systems, rather than an addition."[201] More specifically, Article 28 states "[t]he controller shall ... implement appropriate technical and organizational measures ... in an effective way ... in order to meet the requirements of this Regulation."[202] Furthermore, Article 23 calls for controllers to process only the data "*absolutely necessary* for the completion of its duties," and limits access to personal data to only those "need[ed] to act out the processing."[203] The fundamental data subject rights the GDPR added to EU data protection law include: the right to access, the right to be forgotten, and the right to restrict processing.[204]

---

[196] *Id.*

[197] *Id.*

[198] EUGDPR, *supra* note 188.

[199] Detlev Gabel & Tim Hickman, *Chapter 9: Rights of data subjects—Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Sept. 13, 2017), https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation [https://perma.cc/Q4J5-G66W].

[200] EUGDPR, *supra* note 188.

[201] *Id.*

[202] Council Regulation 697/2016/EC Apr. 27, 2016, The General Data Protection Regulation, 2016 O.J. (L 119/1) art. 28(1) [hereinafter General Data Protection Regulation], https://web.archive.org/web/20171013160353/http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf; *id.*

[203] EUGDPR, *supra* note 188; General Data Protection Regulation, art. 23 (emphasis added).

[204] Gabel & Hickman, *supra* note 199.

The right to access is a feature necessary to ensure data subjects are able to enforce their data protection rights under the GDPR.[205] "The GDPR expand[ed] the mandatory categories of information which must be supplied in connection with data subject access request[s]."[206] Under Article 15, data subjects have the right to obtain a copy of the personal data the controller processes as well as general information about where the controller is processing their data, the purpose of processing, the category of data being processed, and the recipients who will have access to the data.[207]

The right to be forgotten, or "Data Erasure," entitles the data subject to require the controller to delete the subject's data, terminate additional distribution, and potentially have third parties cease processing his or her personal data.[208] However, data subjects must meet one of the reasons for erasure as outlined in Article 17, which include but are not limited to: (1) that the data is no longer needed for its lawful, original purpose, (2) that the lawful basis for the processing is the data subject's consent which may be withdrawn, or (3) erasure is necessary to comply with EU law or national law of the Member State.[209]

Finally, a new concept in the GDPR is the right to restrict processing.[210] "In some circumstances, data subjects may not be entitled to require the controller to erase their personal data but may be entitled to limit the purposes for which the controller can process [that] data."[211] Nevertheless, this right is usually coupled with the right to erasure as a temporary means to protect the data subject until the governing body can make a formal decision on an erasure request.[212] Data subjects have the right to restrict the processing of personal data if: (1) the accuracy of the data is contested,[213] (2) the processing is unlawful and the

---

[205] *Id.*

[206] *Id.*

[207] General Data Protection Regulation, art. 15(1)(a)–(h).

[208] *Id.* at art. 17(1)(a)–(f).

[209] *See* Gabel & Hickman, *supra* note 199; *see also* EUGDPR, *supra* note 188.

[210] Gabel & Hickman, *supra* note 199.

[211] *Id.*

[212] *Id.*

[213] Note that this restriction only lasts for as long as it takes to verify the accuracy of the data in question. *Id.*

data subject requests restriction as opposed to erasure, (3) the controller no longer needs the data for the original purpose but the data is still necessary for the controller to establish or defend a legal right, or (4) verification of overriding grounds is pending during the context of an erasure.[214]

Overall, the GDPR's expansion of data subject rights has created new burdens for firms and businesses accessing and processing EU data.[215] Organizations now face a much broader range of circumstances in which data subjects can trigger administrative burdens and outright loss of access to consumer information.[216] The GDPR's focus on transparency and accountability puts

> individuals and their rights at the heart of the GDPR. Controllers will need to consider all aspects of their processing activities in light of the rights afforded to individuals, so that they will ultimately be in a position to demonstrate compliance not only when individuals seek to exercise those rights, but with their overall obligations under the GDPR.[217]

3. China

The Chinese Cybersecurity Law (CSL) came into effect on June 1, 2017, becoming the first comprehensive law to address cybersecurity concerns in China.[218] The law imposes new security standards for both cyber and physical aspects of networks including strict data localization regulations, increased government access to cyber activities, and monetary penalties for non-compliance.[219]

---

[214] *Id.*

[215] *See GDPR in Context: Data Subject Rights*, MATHESON (2017), http://www.matheson.com/images/uploads/documents/MATH_10010_GDPR_in_Context_-_Data_Subject_Rights.pdf [http://perma.cc/SK2A-D6FN] (describing burdens and scope of responsibility for companies regarding data subjects).

[216] *See id.*

[217] *Id.*

[218] Carley Ramsey & Ben Wootliff, *China's Cyber Security Law: The Impossibility of Compliance?*, FORBES (May 29, 2017, 3:29 AM), https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/#5f52c297471c [https://perma.cc/6KPP-HFGR].

[219] *See China Passes New Cybersecurity Law*, COVINGTON & BURLING 1 (Nov. 8, 2016), https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf [https://perma.cc/656V-WT8Y]; *see also* Zack Dong & Gerard M. Stegmaier, *New Developments in China's Cybersecurity*

China's move to strengthen its cybersecurity regulations is not dissimilar to the global shift in favor of tighter cybersecurity.[220] "China is a vocal proponent of 'cyberspace sovereignty,' a theory that [advocates the right for the] state[] ... to [exclusively] regulate the internet activity within their border[]."[221] However, the application of CSL has been surrounded by controversy, particularly from the international business community.[222]

The CSL expressly applies to two entities: "Network Operators" and "Critical Information Infrastructure Operators."[223] Network operators are defined as "owners, operators, and service providers of networks."[224] This definition is extremely vague and can be broadly interpreted to include any organization that operates a computer network or data storage unit in China.[225] Thus, a Chinese or foreign company that collects data and information by providing services, conducting business activities, or even just hosting a website in China is likely subject to CSL regulations as a "Network Operator".[226]

Network operators are obligated to "safeguard their networks against disruption, damage or unauthorized access, and to prevent data leakage, theft or tampering."[227] CSL requires network operators to build an effective and clear security system within their organizations and find "rational technical solutions" to improving data protection and mitigating network risks.[228]

Law, REED SMITH (July 6, 2017), https://www.reedsmith.com/en/perspectives/2017/07/new-developments-in-chinas-cybersecurity-law.

[220] Ramsey & Wootliff, *supra* note 218.

[221] *See China Passes New Cybersecurity Law*, *supra* note 219, at 2.

[222] Cate Cadell & Michael Martina, *Foreign business groups push for delay in controversial China cyber law*, REUTERS (May 12, 2017, 5:40 AM), https://www.reuters.com/article/us-china-cyber-law/foreign-business-groups-push-for-delay-in-controversial-china-cyber-law-idUSKBN188156 [https://perma.cc/F6X5-6L4H].

[223] *An In-Depth Examination of China's New Cybersecurity Law Part I: Who Must Comply?*, ROPES & GRAY (July 7, 2017), https://www.ropesgray.com/newsroom/alerts/2017/07/Security-Whos-Regulated-Under-the-New-PRC-Cybersecurity-Law-An-In-Depth-Examination.aspx.

[224] *Id.*

[225] *Id.*

[226] *See id.*

[227] *China Passes New Cybersecurity Law*, *supra* note 219.

[228] *Overview of China's Cybersecurity Law*, *supra* note 115, at 9.

Network operators will also be subject to specific rules depending on their classification under the Multi-level Network Security Protection Scheme.[229] The Multi-level Network Security Protection Scheme is an existing regulation that requires companies to meet certain security standards based on an evaluation of the information companies are gathering and the potential threat to national security a breach would create.[230]

"Critical Information Infrastructure Operators" are a subset of "Network Operators" that "are subject to notably stricter requirements."[231] While this is a key distinction under the regulation, the CSL does not clearly define a "Critical Information Infrastructure Operator."[232] Article 31 provides a non-exhaustive list of industrial sectors that are considered "critical information infrastructure,"[233] with a catchall provision that includes "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest."[234] This broad definition means that any company that is a supplier to a critical sector, as well as any company that holds a significant amount of information on Chinese citizens, could become a target for regulations under the CSL.[235]

Organizations that are classified critical information infrastructure operators must regularly assess their cyber risk in accordance with Article 38 of the CSL.[236] The largest change in the CSL is that all personal information and important data

---

[229] *China Passes New Cybersecurity Law*, *supra* note 219.

[230] *National Security and China's Information Security Standards*, CTR. FOR STRATEGIC & INT'L STUD. (Nov. 8, 2012), https://www.csis.org/analysis/national-security-and-china's-information-security-standard [https://perma.cc/NW7C-WWSY].

[231] *An In-Depth Examination of China's New Cybersecurity Law Part I: Who Must Comply?*, *supra* note 223.

[232] *See id.*

[233] The CSL references the following industry sectors as "critical information infrastructures": "public communication, information services, energy, transportation, water, finance, public services, and e-government." *Id.*

[234] *See id.*; *see also China Passes New Cybersecurity Law*, *supra* note 219, at 2.

[235] Ramsey & Wootliff, *supra* note 218.

[236] *Overview of China's Cybersecurity Law*, *supra* note 115, at 11.

that critical information infrastructure operators collect in China must be stored domestically.[237] If an organization needs to transmit data offshore, a designated government agency must conduct a security assessment and the transferred data must be adjusted to best fit the CSL requirements.[238] Thus, organizations that operate critical information infrastructures in China and transmit data to headquarters, partners, or suppliers overseas will need to reassess and reorganize their approach to data collection and storage.[239]

Finally, the CSL added specific penalties for foreign offenders.[240] "In addition to the usual penalties for non-compliance[241] ... the new Law provides for specific penalties such as the freezing of assets or other sanctions" to any foreign organization or individuals that attack or harm any critical information infrastructures in China.[242]

Companies operating in China or seeking access to Chinese markets, must evaluate how the new laws may impact operations.[243] While the CSL does seek to balance the dual goals of enhancing cybersecurity and developing the digital economy through the free flow of data,[244] overseas opposition groups lobbied hard to delay the CSL implementation.[245] Industry groups claim that the influx of new measures gives the Chinese government "unprecedented access to foreign companies' technology" and the information they collect through the movement of data.[246] Furthermore, more than fifty trade associations and chambers of commerce signed a letter in May 2017 in an effort to delay the CSL's implementation, arguing "the law could affect billions of

---

[237] *Id.* at 12.

[238] *Id.*

[239] *Id.*

[240] *China Passes New Cybersecurity Law*, *supra* note 219, at 3.

[241] Typical penalties usually include "warnings, suspension of operations, revocation of licenses, fines set within a fixed range." *Id.*

[242] *Id.*

[243] *Id.*

[244] *Id.* at 1.

[245] *Foreign Firms Grapple with China's 'Punitive' Cybersecurity Laws*, S. CHINA MORNING POST (May 25, 2017), http://www.scmp.com/news/china/economy/article/2095595/foreign-firms-grapple-chinas-punitive-cybersecurity-laws [https://perma.cc/ZGB2-UYDA].

[246] *Id.*

dollars of cross-border trade and lock out foreign cloud operators because of limits on how they operate in the country."[247] Moreover, according to the letter from bodies representing businesses based in the United States, Europe, Japan, Korea, Australia and elsewhere, "[t]hese measures will add costly burdens, restrict competition and may decrease the security of products and [jeopardize] the privacy of Chinese citizens."[248]

IV. AN INTERNATIONAL CONVENTION ON CYBERSECURITY AND THE FREE TRADE OF DATA

Cyberspace has been notoriously difficult to regulate.[249] Large-scale regulations require coordination between governments and many private companies with many different infrastructures.[250] Moreover, policyholders also must consider the balance between individual privacy rights and potential business growth, making cybersecurity a novel issue.[251]

While cybercrimes have obvious effects on economic activity, cybersecurity can have similar negative economic implications "if only because of its' high cost and deliberate information inefficiencies due to deliberate isolation of networks."[252] In other words, cyberattacks harm the economy, and without a coordinated approach to cybersecurity, the digital market is bogged down with "information inefficiencies."[253] Likewise, "no nation-state can achieve adequate cybersecurity on its own;" cybercrimes do not respect geographic or political borders, and without international coordination, economic ramifications are merely surface issues to the idea of cyberwarfare.[254]

---

[247] *Id.*

[248] *Id.*

[249] *Touring the World of Cybersecurity Law*, RSA CONF. 3 (Feb. 29, 2016), https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf [https://perma.cc/CKZ5-NDJG].

[250] *Id.*

[251] *See id.*

[252] David Satola & Henry Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reactions on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 WM. MITCHELL L. REV. 1745, 1749 (2011).

[253] *See id.*

[254] *See id.* at 1783.

To address the shortcomings of the current, decentralized cybersecurity system, an international platform should recognize a convention ensuring a coordinated, multilateral strategy to address cybersecurity.[255] Also, to balance the overhaul of regulations that come with an international agreement, the WTO should update trade policies to include big data as a formal, regulated commodity in which free trade efforts must apply to the fullest extent possible.[256]

A. A Multilateral Convention on an International Platform

Cybercrimes are transnational and require a transnational response.[257] The current decentralized measures the private and public sectors provide cannot reach the adequate level of security necessary to promote the digital trade while also protecting consumers.[258] The speed and technical complexity of cyber-activity need a "prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks."[259]

In 1999, members of government, industry, NGOs, and academia, from many nations, met at Stanford University's Center for International Security and Cooperation to discuss a potential plan for an international agreement concerning cybersecurity.[260] The Stanford meeting drafted a multilateral cybersecurity convention, titled the "Proposal for an International Convention on Cyber Crime and Terrorism."[261] The Proposal argues that an international convention on cybersecurity would ensure that State Parties unanimously:

- "adopt laws making dangerous cyber activities criminal;

---

[255] Abraham D. Sofaer et al., *A Proposal for an International Convention on Cyber Crime and Terrorism*, STAN. U., i (Aug. 2000), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf [https://perma.cc/7ZSJ-JB27].

[256] *See* Diane A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 633 (2014).

[257] Sofaer et al., s*upra* note 255, at ii.

[258] *See id.* at i.

[259] *Id.* at ii.

[260] *Id.* at i.

[261] *See id.*

- enforce those laws or extradite criminals for prosecution by other States;
- cooperate in investigating criminal activities and in providing usable evidence for prosecutions; and
- participate in formulating and agree to adopt and implement standards and practices that enhance safety and security."[262]

An international agency created pursuant to the Convention would provide a forum for "international discussion, ongoing response to technological developments, and technical assistance to developing States."[263] The Proposal suggests that policymakers form the international "Agency for Information Infrastructure Protection" to serve as a "formal structure in which interested groups will cooperate through experts in countries around the world in developing standards and practices concerning cyber security."[264]

The challenge of controlling cybercrimes requires a full range of responses, including both voluntary and legally mandated cooperation.[265] An international cybersecurity agreement will only be possible, however, if policymakers can take into account the "substantial differences that exist between activities regulated by established international regimes and cyber systems" while also integrating the new policies to help standardize cybersecurity efforts.[266] Considerable financial burdens and sovereignty issues are byproducts of unifying cybersecurity efforts.[267] "Many states will be unprepared … to agree to limit their control of cyber activities they regard as essential" to the national and economic security interests.[268] Cooperation between developed and developing nations is essential to the "development and implementation of technological solutions and standards to enhance the capacity

---

[262] *Id.* at ii.

[263] Sofaer et al., s*upra* note 255, at ii.

[264] *Id.* at iv.

[265] *Id.* at 2.

[266] *See* ABRAHAM D. SOFAER, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 180 (The National Academies Press ed., 2010).

[267] *See id.*

[268] *Id.*

of states and users effectively to protect computers and systems from future attacks."[269]

"The globally-interconnected digital information and communication infrastructure known as cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security."[270] Currently, many believe that cybersecurity as a concept involves only national or industry-based security standards and consumer privacy laws.[271] An international agreement on cybersecurity could focus more on "Internet governance," which involves balancing "human rights and the economic and developmental interests associated with a vibrant, innovative, and competitive [information and communication technology][272] sector" with state security interests.[273] States should consider the high potential benefits of an international cybersecurity agreement against some administrative and sovereignty burdens.[274]

Scholars still debate whether states should address cybersecurity issues through the North Atlantic Treaty Organization (NATO) or the United Nations (U.N.).[275] NATO is arguably the most important collective defense and has already addressed cyber threats in policy and operational terms.[276] In 2002, the NATO Summit in Prague established the Cyber Defense Program to create a unified front to defend against cyberattacks.[277] The Cyber Defense Program then created the NATO Computer Incident Response Capability to further provide NATO with procedures to "prevent,

---

[269] Sofaer et al., s*upra* note 255, at 2.

[270] Melissa Hathaway, *Securing Our Digital Future*, WHITE HOUSE (May 29, 2009), https://obamawhitehouse.archives.gov/blog/2009/05/29/securing-our-digital-future [https://perma.cc/NYY9-VWPP].

[271] Satola & Judy, *supra* note 252, at 1786.

[272] John Giles, *What is ICT, What is the Meaning or Definition*, MICHALSONS (July 5, 2017), https://www.michalsons.com/blog/what-is-ict/2525 [https://perma.cc/3G5N-KD9M] (stating that "ICT" stands for "information and communication technology").

[273] Satola & Judy, *supra* note 252, at 1786.

[274] *See id.*

[275] *Id.* at 1783–84.

[276] David P. Fidler et al., *NATO, Cyber Defense, and International Law*, (2013), https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub.

[277] *Id.* at 4.

detect, and respond to cyber threats."[278] Despite NATO's preventative approach, the cyberattacks on Estonia in 2007 revealed NATO's inadequacy in cyber-protection.[279] The Estonian incident "helped bring the stakes of cyber threats into sharper perspective for NATO" and sparked a significant restoration in NATO's political commitment and operational capabilities to address cybercrimes.[280] NATO has continually given prominence to cyber-defense strategies through the Strategic Concept adopted at the Lisbon summit in 2010, the Cyber Defense Concept, Policy, and Action Plan in 2011 and the Chicago summit declaration in 2012.[281]

The U.N. has been less forthcoming on international coordination for cybersecurity policies.[282] The first major work emerged in 2001 with the U.N. Convention on Cybercrime.[283] The treaty signified the first international treaty

> to define and standardize responses to Internet crimes. It sought to bridge the gap between international domestic laws regarding behavior, like copyright infringement, fraud, hate crimes, and issues regarding network security. Most of what this convention and treaty aimed at was to act as a facilitating document for international cooperation when it comes to preventing, labeling, and punishing cyber-crimes.[284]

The treaty has been ratified by the EU, Australia, Canada, Japan, and several other countries.[285] In 2012, the U.N. Secretary General Ban Ki-Moon appointed a governmental panel of experts from fifteen states, called the "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in Context of International Security," to draft an expert report on developments in cybersecurity and information technology.[286]

---

[278] *Id.*

[279] *Id.* at 5.

[280] *Id.*

[281] *Id.* at 5–6.

[282] *See* Joseph Espinoza & Kleopatra Moditsi, *Combating Cyber Security Threats*, OLD DOMINION U. MODEL UNITED NATIONS SOC. 1, 3–4 (2016), https://www.odu.edu/content/dam/odu/offices/mun/issue-briefs-2016/ib-cyber-intelligence-gathering.pdf [https://perma.cc/RVC8-BHXX].

[283] *Id.* at 3.

[284] *Id.*

[285] *Id.*

[286] *Id* at 4.

This report, now seen as a seminal work on the cybersecurity actions, "highlights four main areas to be addressed: cooperation, international law, confidence-building measures, and improving state IT capacities."[287] The most recent report from the Government Groups of Experts included four landmark findings in the cybersecurity field:

- "the existence of state sovereignty in cyberspace,
- international obligations made by states are applicable in cyberspace,
- states cannot use proxies to break international law and norms, and
- the recognition of the UN as the principal organization for the establishment of fundamental principles on the topic."[288]

The international platform through which nations establish a multilateral convention on cybersecurity would likely influence how the world understands the term "cybersecurity."[289] NATO is primarily a defensive organization.[290] Cybersecurity from NATO's point of view "ha[s] security at its core," which means an appropriate agreement would promote a government's ability to safeguard its national security, at the expense of expanding individual and business rights in the digital market.[291] Those that sponsor a defensive approach to cybersecurity believe an international cybersecurity treaty should warrant nations the power to "know exactly who sent and received every transmission, every transmission's traceroute, and the contents of every transmission; it can delete, block, and/or seize any transmission of which it disapproves; and it can punish efficiently those who send or receive unapproved transmissions."[292]

At the other end of the spectrum, the U.N. is an international organization committed to promoting social progress, better living standards, and human rights in addition to international

---

[287] *Id.*
[288] *See* Espinoza & Moditsi, *supra* note 282, at 4.
[289] Satola & Judy, *supra* note 252, at 1750.
[290] *See* Fidler et al., *supra* note 276.
[291] Satola & Judy, *supra* note 252, at 1750.
[292] *Id.*

peace and security.[293] A multilateral convention on cybersecurity from the U.N.'s perspective could better incorporate the idea of internet governance, which balances internet security with "the type of freedoms protected by instruments such as the First, Fourth, Fifth, and Fourteenth Amendments of the United States Constitution, the European Union Charter of Fundamental Rights, and numerous United Nations human rights documents."[294]

B. The World Trade Organization and the Free Trade of Data

Every international transaction entails a data flow across borders.[295] Whether the exchange falls between business groups or between subsidiaries of the same company, "the business network feeds on communications between partners, often scattered all over the world."[296] A multilateral convention should centralize state cybersecurity actions, but not at the cost of digital trade.[297] To protect the digital market, the WTO should recognize data as a commodity and impose free trade obligations to allow the cross-border flow of data between international parties.[298]

The WTO's General Agreement on Trade in Services (GATS) is a positive agreement between members: "a Member agrees to open its markets to services and service providers of other Members in only those service sectors listed in the Member's Schedule of Specific Commitments, and as limited by any terms and conditions specified in that Schedule."[299] The most significant obligation under GATS Article II requires "a Member to extend unconditionally, to services and services suppliers of any other Member, 'treatment no less favorable' than that it accords to like services

---

[293] United Nations, *What We Do*, UNITED NATIONS CAREERS (Jan. 25, 2018), https://careers.un.org/lbw/home.aspx?viewtype=WWD [https://perma.cc/378N-FPK3].

[294] Satola & Judy, *supra* note 252, at 1750.

[295] Davide Borelli, *International Trading of Big Data*, 3 ATHENS J. L. 21, 21 (2017), https://www.athensjournals.gr/law/2017-3-1-2-Borelli.pdf, [https://perma.cc/R2LQ-XDBH].

[296] *Id.*

[297] *See id.*

[298] *See* Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, 21 HARV. J. L. & TECH. 683, 699 (1999).

[299] MacDonald & Streatfeild, *supra* note 256.

and service suppliers of any other Member."[300] The "most favored nation[s]" clause requires open markets for all member nations.[301]

However, GATS Article XIV provides a list of general exceptions to a Member's open-market commitments,[302] which "are designed to allow Members to adopt measures, which may otherwise violate a Member's commitments, to protect public morals, public order, or other important societal interests."[303] The relevant exception to the free trade of data is Article XIV(c)(ii), which provides that GATS does not prevent a nation from limiting trade to protect privacy of personal data.[304] Thus, a member may adopt a measure:

> necessary to secure compliance with laws or regulations which are not inconsistent with the provision of this Agreement including those relating to:
>
> > (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts ....[305]

Members invoking the GATS exception must prove that the measure is "necessary" to the relevant public policy goals.[306]

Diane MacDonald and Christine Streatfeild analyze the WTO's GATS and the "necessary" requirement in terms of the cross-border trade of data.[307] MacDonald and Streatfeild insist that, when discussing the necessity requirement, the WTO's Appellate Body has referred to a

> range of degrees of necessity. At one end of this continuum lies "necessary" understood as "indispensable"; at the other end, is "necessary" taken to mean as "making a contribution to." We consider that a "necessary" measure is, in this continuum, located

---

[300] *Id.* at 634.
[301] *Id.*
[302] *Id.* at 637.
[303] *Id.* at 637–38.
[304] *Id.* at 638.
[305] *Id.*
[306] *Id.*
[307] *Id.* at 641–42.

> significantly closer to the pole of "indispensable" than to the opposite pole of simply "making a contribution to."[308]

MacDonald and Streatfeild argue that the WTO needs to reanalyze the issues surrounding the digital trade.[309] As technology advances, new infrastructures offer protection that may revoke the "necessary" status of many conservative data regulations or may not even be processing and disseminating "personal data."[310] MacDonald and Streatfeild consider the data exchanged through financial institutions and wonder:

> [b]ut, is the processing of credit card transaction data regarded as "the processing and dissemination of personal data"? Is "personal data" equivalent to financial data or data that simply records a credit card transaction? What if the data has been disaggregated, such that it is stripped of markers that would allow the identification of a particular individual? How can disaggregated data still be regarded as "personal data" or "confidential data"?[311]

When considering the necessity requirement, many countries argue that digital trade should be restricted based on the recognition of personal data privacy as a fundamental right.[312] Thus, protecting the privacy of residence is of "paramount importance" to these countries.[313] However, MacDonald and Streatfeild push back on this notion and leave one big question the WTO has yet to answer: "does this privacy mandate outweigh the importance many others, such as the United States, put on the free flow of information across the Internet?"[314]

The WTO has left many questions unanswered regarding the growth of technology and the importance of the digital market.[315] MacDonald and Streatfeild admit that, in practice, the WTO dispute resolution panels usually uphold data restrictions based on the Article XIV privacy exception.[316] Yet, MacDonald

---

[308] *Id.* at 639–40.
[309] *Id.* at 642–46.
[310] *Id.* at 642–43.
[311] *Id.* at 644.
[312] *See id.* at 645.
[313] *Id.*
[314] *Id.*
[315] *See id.* at 651.
[316] *See id.* at 642.

and Streatfeild argue that, while "[a] tension exists between businesses that rely on that information for efficient ... advertising, and business processes and consumers who are increasingly demanding enhanced Internet privacy," technological advancements and the explosions of cross-border data transmissions "have placed the personal data issue on a collision course with international trade disciplines."[317]

To promote the digital trade, the WTO must weigh privacy interests and new technologic protections.[318] While states may be ready to seize the opportunity of digitization, arguments of sovereignty and privacy rights impose borders in the digital space.[319] Trade agreements have helped overcome some of the problems and inconsistencies within international trade, and the WTO has provided a framework to bolster global conversations as technology advances.[320] To encourage business productivity, efficiency and transparency in the digital market, the WTO needs to incorporate the free trade of data into its affirmative duties.[321]

CONCLUSION

The digital market needs a synthesis of new ideas combined with the common international structures to create a policy initiative for new realms of human innovation.[322] Data is now everywhere—in every sector, in every economy, in every organization and user of data—the public sector included.[323] The opportunity big data offers business in terms of operational efficiency, overall firm performance, and customer service can potentially increase profit margins up to sixty percent.[324]

---

[317] *Id.* at 650, 652.

[318] *Id.* at 652.

[319] Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT'L L. 407, 407 (2017).

[320] *Id.* at 408.

[321] *See id.*

[322] 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 J. MARSHALL J. COMP.

[323] Wamba et al., *supra* note 20.

[324] *See* Manyika et al., *supra* note 15.

Legally, underdeveloped property rights and lack of regulation of trade barriers has hindered "the fourth industrial revolution."[325] Lack of property rights, combined with the digital divide the Technologic Giants exploit to eliminate any future competitors, severely limits competition and the ability of new start-ups to enter the market.[326] Moreover, government restrictions on cross-border data flow negatively affect trade through increasing business costs for digital platforms, increasing the cost of digitally intense services imports such as professional services and cloud computing, discouraging the globalization and connection of businesses, reducing productivity and exports, and limiting potential productivity gains across markets.[327]

While the digital trade does offer vast business opportunities, one cannot ignore cybersecurity as an increasing threat.[328] As the world becomes more and more digital, society is exposed to cyberattacks on vital areas such as power grids and air traffic controls.[329] Cyberattacks are evolving quickly, and the system of decentralized cybersecurity is struggling to catch up.[330] The constant threat has widened the gap in the digital debate between conservative security approaches like those taken in the EU and China, to softer approaches of compliance like regulations in the United States.[331]

An international convention on cybersecurity coupled with WTO establishment of data as a commodity to which free trade principles apply may be the standardization the global realm needs. Standardization of cybersecurity would also present a unified front against cybercrime, offering quicker response actions,

---

[325] Burri, *supra* note 319.

[326] Tene & Polonetsky, *supra* note 60, at 239.

[327] Joshua P. Meltzer, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, BROOKINGS (Apr. 12, 2017), https://www.brookings.edu/testimonies/global-digital-trade-1-market-opportunities-and-key-foreign-trade-restrictions/ [https://perma.cc/9RBB-HRHW].

[328] Edgar, *supra* note 9.

[329] Lewis, *supra* note 140.

[330] *See id.*

[331] *See* Council Regulation No. 697/2016/EC on the General Data Protection Regulation, 2016 O.J. L 119/1; Anderson-Fortson, *supra* note 144; *see also An In-Depth Examination of China's New Cybersecurity Law Part I: Who Must Comply?*, *supra* note 223 (discussing an in-depth analysis of China's CSL).

better accountability standards, and overall more protection for citizens and business.[332] However, policymakers should also recognize that the advances in technology can offer safer data but can still bolster the digital market.[333] Coordination between the WTO trading policies and a multilateral cybersecurity agreement will no doubt lead to complex and thorny discussions covering everything from infrastructure designs to state sovereignty rights.[334] However, the law does not exist in a vacuum.[335] Technology and public policy related to economics, liberty and the standard of living all implicate the development of relationships between nations.[336] As technology advances, the law must as well.[337]

---

[332] *See* Satola & Judy, *supra* note 252, at 1783.
[333] *See* MacDonald & Streatfeild, *supra* note 256, at 650.
[334] *Id.* at 652.
[335] Bergemann, *supra* note 322, at 629.
[336] *Id.*
[337] MacDonald & Streatfeild, *supra* note 256, at 652.