Indiana Law Journal

Volume 93 | Issue 4 Article 7

Winter 2018

Too-Big-To-Fail 2.0? Digital Service Providers

Nizan Geslevich Packin
Nizan.Packin@baruch.cuny.edu

Too-Big-To-Fail 2.0? Digital Service Providers as Cyber-Social Systems

NIZAN GESLEVICH PACKIN*

The security of communication networks and databases has become a main element of national security and economic competitiveness. Constant growth in information systems, financial technology, and e-commerce has improved efficiency and pushed economic growth. This growth has also made our society dependent on networked digital technologies and digital structures and devices, which facilitate, enhance, and scale most modern human endeavors. Consequently, the biggest digital service providers have become omnipotent, critical players in our economy that operate essential services and control how and where data is collected, stored, and handled. Recent attacks on information infrastructures such as the U.S. election system, which was designated a Critical Infrastructure in need of protection in 2017, as well as security breaches at institutions including key digital service providers, have caused concerns about these institutions' stability and standing. The breaches showed that in addition to a technical solution, a system-wide approach is needed to address these issues.

One particularly important aspect of such an approach relates to the elevated probability of some kind of failure, or disastrous malfunctioning, of key digital service providers—their services or their products—as a result of cyberattacks. This Article focuses on such potential failures or malfunctionings of nonfinancial institutions and of omnipotent, global digital service providers in particular, a scenario referred to here as "Too-Big-To-Fail 2.0," by way of an analogy to financial failures that can cause massive damage to society. The Article sheds light on this relatively unappreciated risk by comparing it to the (i) attempts of the Dodd-Frank Act to stop financial institutions from shifting the risks of too-big-to-fail externalities to society and (ii) laws protecting Critical Infrastructures. The Article is also greatly inspired by a recent European Union (EU) directive that deals with digital service providers. The Article serves as a call for action, arguing that, based on these comparisons and recent regulation, as well as other factors, key digital service providers should be defined as "Critical Service Providers" given their importance to our economy and society, and need to improve their risk management.

The Article explains why addressing Too-Big-To-Fail 2.0 has not yet become a political and societal priority. First, digital service providers are technology companies, which, many believe, are shaped by market forces such that they fail and succeed in equal measure without producing negative ripple effects on the economy or society. Second, technology giants are not as carefully regulated as banks because

---

* Nizan Packin is an Assistant Professor at Baruch College, City University of New York, an Affiliated Faculty at Indiana University Bloomington's Program on Governance of the Internet & Cybersecurity, and an Adjunct Professor at New York University. A special thanks to the members of the Minerva Center for the Rule of Law under Extreme Conditions and the Cyber Center at the University of Haifa, as well as the members of the Ostrom Cybersecurity & Internet Governance Colloquium, and Frederick Ding for helpful comments. Thanks also to David Skeel, Gideon Parchomovsky, George Triantis, Ariel Ezrachi, Tal Zarsky, Maayan Filmar, and Karni Shagal.

unlike banks, they do not take insured deposits backed by the government. Third, even heavily regulated financial institutions have not been required until recently to focus on cybersecurity. Finally, some believe that there is no point in worrying about Too-Big-To-Fail 2.0 as it is difficult to prepare for theoretical unknowns. Despite these arguments, however, the Article contends that given the factors outlined in the Critical Service Provider list of criteria, such as size, business involvement in multiple industry sectors, and impact on technology, the economy, and cyber-social systems, Too-Big-To-Fail 2.0 is a valid concern.

Recognizing this problem, the Article then calls for the design of a new systematic approach, resembling to a limited extent that of the Dodd-Frank Act, to understand which entities qualify as Critical Service Providers and why they should have enhanced risk management procedures. The Article proposes certain criteria to ground such an approach. Finally, the Article suggests that the companies designated as Critical Service Providers should be subject to some type of supervisory scrutiny, which would be the product of a collaborative private-public initiative and result in better risk management and internalizing.

INTRODUCTION

This Article focuses on the importance of key digital service providers to the American economy and society. The precedence for identifying certain goods or entities as "critical" to the United States first arose in the 1920s when dependence on foreign imports of certain materials was determined to be a vulnerability for the military. And while throughout the years more and more goods and entities were viewed

as potential American vulnerabilities that must be protected, only in recent years has the significance of data management and cybersecurity in this context become noticeable. This is largely because cyberattacks on leading institutions, governments, and private-sector businesses have become a frequent and constant growing threat. Consequently, the connection between security breaches and cyberattacks on key institutions and the likelihood of a catastrophic ripple effect on our technological, economic, and social development has become more real than ever. This is especially true given how relatively effortless it is to launch a broad-scale cyberattack, as was demonstrated on May 12, 2017, when attackers took advantage of Microsoft software vulnerabilities and disrupted operations in more than 150 countries.[1]

But May 12, 2017, is just one recent example. This connection has been demonstrated frequently over the last few years in various industries identified as critical infrastructure.[2] Nevertheless, information about the cyberattacks that impact American critical infrastructure, such as the number, type, and severity,[3] remains limited and unsophisticated. Covering both cyber-related and general threats, some laws have been put in place to protect critical infrastructure and its operators. This started with Congress's use of the term in Public Law 101-189, which defined "critical technologies" as "essential for the United States to develop to further the long-term national security or economic prosperity of the United States."[4] But existing

---

1. "We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems." *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 10 (2016) (statement of James R. Clapper, former Director of National Intelligence), http://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf [https://perma.cc/WJW9-69GB]; *see also* Dustin Volz & Eric Auchard, *More Disruptions Feared from Cyber Attack; Microsoft Slams Government Secrecy*, REUTERS (May 12, 2017, 10:38 AM), http://www.reuters.com/article/us-britain-security-hospitals-idUSKBN18820S [https://perma.cc/E2TN-AWVE] (describing how a "worm dubbed WannaCry—'ransomware' that [instantly] locked up more than 200,000 computers in more than 150 countries"—disrupted operations at car factories, hospitals, shops, and schools as it took advantage of Microsoft software vulnerabilities). Among the victims were Britain's National Health Service resulting in dozens of hospitals canceling their operations, FedEx in the United States, one of Germany's largest train operators, Russian banks, and more. Volz & Auchard, *supra* note 1. The "attack lost momentum . . . after a security researcher took control of a server connected to the outbreak, which crippled a feature that caused the malware to rapidly spread across infected networks." *Id.* "California-based cyber risk modeling firm Cyence [estimated] the total economic damage at $4 billion," and according to Microsoft's President Brad Smith, "governments around the world should 'treat this attack as a wake-up call' and 'consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits.'" *Id.*

2. For example, in recent years, hundreds of systems within the U.S. Department of Commerce were forced to disconnect from the internet due to cyberattacks. *See* Gregg Keizer, *Chinese Hackers Hit Commerce Department*, INFO. WK. (Oct. 6, 2006, 2:03 PM), http://www.informationweek.com/chinese-hackers-hit-commerce-department/d/did/1047684 [https://perma.cc/W6U7-MUSS].

3. Scott J. Shackelford & Zachery Bohm, *Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation*, 40 CAN.-U.S. L.J. 61, 63 (2016).

4. OFFICE OF SCI. & TECH. POLICY, NAT'L CRITICAL TECHS. REVIEW GRP., NATIONAL

U.S. regulations that attempt to identify and improve the stability of entities defined as critical, technology-based or not, including, since January 2017, the U.S. Department of Homeland Security's (DHS) designation of the election systems as critical infrastructure in the wake of increasing cyberattacks, do not cover all important service providers.[5] The regulations do not cover, for example, digital service providers.

Similar but unrelated to attempts to protect critical infrastructures, regulations have been proposed following the 2008 financial crisis to address the threat of potentially critical, major private-sector entities collapsing to the detriment of the markets, the economy, and all of society.[6] In particular, widespread public objection to the possibility of too-big-to-fail scenarios with societally harmful externalities led to the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act").[7] This act, which has been widely criticized for its ineffectiveness, focused on risk management at financial institutions and attempted to reflect the administrations' promise that, in the future, consumers would no longer be required to financially assist in solving private-sector, corporate behemoths' failures and malfunctionings.[8] Nevertheless, many commentators still argue that the failure of financial too-big-to-fail entities is unavoidable, that better risk management procedures are needed, and that the Dodd-Frank Act fails to offer a real solution to this problem.[9]

CRITICAL TECHNOLOGIES REPORT 163 (1995).

5. *See* Natalie Olivo, *DHS Says Election System Is 'Critical Infrastructure,'* LAW360 (Jan. 9, 2017, 3:38 PM), https://www.law360.com/privacy/articles/878619/dhs-says-election-system-is-critical-infrastructure-?nl_pk=5bceaabe-4b16-48ab-9db2-23250e5753d9&utm_source=newsletter&utm_medium=email&utm_campaign=privacy [https://perma.cc/M3TR-NTBD] ("According to Johnson's statement, this designation will place the infrastructure that makes up U.S. election systems—including polling places and voting machines—in the company of other critical infrastructure sectors that receive prioritized DHS cybersecurity attention. . . . 'Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems . . . . Election infrastructure is vital to our national interests, and cyberattacks on this country are becoming more sophisticated, and bad cyber actors—ranging from nation states, cybercriminals and hacktivists—are becoming more sophisticated and dangerous.' Johnson stressed that the critical infrastructure determination 'does not mean a federal takeover' concerning U.S. elections. Rather, he said, it allows DHS to prioritize cybersecurity assistance to state and local election officials."); Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013) (defining critical infrastructure); *see also What Is Critical Infrastructure?*, DEP'T OF HOMELAND SECURITY (Oct. 14, 2016), https://www.dhs.gov/what-critical-infrastructure [https://perma.cc/P7VG-TP5V]; Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 92, at 10–11 (Feb. 12, 2013) [hereinafter PPD-21].

6. *See generally* Nizan Geslevich Packin, *Supersize Them? Large Banks, Taxpayers and the Subsidies that Lay Between*, 35 NW. J. INT'L L. & BUS. 229 (2015).

7. Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified in scattered sections of Title XII of the United States Code).

8. *See, e.g.*, Annalyn Censky, *Obama on New Law: 'No More Taxpayer Bailouts,'* CNN (July 21, 2010, 12:46 PM), http://money.cnn.com/2010/07/21/news/economy/obama_signs_wall_street_reform_bill [https://perma.cc/6TVT-5AGW].

9. *See, e.g.*, Nizan Geslevich Packin, *The Case Against the Dodd-Frank Act's Living Wills: Contingency Planning Following the Financial Crisis*, 9 BERKELEY BUS. L.J. 29

Most commentators thus far have focused solely on the failure or malfunctioning associated with financial institutions in discussions of critical private-sector entities. This is partly because the 2008 crisis was the product of precisely this failure; crises are often followed by "bubble law"—misguided populist reactions that produce "quack" regulation with little empirical support. This reactionary legislation addresses the pitfalls of past crises rather than predicting new disastrous events, which are hypothetical, unimaginable, and sometimes referred to as "black swans."[10] Financial institutions are central to these regulatory attempts because they provide monetary services and credit. Indeed, their interconnectedness and reliance on government backing make them unique and more important to maintain than most entities, public or private. But while it is difficult to identify the potentially critical types of institutions to our economy and society before crises start, it is clear that other major entities, including nonfinancial ones such as technology companies, also provide key services to our society and economy. As Charles Perrow argues in his *Normal Accidents*, technology fails because systems complexity makes failure inevitable.[11] In particular, in the twenty-first century, social and economic stability has drastically depended on supporting secure ongoing organizational services, efficient and safe information management systems, and secure data based on networked digital technologies.

Size alone may not determine whether an entity is critical. For instance, politicians are less likely to receive much public interest or even support for preserving a gigantic business entity selling clothing brands with a vast consolidated assets portfolio, although technically such an organization's failure may inflict substantial risk to social stability beyond the financial sector. Other private-sector entities provide products and services on which we depend—they are fundamental to our lives today and deeply influence us. This Article argues that these entities include key digital service providers such as Google, Amazon, Apple, Facebook, and possibly Microsoft, and

---

(2012); Shahien Nasiripour, *No, Obama Didn't Kill Too Big To Fail*, HUFFPOST (Apr. 13, 2016, 8:29 PM), http://www.huffingtonpost.com/entry/obama-too-big-to-fail_us_570ec890e4b0ffa5937e242e [https://perma.cc/AGP6-TSJR].

10. *See* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE 274–85 (2d ed. 2010); Stephen M. Bainbridge, *Dodd-Frank: Quack Federal Corporate Governance Round II*, 95 MINN. L. REV. 1779, 1784 (2011); James Fanto, *Anticipating the Unthinkable: The Adequacy of Risk Management in Finance and Environmental Studies*, 44 WAKE FOREST L. REV. 731, 735–36 (2009); Karl S. Okamoto, *After the Bailout: Regulating Systemic Moral Hazard*, 57 UCLA L. REV. 183, 195–96 (2009); Larry E. Ribstein, *Bubble Laws*, 40 HOUS. L. REV. 77, 77–78 (2003); Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, 114 YALE L.J. 1521 (2005).

11. Charles Perrow, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES (1999). "Secretary Geithner told SIGTARP that he believed creating effective, purely objective criteria for evaluating systemic risk is not possible: 'What size and mix of business do you classify as systemic? . . . It depends too much on the state of the world at the time. You won't be able to make a judgment about what's systemic and what's not until you know the nature of the shock' the economy is undergoing." *Does the Dodd-Frank Act End "Too Big To Fail?": Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the H. Comm. on Fin. Servs.*, 112th Cong. 92 (2011) (statement of Christy Romero, Acting Special Inspector General, Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP)).

that they should be defined as "Critical Service Providers," because they provide vital and strategic functions and services to our society and economy. As such, a failure or disastrous malfunctioning of their services or products, not to mention their own potential failure, which is not only limited to a bankruptcy scenario, is likely to impose an immediate crisis of confidence as well as negative externalities on the general public.

This Article argues for this definition of Critical Service Providers not just because of the size and volume of these entities in the financial markets (equal to those of a midsize Western economy), but mainly because their power and importance stretch far beyond their mere scope. These entities have become extremely political as they reach levels of influence and impact that modern economies have never permitted even the largest financial institutions to reach[12] and redefine the very notions of politics and governance.[13] A recent example of this, was described in the November 2018 New York Times' exposé, which uncovered Facebook's attempts to dissemble its influence during the 2016 elections. Among those attempts was the use of a Republican-affiliated opposition research firm to retaliate against and discredit Facebook's critics, while disseminating negative stories about its competitors, in scope and scale that have never been seen before.[14]

Moreover, vertical and horizontal integration by these businesses is broader than ever and encompasses scientific innovations, media, computing, telecommunication, retail, and even financial services, over which the key digital service providers now compete with traditional financial service providers.[15] Additionally, leadership by

---

12. *See* Jeremy Ghez, *Why U.S. Tech Giants Might Not Dominate the World After All*, FORBES (Nov. 16, 2016, 11:37 AM), http://www.forbes.com/sites/hecparis/2016/11/16/why-us-tech-giants-might-not-dominate-the-world-after-all [https://perma.cc/VCZ6-E45H]. Similarly, in a series of papers from the last two years, Professor Maurice E. Stucke and Professor Ariel Ezrachi argue that, in the world of big data and artificial intelligence, network effects can fundamentally and forever change the way competition works in the digital economy and create barriers to entry, enabling big platforms to engage in behaviors such as collusion, tacit collusion, and price discrimination, to the detriment of consumers. In their scholarship, they discuss the changing dynamics of what they call the "digitized hand" and explain how the market in the ear of the digital economy may in fact appear to be more competitive than it really is. *See, e.g.*, ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016).

13. *See, e.g.*, Robert Epstein, *How Google Could Rig the 2016 Election*, POLITICO MAG. (Aug. 19, 2015), http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548 [https://perma.cc/DU2N-66W9]; Seth Fiegerman, *Facebook Is Well Aware that It Can Influence Elections*, CNN (Nov. 17, 2016, 11:33 AM), http://money.cnn.com/2016/11/17/technology/facebook-election-influence [https://perma.cc/2RWR-4D7G]; Issie Lapowsky, *Here's How Facebook* Actually *Won Trump the Presidency*, WIRED (Nov. 15, 2016, 1:12 PM), https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news [https://perma.cc/T96Z-6ZQ8].

14. Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg & Jack Nicas, *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html [https://perma.cc/5BLT-CQSV].

15. *See generally* Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data and Social Netbanks: Are You Ready to Replace Your Bank?*, 53 HOUS. L. REV. 1211 (2016).

key digital service providers in cloud services—software used by all major industries and even government agencies—is noteworthy[16] and may have alarming consequences in the context of cybersecurity, especially as dependence on cloud services continues to rise. Finally, overall impact by key digital service providers on our cyber-social systems is unmatched and only recently have scholars begun to examine it.[17]

Despite the above, and the massive externalities on the general public that potential failures associated with key digital service providers would impose, these entities' safety and stability are not yet a top regulatory priority. One explanation for this could be that some believe that digital service providers are technology companies, and as such it is only natural for them to come and go as part of the commonplace evolution of innovation, with the market forces correcting for unforeseen harms. But, as argued in this Article, while this might have been a convincing narrative in the past, when issues with technology companies mainly centered around anticompetitive behavior, this is no longer the case with the key digital service providers. Indeed, today's tech giants simply acquire and absorb any potential future competitors. These purchases also result in a chilling effect on funding of small startups, given the tech giants' potential ability to out-man, out-fund, and immediately compete with any new innovative players.[18] Likewise, while the failures or malfunctionings of key technology companies and their products might seem severe than that of key financial institutions, which are interconnected and rely on government backing, this

---

16. *See* Chris Neiger, *Too Big To Fail: Amazon Takes Aim at the Financial Services Cloud*, MOTLEY FOOL (Feb. 27, 2016, 2:00 PM), http://www.fool.com/investing/general/2016/02/27/too-big-to-fail-amazon-takes-aim-at-the-financial.aspx [https://perma.cc/AES9-7QUY].

17. For more on this point, see Stanford's new 2015 Cyber Initiative, which researches cyber-social systems and their impact on society. "Cyber-social systems" refers to "cyber technologies [that] interact with existing social systems." *Introduction to the Concept of Cyber-Social Systems*, STAN. CYBER INITIATIVE, https://cyber.stanford.edu/research-and-publications/introduction-concept-cyber-social-systems [https://perma.cc/592A-FLFG].

> Social systems comprise the various organizations of human activity, including transportation, markets, political arenas, and other communities. Cyber technologies encompass networked digital technologies—notably, the internet—and extend, for instance, to infrastructure control systems and wireless biomedical devices. Thus, cyber-social systems, both large and small, use embedded digital structures and devices to facilitate, enhance and scale human endeavors.

Id.

18. Professor Tim Wu describes it in the following way: "No one's willing to fund [profound innovation] because you're not going to displace Facebook or Google. So we go around the edges somewhere and try and find some cute little thing that doesn't bother anybody too much and get bought out. And so the movement to break away from the consumer welfare standard is growing. Sometimes called the New Brandeis movement, the idea is that the law should prioritize competition. It's the same sort of standard EU regulators have been using to crack down on big tech companies; these standards were originally based on the American approach under Brandeis and Roosevelt." Nilay Patel, *It's Time To Break Up Facebook*, VERGE (Sept. 4, 2018, 1:00 PM) (alteration in original) (internal quotation marks omitted), https://www.theverge.com/2018/9/4/17816572/tim-wu-facebook-regulation-interview-curse-of-bigness-antitrust [https://perma.cc/BB5Z-L9W9].

Article argues that there are also major concerns involved in failures related to key digital service providers.

Accordingly, the regulatory vacuum concerning key digital service providers is disturbing and should be addressed in a different legal framework as it is beyond the scope of this Article—as should these entities' liability and protection requirements against cyberattacks, given the dire potential risks and consequences for society. As Central Intelligence Agency (CIA) Director Leon Panetta stated in his secretary of defense confirmation testimony before the Senate Armed Services Committee, "[t]he next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[19] Since cybertechnologies encompass networked digital technologies that extend, for example, to infrastructure control systems, the potential risks associated with and horrific possible consequences of the failure of a key digital service provider have led some jurisdictions to regulate the risk management procedures of key digital service providers in the context of cybersecurity.[20] This is because cyberattacks can directly impact the stability of such entities. In recent years, even the largest, most sophisticated global institutions, including technology and media entities, such as Microsoft and Yahoo, have fundamentally failed to keep up with hackers who can cause detrimental breaches[21] relatively effortlessly and remotely.[22] Cybersecurity is a complex and multifaceted challenge that is constantly on the rise in its importance and impacts

---

19. For Leon Panetta's statement, see Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 233 (2016), http://ncjolt.org/wp-content/uploads/2016/12/Trautman_Final.pdf [https://perma.cc/TY2Y-DYRQ]. On August 8, 2016, the European Union's NIS Directive began to be enforced after it had been approved by the European Parliament on July 6, 2016. It includes key digital service providers in the list of regulated critical infrastructure entities. *See* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:194:FULL [https://perma.cc/YS36-63G4].

20. Trautman, *supra* note 19.

21. While the means of cyberattacks vary, the pattern of targets has been relatively consistent and mainly include large databases and point-of-sale systems, such as those of government agencies and political organizations (e.g., the U.S. Department of Homeland Security, the Federal Bureau of Investigation, the Democratic National Committee, the U.S. Department of the Treasury, and the Office of the Comptroller of the Currency); infrastructure operators; major banking institutions; technology companies (e.g., Oracle, Dropbox, Apple, and Yahoo); voting records; network management companies; and online social networks. *See, e.g.*, Damian Paletta, *Personnel Data Breach a 'Huge Deal*,*'* WALL ST. J., July 9, 2015, at A3 (reporting on the attack on the Office of Personnel Management); Riley Walters, *Cyber Attacks on U.S. Companies in 2016*, HERITAGE FOUND. (Dec. 2, 2016), http://www.heritage.org/research/reports/2016/12/cyber-attacks-on-us-companies-in-2016 [https://perma.cc/4MTU-3QQH].

22. For example, according to Verizon's 2016 data breach investigations report, "it took hackers minutes or less to compromise systems in ninety-three percent of the 2,260 breaches that Verizon analyzed, and the infiltrators were able to extract the data from the system within days in more than ninety-eight percent of the incidents." Allison Grande, *Data Breach Report Calls for Race To Catch Up with Hackers*, LAW360 (Apr. 26, 2016, 11:44 PM), http://www.law360.com/articles/789110/data-breach-report-calls-for-race-to-catch-up-with-hackers [https://perma.cc/9N9D-J84U].

more than financial institutions and government agencies, which are often mentioned in the media in that context.[23] Furthermore, cybersecurity is proving to be a cross-industry issue, although it appears that the financial sector players are currently ahead of all industries with their development of fraud and cybercrime prevention technology and operations.[24] This methodology will demand new proficiencies, including those that will fill gaps in the technology marketplace in an attempt to solve current information system challenges and to proactively use analytics when deciding real-time, risk-based issues.[25] The rise of the information society has created many opportunities for business entities to improve services to customers via new means and platforms. These means and platforms are more operationally efficient in terms of time and money. Moreover, this efficiency is rising while internet search is changing with digital personal assistants on the rise, and individuals that are distancing themselves from the junctions of decision making, putting their trust in the super platforms, enabling them more and more control of the interface.[26]

At the same time, hackers, criminals, and cyberterrorists are discovering new methods to take advantage of limitations and constantly strive to improve and update their attack schemes. Attackers keep searching for the weakest links in the information supply chain and often attempt to hack or harm entities and institutions by indirectly attacking related third parties or backdoor channels even when the organizations they are after have secure systems.[27] Third-party providers and websites are exposed to, maintain, and even carry large amounts of data about consumers, making them targets as well.[28]

---

23. For an analysis of "cybersecurity," as "a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions," see Lene Hansen & Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School,* 53 INT'L STUD. Q., 1155, 1155–75 (2009). For more on banking and cybersecurity, see SAS INST. INC., CYBERRISK IN BANKING: A REVIEW OF THE KEY INDUSTRY THREATS AND RESPONSES AHEAD (2013), http://www.kroll.com/media/pdf/white-papers/cyberrisk-in-banking-106605.pdf [https://perma.cc/K5XM-8U95]. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, originally only covered financial institutions and government computers, but "Congress has continuously broadened the scope and coverage of the CFAA through subsequent amendments in 1994, 1996, 2001, 2002, and 2008" including all computers in interstate (or international) commerce/communication. That history of the CFAA exactly demonstrates that far more people should care about cybersecurity. *See CFAA Background*, NACDL, https://www.nacdl.org/criminaldefense.aspx?id=34244 [https://perma.cc/UM7B-N79V].

24. SAS INST. INC., *supra* note 23.

25. *Id.*

26. NAVIGATING THE DIGITAL AGE: THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS 207–19 (2015), https://www.nyse.com/publicdocs/Navigating_The_Digital_Age.pdf [https://perma.cc/KE5W-UWCQ].

27. *Id.*

28. SAS INST. INC., *supra* note 23. Similarly, discussing the potential dangers associated with third party websites, and single sign-offs, a recent University of Illinois research paper found that hackers hacking into the tech giants can not only take over the accounts of the tech giants' users but also access third-party websites those users logged into with the tech giants, such as Facebook, Google, etc. The paper argues that once hackers accessed users' accounts they can then access "everything from people's private messages on Tinder to their passport

Battling this trend comes with a high price tag. Not only are the costs of crisis prevention and protection significant, but the cost to society as a whole of these attacks is on the rise, and the lack of global collaboration enables this trend to grow. This Article focuses on these issues from the perspective of key digital service providers, which have been somewhat overlooked in the United States in the context of a potential cyber-driven failure or malfunction and its conceivable, shocking consequences on the economy and society.

Advocating for the creation of a definition for Critical Service Providers, and the importance of enhancing such entities' risk management, this Article starts by explaining why the Too-Big-To-Fail 2.0 issue has not yet become a priority. First, digital service providers are technology companies, which many believe come and go with the market forces correcting for unforeseen harms that do not include negative ripple effects on the economy or society. Second, technology giants are not as carefully regulated as banks because, unlike banks, they do not take insured deposits backed by the government. Third, even financial institutions, which are heavily regulated, were not required, until recently, to focus on cybersecurity. Finally, some believe that there is no point in worrying about Too-Big-To-Fail 2.0, considering how difficult it is to prepare for theoretical unknowns. Nevertheless, the Article argues that after considering the issues outlined in the Critical Service Provider list of factors, such as size, businesses' vertical and horizontal integration, and impact on technology, economy, and cyber-social systems, Too-Big-To-Fail 2.0 appears to be a valid concern.

Recognizing this problem, the Article then calls for the design of a new systematic approach, partially inspired by recent EU regulation and resembling some of the features of the Dodd-Frank Act, to determine the entities that qualify as Critical Service Providers and who will categorize them as such. The Article proposes certain criteria to ground such an approach and addresses the undesired incentives that come into play when Critical Service Providers understand their importance and impact. Finally, the Article suggests that the companies designated as Critical Service Providers should be subject to some type of a supervisory scrutiny and regulation, which would preferably be the product of a collaborative private-public initiative.

The Article unfolds as follows: Part I briefly introduces the too-big-to-fail concept from its inception and the strategies used to address it to the entities that have been considered critical within its framework, focusing on the United States and the financial sector. Part II examines the connection between Critical Infrastructure Providers and Too-Big-To-Fail 2.0. Part III zooms in on key digital service providers, arguing that they should be viewed as Critical Service Providers. Part IV describes the challenges posed by cybersecurity in free economies, including some recent examples of breaches in the international technology sector, and examines how those challenges specifically affect the biggest global and omnipotent key digital service providers. It also discusses the potential consequences of such massive and lethal

---

information on Expedia, all without leaving a trace. Even more staggering: You could be at risk even if you've never used Facebook to log into a third-party site." Mohammad Ghasemisharif, Amruta Ramesh, Stephen Checkoway, Chris Kanich & Jason Polakis, *O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web*, August 15–17, 2018 https://www.cs.uic.edu /~polakis/papers/sso-usenix18.pdf [https://perma.cc/C3E2-2WHW].

cyberattacks and a possible too-big-to-fail scenario, while analyzing the issue of expectations within public choice theory. Part V surveys current regulations that could be relevant to cyberattacks, including those designed to address issues other than the failures of corporate giants or financial institutions. It also calls for a new systematic approach to determining who will designate Critical Service Providers, especially when changed circumstances might require this label to be applied to new, currently unimaginable entities, based on the Article's outlined criteria. A conclusion advocating for some scrutiny and regulation of Critical Service Providers follows.

I. TOO-BIG-TO-FAIL—THE FINANCIAL STORY

A. From 1984 Until the 2008 Crisis

In order to understand why key digital service providers should be associated with the concept of Too-Big-To-Fail, it is imperative to fully understand the concept itself. The term "Too-Big-To-Fail" was first coined in 1984, concerning the federal bank's intervention to prevent Continental Illinois National Bank from failing.[29] In the decades that followed, the public and the media gave some attention to the term.[30] During the financial crisis of 2008, the concept resurfaced once again: regulators announced that the U.S. government would provide capital to the top nineteen bank holding companies, if "stress tests" revealed that they could not raise it on their own.[31] The government ended up infusing more than $220 billion of capital into eighteen of those financial institutions, thus indicating that they were presumptively too-big-to-fail.[32] This happened after advocates from both sides of the political aisle agreed that these institutions must be saved, arguing that their failure would shake the economy and negatively impact society as a whole.[33]

The 2008 economic crisis and the bailouts that resulted from it were the products of a flawed and fragmented regulatory system operating with outdated notions of

---

29. *See* DAVID S. HOLLAND, WHEN REGULATION WAS TOO SUCCESSFUL—THE SIXTH DECADE OF DEPOSIT INSURANCE: A HISTORY OF THE TROUBLES OF THE U.S. BANKING INDUSTRY IN THE 1980S AND EARLY 1990S, at 37–51 (1998).

30. *See, e.g.*, Benton E. Gup, *Are Fannie Mae and Freddie Mac Too Big To Fail?*, *in* POLICIES AND PRACTICES IN GOVERNMENT BAILOUTS 285, 310 (Benton E. Gup ed., 2004); Lawrence A. Cunningham, *Too Big to Fail: Moral Hazard in Auditing and the Need to Restructure the Industry Before It Unravels*, 106 COLUM. L. REV. 1698, 1726–27 (2006); Helen A. Garten, *Banking on the Market: Relying on Depositors to Control Bank Risks*, 4 YALE J. ON REG. 129, 146 (1986); Jeffrey E. Garten, Opinion, *Too Big To Fail*, N.Y. TIMES (Sept. 26, 1997), http://www.nytimes.com/1997/09/26/opinion/too-big-to-fail.html [https://perma.cc/7GZU-53Z5].

31. *See* Packin, *supra* note 9, at 33 n.11.

32. Arthur E. Wilmarth, Jr., *Reforming Financial Regulation To Address the Too-Big-To-Fail Problem*, 35 BROOK. J. INT'L L. 707, 713 (2010).

33. *See generally* Packin, *supra* note 9.

systemic risk.[34] In the aftermath of the financial crisis, rating agencies,[35] regulators,[36] global organizations,[37] and academics[38] made the argument that the largest financial institutions enjoy competitive advantages[39] because the market perceives them as likely to be saved in future financial crises.[40] This perception is also anchored in the

---

34. Professor Steven Schwarcz defines systemic risk as "the risk that (i) an economic shock such as market or institutional failure triggers (through a panic or otherwise) either (X) the failure of a chain of markets or institutions or (Y) a chain of significant losses to financial institutions, (ii) resulting in increases in the cost of capital or decreases in its availability, often evidenced by substantial financial-market price volatility." Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 204 (2008).

35. *See, e.g.*, STANDARD & POOR'S, BANKS: RATING METHODOLOGY AND ASSUMPTIONS 11 (2011), http://img.en25.com/Web/StandardandPoors/BanksRatingMethodology_Final110911.pdf [https://perma.cc/RU7W-N6RP].

36. Former Federal Reserve Chairman Ben Bernanke said that new regulations aim to end the need for subsidies. *See* Christopher Ryan, *Elizabeth Warren: Too-Big-To-Fail Banks Get $83bn/year Subsidy. Why?*, AM. BLOG (Feb. 28, 2013, 12:41 PM), http://americablog.com/2013/02/elizabeth-warren-83bn-bank-subsidy.html [https://perma.cc/45ZZ-7V77].

37. *See, e.g.*, Gara Afonso, João A. C. Santos & James Traina, *Do "Too-Big-To-Fail" Banks Take on More Risk?*, 20 FED. RES. BANK N.Y. ECON. POL'Y REV. 41, 42 (2014), https://www.newyorkfed.org/medialibrary/media/research/epr/2014/1412afon.pdf [https://perma.cc/G94H-3B3W] (finding that the biggest banks rely on the government to save them); Kenichi Ueda & Beatrice Weder di Mauro, *Quantifying Structural Subsidy Values for Systemically Important Financial Institutions* (Int'l Monetary Fund, Working Paper No. WP/12/128, 2012), http://www.imf.org/external/pubs/ft/wp/2012/wp12128.pdf [https://perma.cc/2MQS-998P].

38. "The largest financial institutions . . . are able to borrow money much more cheaply than other financial institutions, because their cost of credit is artificially reduced by the Too Big to Fail subsidy." *Who Is Too Big To Fail: Does Title II of the Dodd-Frank Act Enshrine Taxpayer-Funded Bailouts?: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Fin. Servs.*, 113th Cong. 4 (2013), http://financialservices.house.gov/uploadedfiles/hhrg-113-ba09-wstate-dskeel-20130515.pdf [https://perma.cc/3UFS-YRUS] (written testimony of David A. Skeel, Jr., Professor, University of Pennsylvania Law School); *see also* Bryan Kelly, Hanno Lustig & Stijn Van Nieuwerburgh, *Too-Systemic-To-Fail: What Option Markets Imply About Sector-Wide Government Guarantees*, 106 AM. ECON. REV. 1278 (2016) (supporting the idea that there is a too-big-to-fail subsidy).

39. Such competitive advantages include Title II of the Dodd-Frank Act authorizing the Federal Deposit Insurance Corporation (FDIC) to create a bridge institution that can be kept in place for up to five years, during which institutions receive tax-free status. *See* 12 U.S.C.A. § 5390(h)(10) (West 2014). This advantage is clearly an indication that Title II does impose costs on taxpayers.

40. *See, e.g.*, Anat R. Admati, Peter M. DeMarzo, Martin F. Hellwig & Paul Pfleidere, *Fallacies, Irrelevant Facts, and Myths in the Discussion of Capital Regulation: Why Bank Equity Is Not Socially Expensive* 1–7 (Stanford Univ. Rock Ctr. for Corp. Governance, Working Paper No. 161, 2013), https://ssrn.com/abstract=2349739 [https://perma.cc/3AE4-MFSC]; Viral V. Acharya, Deniz Anginer & A. Joseph Warburton, The End of Market Discipline? Investor Expectations of Implicit Government Guarantees 3–4, 13 (May 1, 2016) (unpublished manuscript), https://ssrn.com/abstract=1961656 [https://perma.cc/45DQ-ST5H] (arguing that big banks borrow funds at lower costs from private lenders because the implicit guarantees reduce the amount of big banks' credit risk in comparison to smaller banks).

Dodd-Frank Act's regulation of systemically important financial institutions (SIFIs),[41] as described below.

The catchy term too-big-to-fail is usually mentioned in the context of SIFIs, but it is not just banks' failure that this regulatory principle governs. Historically, different types of important service providers have been viewed as too important to fail.[42] Three notable examples include the 1930s railroads operation because of their critical infrastructure functions and role in the overall economy,[43] California's multibillion-dollar bailout of Pacific Gas & Electric Company approved by a federal court,[44] and the post-9/11 Air Transportation Safety and System Stabilization Act, which the U.S. Congress passed to provide the airline industry with financial aid.[45] In these cases, the externalities of potential failure of these nonfinancial institutions would have taken too great a toll on society.

But beyond consumers' financial support for critical entities, in 2008, the too-big-to-fail issue altered the entities' behavioral incentives and ethical standards. In the years since the financial crisis, one of the perverse effects of the too-big-to-fail problem has been revealed: the government's inconsistent or lax disciplinary approach towards important financial institutions that fail to comply with the law.[46] This policy was nicknamed "too-big-to-jail"; as then-attorney general Eric Holder explained it, the Department of Justice (DOJ) could not indict systemic institutions out of fear of the "collateral consequences" of economic harm.[47] This policy, evident in

---

41. Pursuant to the Dodd-Frank Act, SIFIs are institutions that are so essential to the U.S. financial system that their failure would cause traumatic damage to the financial markets, as well as the entire economy. Nevertheless, it is not clear if all SIFIs must be defined as such, or only those whom the FSOC believes are required to do so. *Compare* Dodd-Frank Wall Street Reform and Consumer Protection Act §113(a)(1), 12 U.S.C. § 5323(a)(1) (2012) (using the term "may"), *with id.* § 112(a)(2)(H), 12 U.S.C. § 5322(a)(2)(H) (indicating a requirement).

42. *See, e.g.*, Shlomit Azgad-Tromer, *Too Important To Fail: Bankruptcy Versus Bailout of Socially Important Non-Financial Institutions*, 7 HARV. BUS. L. REV. 159 (2017).

43. Joseph R. Mason & Daniel A. Schiffman, *Too Big To Fail, Government Bailouts, and Managerial Incentives: The Case of the Reconstruction Finance Corporation Assistance to the Railroad Industry During the Great Depression*, *in* TOO BIG TO FAIL: POLICIES AND PRACTICES IN GOVERNMENT BAILOUTS 49, 49–54 (Benton E. Gup ed., 2004).

44. *Judge Approves PG&E Bailout*, WALL ST. J. (Dec. 23, 2003), https://www.wsj.com/articles/SB107214516968910000 [https://perma.cc/22CB-3VH7].

45. Air Transportation Safety and System Stabilization Act, Pub. L. No. 107-42, 115 Stat. 230 (2001) (codified at 49 U.S.C. § 40101 (2012)); *see also* Margaret M. Blair, *The Economics of Post-September 11 Financial Aid to Airlines*, 36 IND. L. REV. 367 (2003).

46. *See generally* Nizan Geslevich Packin, *Breaking Bad? Too-Big-To-Fail Banks Not Guilty as Not Charged*, 91 WASH. U.L. REV. 1089 (2014).

47. *Oversight of the U.S. Department of Justice: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013) (statement of Eric. H. Holder, Jr., Att'y Gen. of the United States), https://fas.org/irp/congress/2013_hr/hjc-doj.pdf [https://perma.cc/K35H-V6QF]; *Who Is Too Big To Fail: Are Large Financial Institutions Immune from Federal Prosecution?: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Fin. Servs.*, 113th Cong. 6 (2013) (statement of Mythili Raman, Acting Assistant Att'y Gen., Criminal Division, Department of Justice).

JPMorgan's $13 billion settlement in 2013 with the government for the bank's responsibility in the 2008 crisis, has been criticized as undermining the rule of law.[48] Despite the U.S. government's insistence that it does not release anyone from potential prosecution, most settling entities have received deferred or nonprosecution agreements and eventually avoided indictment or convictions. Further evidence of this practice came in July 2016, when it was revealed that Britain's chancellor, George Osborne, and the United Kingdom's former financial watchdog, the Financial Services Authority, "obstructed" the 2012 U.S. investigation into HSBC's money laundering and contributed to watering down the bank's punishment.[49]

Allowing important institutions to escape legal liability has created a major problem—the public perception of bias in the legal system and favorable prosecutorial treatment of institutions with large numbers of employees and shareholders and great economic impact,[50] and indictments for the economically weak but not for the economically powerful.[51] Accordingly, given that the too-big-to-jail policy incentivizes unethical behavior, it can be argued that it encourages unwelcome business practices and maybe even criminality.[52] Certainly, a simple cost-benefit analysis shows that fines for an illegally obtained profit can be paid off by committing more illegal activities in the future, for which the fined entities and their executives are unlikely to be held accountable.

The too-big-to-jail issue is not unique to the financial sector.[53] Several years after the financial crisis, these public perceptions of bias began to crop up in the media again, this time in connection with key digital service providers. The public was responding to several reports of potential corporate malfeasance, including a Federal Trade Commission (FTC) probe of Google's business practices that produced no evidence of wrongdoing, despite media reports that the FTC had accidentally disclosed

---

48. *See Wall Street Fraud and Fiduciary Duties: Can Jail Time Serve as an Adequate Deterrent for Willful Violations?: Hearing Before the Subcomm. on Crime & Drugs of the S. Comm. on the Judiciary*, 111th Cong. 127–29 (2010) (statement of James K. Galbraith, Lloyd M. Bentsen, Jr., Chair in Government/Business Relations, Lyndon B. Johnson School of Public Affairs, University of Texas at Austin); Court E. Golumbic & Albert D. Lichy, *The "Too Big To Jail" Effect and the Impact on the Justice Department's Corporate Charging Policy*, 65 HASTINGS L.J. 1293, 1322 (2014); Letter from Senator Jeffrey A. Merkley to Eric Holder, Att'y Gen., Dep't of Justice (Dec. 13, 2012), https://www.merkley.senate.gov/news/press-releases/merkley-blasts-too-big-to-jail-policy-for-lawbreaking-banks [https://perma.cc/4FPM-Q6KG].

49. Rupert Neate, *HSBC Escaped US Money-Laundering Charges After Osborne's Intervention*, GUARDIAN (July 11, 2016, 3:36 PM), https://www.theguardian.com/business/2016/jul/11/hsbc-us-money-laundering-george-osborne-report [https://perma.cc/8RYJ-K454].

50. Sharon E. Foster, *Too Big To Prosecute: Collateral Consequences, Systematic Institutions and the Rule of Law*, 34 REV. BANKING & FIN. L. 655, 658 (2015).

51. *Id.*

52. *See* Oscar Williams-Grut, *Too Big to Jail: George Osborne Helped HSBC Avoid US Criminal Charges For Money Laundering*, BUS. INSIDER (July 12, 2016, 3:28 AM), http://uk.businessinsider.com/hsbc-too-big-to-jail-report-george-osborne-letter-warned-of-financial-contagion-if-bank-prosecuted-2016-7 [https://perma.cc/BL7V-XQAE].

53. *See, e.g.*, BRANDON L. GARRETT, TOO BIG TO JAIL: HOW PROSECUTORS COMPROMISE WITH CORPORATIONS (2014) (arguing that federal prosecutions have involved many different types of large public corporations, including Google).

evidence of Google's anticompetitive behavior. After enraged public reactions to and much media coverage of the story, FTC leaders allowed Google to make voluntary changes to its practices rather than face a lawsuit.[54]

Governments can do much more for key private-sector institutions than avoid prosecutions when dealing with them. Government subsidies can impact business practices and increase or decrease productivity in order to advance social or economic interests and avoid major economic harms. Unfortunately, subsidies both create and eliminate undesired incentives, which result in unintended consequences.[55] For instance, the government's approach to the banking sector inadvertently encouraged institutions to (i) borrow much more, (ii) take excessive risks, and (iii) expand into various unrelated industries.[56]

B. No More Too-Big-To-Fail?

Public awareness of the government's favorable treatment of too-big-to-fail entities has risen drastically in recent years. In particular, attention has spiked in the wake of the $11 trillion of assistance to financial institutions and more than $6 trillion in economic stimulus programs spent by the United States, the United Kingdom, and the EU.[57] Given the harsh economic and social consequences of the failure of a megainstitution, observers have argued that the best way to address the too-big-to-fail problem is to break up such institutions.[58] One of the commentators, Alan Greenspan, said that "[i]f they're too big to fail, they're too big."[59]

---

54. *See, e.g.*, Benjamin Edelman, *Does Google Leverage Market Power Through Tying and Bundling?*, 11 J. COMPETITION L. & ECON. 365 (2015) (examining Google's pattern and practice of leveraging its dominance in order to enter new markets, compel usage of its services, and dominate competing offerings); Ryan Lynch, *Why Google Felt Lucky at FTC*, FORBES (Mar. 31, 2015, 3:05 PM), http://www.forbes.com/sites/mergermarket/2015/03/31/why-google-felt-lucky-at-ftc [https://perma.cc/8PEU-UABZ]; Rick Rule, *FTC's Pass on Google Opens the Door for the Justice Department*, U.S. NEWS (Jan. 9, 2013, 9:00 AM), http://www.usnews.com/opinion/articles/2013/01/09/ftcs-pass-on-google-opens-the-door-for-the-justice-department [https://perma.cc/UFJ9-EWDD]. The FTC also declined to take action in its response to Google Street View, even as multiple state attorneys general and foreign regulators cracked down on the same Google practices. *See Investigation of Google Street View*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/streetview [https://perma.cc/KS2A-QLYL].

55. For examples of such unintended consequences in different industries, see Packin, *supra* note 6.

56. *Id.*

57. *See* FED. DEPOSIT INS. CORP., TBTF SUBSIDY FOR LARGE BANKS—LITERATURE REVIEW (2013), https://www.fdic.gov/news/news/speeches/litreview.pdf [https://perma.cc/5ZZ8-WM27].

58. Commentators agree that "catastrophic risks are difficult to identify and their consequences in the complex financial institutions are almost impossible to predict." James A. Fanto, *Financial Regulation Reform: Maintaining the Status Quo*, 35 BROOK. J. INT'L L. 635, 653 (2010).

59. *Greenspan Calls to Break Up Banks 'Too Big To Fail,'* N.Y. TIMES (Oct. 15, 2009, 3:48 PM), http://dealbook.nytimes.com/2009/10/15/greenspan-break-up-banks-too-big-to-fail/?_r=0 [https://perma.cc/HQ4M-G69S].

Attempting to address the problems that caused the financial crisis and resolve the too-big-to-fail problem, lawmakers have sought significant regulatory reform. The Dodd-Frank Act was signed into law on July 21, 2010; *inter alia*, it authorizes regulators to take certain actions to reduce both the likelihood that a large financial company will fail and the impact of any such failure. It also turns the Federal Reserve into a "super regulator" for a number of financial conglomerates, including previously unregulated financial entities,[60] creates new regulatory agencies such as the Financial Stability Oversight Council (FSOC) to monitor financial institutions,[61] and tasks multiple agencies with supervising different parts of the financial system.[62] Finally, as President Obama declared upon its enactment, the Dodd-Frank Act attempts to solve the too-big-to-fail problem and avoid foisting its costs onto society.[63] This was meant to ensure that the U.S. government would never again provide funds

---

60. Together, these financial entities are referred to as the "shadow banking system." For more on the shadow banking system, see Gary Gorton & Andrew Metrick, *Regulating the Shadow Banking System*, BROOKINGS PAPERS ON ECON. ACTIVITY (2010), https://www.brookings.edu/bpea-articles/regulating-the-shadow-banking-system-with-comments-and-discussion [https://perma.cc/UC2S-THC2] (arguing that although the shadow banking system greatly contributed to the recent financial crisis, it remains relatively unregulated even after the enactment of the Dodd-Frank Act).

61. Pursuant to section 111 of the Dodd-Frank Act, 12 U.S.C.A. § 5321 (West 2014), the FDIC Board of Directors approved a joint Notice of Proposed Rulemaking (NPR) on March 29, 2011, for covered systemic organizations to file and report resolution plans and credit exposure reports. 76 Fed. Reg. 22,648 (proposed Apr. 22, 2011) [hereinafter FDIC's NPR]. On September 13, 2011, the FDIC Board of Directors approved a final rule to be issued jointly by the FDIC and the Federal Reserve Board to implement section 165(d) of the Dodd-Frank Act, 12 U.S.C.A. § 5365(d), laying out what the largest and most complex financial firms must include in living wills. The final rule became effective November 30, 2011. *See* Resolution Plans Required, 76 Fed. Reg. 67,323 (Nov. 1, 2011) (codified at 12 C.F.R. pts. 243, 381).

62. For example, on September 13, 2011, the FDIC Board of Directors approved a complementary Interim Final Rule under the Federal Deposit Insurance Act to require insured depository institutions with $50 billion or more in total assets to submit periodic contingency plans to the FDIC for resolution in the event of the depository institution failure. *See* Special Reporting, Analysis and Contingent Resolution Plans at Certain Large Insured Depository Institutions, 75 Fed. Reg. 27,464 (proposed May 17, 2010) (to be codified at 12 C.F.R. pt. 360); Press Release, FDIC, FDIC Board Approves Interim Final Rule Requiring Resolution Plans for Insured Depository Institutions Over $50 Billion (Sept. 13, 2011), http://www.fdic.gov/news/news/press/2011/pr11150.html [https://perma.cc/GX89-SBQA].

63. *See Regulating and Resolving Institutions Considered "Too Big To Fail:" Hearing Before the S. Comm. on Banking, Hous. & Urban Affairs*, 111th Cong. 5 (2009) (statement of Gary H. Stern, President & CEO, Fed. Reserve Bank of Minneapolis), http://www.minneapolisfed.org/news_events/pres/sterntestimony05-06-09.pdf [https://perma.cc/KV9D-H7KE]; Cheryl D. Block, *Overt and Covert Bailouts: Developing a Public Bailout Policy*, 67 IND. L.J. 951, 991 (1992) ("The first justification for the presumption against bailout is that government intervention to protect private industry violates the free-market principles that generally govern our economy.").

like the $1.525 trillion given through the Troubled Asset Relief Program (TARP)[64] and the Stimulus Package,[65] covered by taxpayer money,[66] in addition to ongoing government-assisted financial support to too-big-to-fail financial institutions.[67]

The Dodd-Frank Act also includes an enhanced supervisory scheme for SIFIs, pursuant to which the largest nonbank financial companies and bank holding companies require special monitoring and supervisory schemes.[68] To monitor, reduce, and ideally prevent risk, the Dodd-Frank Act requires that SIFIs prepare "break the glass" reorganization plans,[69] commonly known as "living wills,"[70] and submit them for review to the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), and the FSOC.[71] These living wills, which are, in essence, hypothetical

---

64. Emergency Economic Stabilization Act of 2008 (EESA), Pub. L. No. 110-343, 122 Stat. 3765 (codified as amended at 12 U.S.C. § 5201 (2012)). EESA helped establish the TARP, which enabled the Treasury to purchase or guarantee up to $700 billion in troubled assets that were owned by financial institutions. *See id.*

65. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified as amended at 26 U.S.C. § 1 (2012)).

66. *See* Joel Achenbach, *A Sense of Resentment Amid the 'For Sale' Signs*, WASH. POST (Sept. 22, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/09/21/AR2008092102534.html [https://perma.cc/S3LY-TSBC]; Jonathan Weber, *The Wall Street Bailout: What About Main Street?*, NEWWEST (Sept. 23, 2008), http://www.newwest.net/topic/article/what_does_the_wall_st_bailout_mean_for_you/C35/L35 [https://perma.cc/BC98-3BSD].

67. The U.S. Department of the Treasury website provides details on programs supplying continued capital to financial institutions. *Financial Stability*, U.S. DEP'T TREASURY, http://www.treasury.gov/initiatives/financial-stability/Pages/default.aspx [https://perma.cc/CBD8-9DTV].

68. 12 U.S.C.A. § 5365(d)(1) (West 2014). Indeed, pursuant to the Final Rule, the law "applies to any bank holding company that has $50 billion or more in total consolidated assets." Final Rule for Federal Reserve System and Federal Deposit Insurance Corporation, 76 Fed. Reg. 67,323, 67,326 (Nov. 1, 2011) (to be codified at 12 C.F.R. pts. 243, 381); *see also* 12 C.F.R. § 381.2(f) (2017) (defining "covered company").

69. *See* 12 U.S.C.A. § 5365(d)(1). Pursuant to the FDIC's NPR and the Final Rule, "[r]apid and orderly resolution" means "reorganization or liquidation of the covered company . . . under the Bankruptcy Code." 12 C.F.R. § 381.2(o) (2017).

70. These plans are named after the "traditional" living wills—legal schemes that provide for a patient's wishes concerning the use of specific life-sustaining treatments after the onset of that patient's terminal disease or another catastrophic accident. *See, e.g.*, Patrick Webster, *Enforcement Problems Arising from Conflicting Views of Living Wills in the Legal, Medical and Patient Communities*, 62 U. PITT. L. REV. 793, 793 (2001).

71. 12 U.S.C.A. § 5365(d)(3)–(5); Final Rule for Federal Reserve System and Federal Deposit Insurance Corporation, 76 Fed. Reg. 67,323. Accordingly, in July 2012, nine of the world's biggest financial institutions submitted to the U.S. regulators and gave the public a peek at their living wills as requested. *See* Jessica Holzer, *Banks' "Living Wills" Unveiled*, WALL ST. J. (July 3, 2012; 4:19 PM), https://www.wsj.com/articles/SB10001424052702304211804577505011956447968 [https://perma.cc/R6MC-WMJZ].

restructuring plans, mandate that each SIFI[72] internally manage and better monitor its business risks and report periodically on noteworthy changes or risks.[73]

II. CRITICAL INFRASTRUCTURE

A. Critical Infrastructure Operators

While the Dodd-Frank Act focuses on regulating financial institutions, especially those that are systemically important, other nonfinancial institutions have also been found to be politically, economically, and socially critical. According to the USA PATRIOT Act,[74] critical infrastructure operators provide the essential services that underpin our modern society and serve as the backbone of our economy, security, and health.[75] In 1998, the Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, set forth the roles, responsibilities, and objectives for protecting the nation's utility, transportation, financial, and other essential infrastructure.[76] It identified activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil, and gas production; and storage. In addition, the PDD identified four activities in which the federal government controls critical infrastructure: (1) internal security and federal law enforcement, (2) foreign intelligence, (3) foreign affairs, and (4) national defense.

Similar to too-big-to-fail entities, critical infrastructure entities are so important that the government believes that their incapacitation or destruction would have a devastating effect on the country's "security, national economic security, national public health or safety, or any combination of those matters."[77] Attempting to better protect our critical infrastructures, since 1998, the different administrations added authorities directing federal government efforts to protect and manage related risks, including Executive Order (EO) 13,636,[78] and the Obama administration's PPD-21

---

72. "FDIC officials said 124 banks would be subject to the rule, 26 of which are U.S. bank holding companies. The rest are subsidiaries of foreign-owned banks." Victoria McGrane & Alan Zibel, *FDIC Drafts Rule on "Living Wills" for Banks*, WALL ST. J. (Mar. 29, 2011, 5:31 PM), http://online.wsj.com/article/SB10001424052748704559904576230842703099306.html [https://perma.cc/8YUX-KSZQ].

73. *See* 12 U.S.C.A. § 5365(d)(2).

74. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended at 18 U.S.C. § 1).

75. *See id.* § 1016(e); 42 U.S.C.A. § 5195c(e) (West 2014).

76. *See* Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804 (May 22, 1998).

77. PPD-21, *supra* note 5.

78. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, *supra* note 5.

from February 12, 2013,[79] which superseded other authorities issued during the George W. Bush administration. PPD-21 ordered an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability. It also called for an update of the National Infrastructure Protection Plan, and a new research and development plan for Critical Infrastructure, to be updated every four years.[80] Finally, the Trump administration also issued an executive order in May 2017 instructing agencies to proactively assess cybersecurity risks and share threat information in order to better safeguard federal networks and infrastructure.[81] Trumps' EO brings the government closer to an approach long embraced by the private sector and ramps up liability risks for companies that have yet to embrace the practices. It followed the budget deal passed by congressional leaders on April 30, 2017, which boosted funding for cybersecurity and privacy initiatives at the DHS and the FTC, including the allocation of nearly $1 billion to help fortify public-sector networks against cyberattacks.[82] This is especially helpful, as the DHS's National Protection and Programs Directorate's Office of Infrastructure Protection (IP) leads the coordinated national effort to manage risks to the nation's critical infrastructure and enhance the security and resilience of America's physical and cyberinfrastructure.[83]

---

79. PPD-21, *supra* note 5.

80. RITA TEHAN, CONG. RESEARCH SERV., CYBERSECURITY: CRITICAL INFRASTRUCTURE AUTHORITATIVE REPORTS AND RESOURCES (2016), *reprinted in Congressional Research Service [CRS] Reports*, FED'N AM. SCIENTISTS, https://fas.org/sgp/crs/misc/R44410.pdf [https://perma.cc/4TBL-FVN5].

81. *See* Exec. Order No.13,228 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,* 82 Fed. Reg. 32,172 (May 11, 2017); Press Release, U.S. Dep't of Homeland Sec., President's Executive Order Will Strengthen Cybersecurity for Federal Networks and Critical Infrastructure (May 11, 2017), https://www.dhs.gov/news/2017/05/11/president-s-executive-order-will-strengthen-cybersecurity-federal-networks-and [https://perma.cc/VCS2-7YPZ] (according to the EO, the NIST Cybersecurity Framework will be a guide for managing cybersecurity risks for government agencies and critical infrastructure businesses, and DHS must engage with owners and operators of the nation's critical infrastructure to identify how agencies can support cybersecurity efforts and report to the President within 180 days on findings and recommendations for better supporting critical infrastructure entities).

82. Allison Grande, *DHS, FTC Cybersecurity Efforts Get Lift with Spending Deal*, LAW360, (May 1, 2017, 8:03 PM), https://www.law360.com/articles/919078/dhs-ftc-cybersecurity-efforts-get-lift-with-spending-deal [https://perma.cc/X999-2J9N].

83. U.S. DEP'T OF HOMELAND SEC., OFFICE OF INFRASTRUCTURE PROTECTION FACT SHEET (2017), https://www.dhs.gov/publication/ip-fact-sheet [https://perma.cc/B9Q4-P4R7].

B. Cybersecurity and Critical Infrastructure

Despite its various legal authorities, U.S. critical infrastructure entities are not well protected and are under constant attack.[84] Sophisticated cyberattacks[85] in particular have been on the rise in recent years.[86] And while U.S. policy makers have long agreed that critical infrastructure sectors should be better protected against cyber risks, as all sectors rely to some extent on computers, networks, and automated systems,[87] the regulators have yet to put clear legal cybersecurity principles in place, although other jurisdictions, including China and the EU have recently done so.[88]

---

84. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013).

85. *Cybersecurity Threats Impacting the Nation: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt. of the H. Comm. on Homeland Sec.*, 112th Cong. 3 (2012) (statement of Gregory C. Wilshusen, Director of Information Security Issues, Government Accountability Office); AMIT AGRAWAL & JACK LAWSON, U.S. EXECUTIVE ORDER 13636 AND CRITICAL SECURITY CAPABILITIES TO CONSIDER 3 (2014), http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/critical-security-capabilities-paper.pdf.

86. Shane Tews & James Cunningham, *The Road Ahead for Cybersecurity*, AM. ENTERPRISE INST. (June 16, 2014, 6:00 AM), http://www.techpolicydaily.com/technology/road-ahead-cybersecurity [https://perma.cc/D7BP-C434].

87. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., RECOMMENDED PRACTICE: DEVELOPING AN INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY INCIDENT RESPONSE CAPABILITY iii (2009), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf [https://perma.cc/89WD-WDAD].

88. ERIC A. FISCHER, CONG. RESEARCH SERV., FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 2–3 (2013), *reprinted in Congressional Research Service [CRS] Reports*, FED'N AM. SCIENTISTS, https://www.fas.org/sgp/crs/natsec/R42114.pdf [https://perma.cc/VMK5-WQ6U]; Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 377 (2015); Chris Laughlin, Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach To Ensure Inevitable Laws and Regulations Are Effective*, 14 COLO. TECH. L.J. 346, 354 (2016) (stating that "[f]rom 2009 through 2014, over 110 bills and resolutions were introduced in Congress related to cybersecurity," but each failed to pass, and even the legislation that passed in 2014 and 2015 "is insufficient either because it does not directly address critical infrastructure cybersecurity or because it does so inadequately for the changing cybersecurity landscape"); Karen Epper Hoffman, *Following the Framework: Government Standards*, SC MAG. (June 2, 2014), https://www.scmagazine.com/following-the-framework-government-standards/article/540122 [https://perma.cc/F9Z5-X7VX]. For a discussion on the EU, see below. As for China, the Chinese legislature passed a new cybersecurity law in November 2016 that went into effect on June 1, 2017, after public consultation on several previous drafts of the legislation. The cybersecurity law has a wide scope and contains provisions relating to both privacy and cybersecurity. Many of the law's key provisions apply to two types of companies: "network operators" and "critical information infrastructure" (CII) providers, which includes companies that provide services that, if lost or destroyed, would damage Chinese national security or the public interest. These broad definitions led to much criticism from American tech giants, such as Microsoft, Google, and Amazon, which view this law as an attempt to get their source code and an advantage over them, rather than a means to increase security. *See* Courtney M. Bowman, Ying Li & Lijuan Hou, *A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization*,

This is a serious failure on the part of legislators given that the scale of potential damage is high[89] and attackers have already targeted critical infrastructure institutions.[90]

After Congress's attempts to pass cybersecurity legislation failed, President Obama, as mentioned above, issued several directives and executive orders, attempting to enhance the currently insufficient patchwork of cybersecurity laws and regulations governing U.S. national security.[91] In early 2013, President Obama issued EO 13,636,[92] which included numerous provisions meant to improve the security and resiliency of critical infrastructure sectors, including a directive for the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework to reduce cyber risks to critical infrastructure.[93] Then, in early 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* ("NIST Framework"),[94] which provided a structure for the existing principles and standards.[95] The Cybersecurity Enhancement Act of 2014[96] directed NIST to coordinate American agencies to work with other jurisdictions to create international cybersecurity principles.[97] Additionally, in December 2015, Congress included the

---

Privacy Law Blog, PROSKAUER LLP (May 9, 2017), http://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization [https://perma.cc/PW5D-F7RP]; *China Adopts Cybersecurity Law Despite Foreign Opposition*, BLOOMBERG NEWS (Nov. 7, 2016, 12:33 AM), https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition [https://perma.cc/YV6D-25UN].

89. Eric Engleman, *The Telecom Industry's Pushback Against Cybersecurity*, BLOOMBERG BUS. (Mar. 7, 2013, 7:21 PM), http://www.bloomberg.com/bw/articles/2013-03-07/the-telecom-industrys-pushback-against-cybersecurity [https://perma.cc/XN4Z-7XWK]; Susan Joseph, *A Cybersecurity Framework for the Nation's Critical Infrastructure: How CableLabs Is Helping*, CABLELABS (Mar. 26, 2014), http://www.cablelabs.com/a-cybersecurity-framework-for-the-nations-critical-infrastructure-how-cablelabs-is-helping [https://perma.cc/RGD8-AFNT]; *see also* MICHAEL HAYDEN, CURT HÉBERT & SUSAN TIERNEY, BIPARTISAN POLICY CTR., CYBERSECURITY AND THE NORTH AMERICAN ELECTRIC GRID: NEW POLICY APPROACHES TO ADDRESS AN EVOLVING THREAT 9 (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf [https://perma.cc/7RJJ-RNLX].

90. *See, e.g.*, Siobhan Gorman, August Cole & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009, 12:01 AM), http://www.wsj.com/articles/SB124027491029837401 [https://perma.cc/L6Y9-Y4AQ].

91. Mercedes K. Tunstall, *The Path to Comprehensive Cybersecurity Laws in the United States*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 61, 62 (2015 ed.).

92. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, *supra* note 5.

93. *Id.* at 11,740–41.

94. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/GXH7-6AN8].

95. *Id.* at 13.

96. Pub. L. No. 113-274, 128 Stat. 2971 (to be codified in scattered sections of Title XV of the United States Code).

97. Jennifer Huergo, *Interagency Report Advocates Support for International Cybersecurity Standardization*, NAT'L INST. OF STANDARDS & TECH (Aug. 11, 2015), http://www.nist.gov/itl/201508_cyber

Cybersecurity Act of 2015, which permits organizations to voluntarily share information about cyber risks and defensive measures with the government while guaranteeing them some protection from liability, in the omnibus spending bill that was later signed by President Obama.[98] Finally, following congressional failure to promote his desired legal initiatives, President Obama signed another executive order in early 2016, which formed the Commission on Enhancing National Cybersecurity. The Commission was tasked with creating a list of recommendations on ways to strengthen cybersecurity measures, including for critical infrastructure.[99]

One possible explanation for the lack of clear legal cybersecurity principles for protecting critical infrastructure is that, while many believe that major attacks will happen soon,[100] cyberattacks in the United States have not resulted in death or drastic damage to national security or the economy thus far. Legislators have not been compelled by national emergencies to craft reactionary legislation or even to prioritize the creation of it, considering the lack of support from the private sector.[101] Yet this

---

_standards_working_group_report.cfm [https://perma.cc/CW7M-AQVS]. Reports made public by NIST in December 2015 showed some progress in that global coordination. *See* 1 INT'L CYBERSECURITY STANDARDIZATION WORKING GRP., NAT'L INST. OF STANDARDS & TECH., INTERAGENCY REPORT ON STRATEGIC U.S. GOVERNMENT ENGAGEMENT IN INTERNATIONAL STANDARDIZATION TO ACHIEVE U.S. OBJECTIVES FOR CYBERSECURITY (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf [https://perma.cc/G8HZ-4GMP]; 2 INT'L CYBERSECURITY STANDARDIZATION WORKING GRP., NAT'L INST. OF STANDARDS & TECH., SUPPLEMENTAL INFORMATION FOR THE INTERAGENCY REPORT ON STRATEGIC U.S. GOVERNMENT ENGAGEMENT IN INTERNATIONAL STANDARDIZATION TO ACHIEVE U.S. OBJECTIVES FOR CYBERSECURITY (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf [https://perma.cc/8L6V-852Z].

98. Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2935–85 (2015) (to be codified in scattered sections of the U.S.C.); Peter Carey, Keith M. Gerver & Kenneth L. Wainstein, *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing*, NAT'L L. REV. (Jan. 2, 2016), http://www.natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information [https://perma.cc/BT93-4TMJ].

99. Commission on Enhancing National Cybersecurity, Exec. Order No. 13,718, 81 Fed. Reg. 7441 (Feb. 9, 2016).

100. *See, e.g.*, HAYDEN ET AL., *supra* note 89, at 9 (discussing the substantial secondary impacts of a power outage); Michael Hayden, Curt Hébert & Susan Tierney, Opinion, *How To Protect Our Electric Grid*, USA TODAY (Mar. 4, 2014, 6:00 AM), http://usat.ly/1i2vJbb [https://perma.cc/6LE2-4QV4].

101. Usha R. Rodrigues, *Dictation and Delegation in Securities Regulation*, 91 IND. L.J. 435, 438 (2016) (explaining that law creation typically follows a pattern of boom and bust; after a crisis arises, public pressure for reform often impels Congress to act, creating a "bubble law" that is reactionary in nature); Jane Susskind, *Can Legislation Ever Keep Up with Technology?*, INDEP. VOTER NETWORK (Aug. 7, 2013), http://ivn.us/2013/08/07/can-legislation-ever-keep-up-with-technology [https://perma.cc/BU5Z-4BKV] ("It's generally known that politics trails society, with legislation acting as a reactionary function as opposed to a preemptive attempt to address shifting societal attitudes. In terms of technology, legislation is 'at least five years behind,' according to Andrea Matwyshyn, a professor at the University of Pennsylvania's Wharton School."). Moreover, even when the legislature is interested in passing a law, the process takes a long time, as the law has to pass the House of Representatives and the Senate, and the differences in the two bills must be reconciled by both

does not mean that cyberattacks cannot disable government operations or critical infrastructure operators.[102] "[Seventy-four] percent of the world's businesses expect to be hacked each year," and "[t]he estimated economic loss of cybercrime is estimated to reach $3 trillion by 2020."[103] A 2014 study demonstrated that 61% of experts believe that "a major [cyber] attack causing widespread harm would occur by 2025."[104] Similarly, a 2015 study revealed that nearly half of critical infrastructure executives "believe it is likely that a cyberattack on critical infrastructure, with the potential to result in the loss of human life, could happen within the next three years."[105] Moreover, attacks on critical infrastructure in other regions of the world, including Europe, have already taken place, and might be the reason why the EU is ahead of the United States when it comes to legislative initiatives aimed at protecting cybersecurity.[106] Indeed, in July 2016, the EU Parliament approved cybersecurity-related

---

chambers before being sent to the president for approval. This time-consuming process requires knowledge of the subject matter, the ability to withstand criticism, and, equally important, the ability to persuade others. It is difficult for such a process to take place successfully in the absence of a drastic crisis relating to cybersecurity. *See also* MILES KEOGH & CHRISTINA CODY, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, CYBERSECURITY FOR STATE REGULATORS 2.0, at 4 (2013), http://csrc.nist.gov/cyberframework/rfi_comments/040513_naruc.pdf [https://perma.cc/7EEA-PE3J]; Steve Grobman, *Out of Aspen: State of Critical Infrastructure Cybersecurity, 2015*, INFORMATIONWEEK: DARK READING (July 22, 2015, 7:00 PM), http://www.darkreading.com/partner-perspectives/intel/outof-aspen-state-of-critical-infrastructure-cybersecurity-2015/a/d-id/1321425 [https://perma.cc/XC8Y-XWGU].

102. Danielle Warner, Note, *From Bombs and Bullets to Botnets and Bytes: Cyber War and the Need for a Federal Cybersecurity Agency*, 85 S. CAL. L. REV. POSTSCRIPT 1, 11 (2012); *see also Worldwide Threat Assessment of the U.S. Intelligence Community*, *supra* note 1, at 5; David E. Sanger, *U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam*, N.Y. TIMES (Mar. 24, 2016), http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html [https://perma.cc/57SR-FUKL].

103. Brad Smith, *The Need For a Digital Geneva Convention*, MICROSOFT: ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0000diaekitjde6fuco2giewexmzj [https://perma.cc/M2SL-RCRQ] (calling on the world's governments to implement international rules to protect the civilian use of the internet, stating that similarly to how "the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace").

104. PEW RESEARCH CTR., CYBER ATTACKS LIKELY TO INCREASE 6–7 (2014), http://www.pewresearch.org/wp-content/uploads/sites/9/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf [https://perma.cc/UGA9-8JWE].

105. Press Release, Intel Corp., New Survey Reveals Critical Infrastructure Cybersecurity Challenges (July 20, 2015), http://www.mcafee.com/us/about/news/2015/q3/20150720-01.aspx [https://perma.cc/SR64-2QLN].

106. *See, e.g.*, TREND MICRO & ORG. OF AM. STATES, REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE IN THE AMERICAS 9 (2015), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf [https://perma.cc/UX4U-UB2S] (disablement and physical destruction of a German steel plant); Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES (Dec. 22, 2014), https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html [https://perma.cc/PK22-89QC] (suspected attack that caused the nationwide internet outage in North Korea, which many connected with U.S.-China

baseline requirements. The EU's Directive on Security of Network and Information Systems ("NIS Directive"),[107] which is further described below, will soon institute the first set of standards for cybersecurity and breach reporting requirements for critical infrastructure in the EU.

III. DIGITAL SERVICE PROVIDERS—CRITICAL ENTITIES?

Since the passage of the Dodd-Frank Act, policy makers have agreed that certain financial institutions are systemically important and therefore too big to fail. Similarly, policy makers agreed on the vendors that constitute critical infrastructure operators subject to special risk-management procedures, including cybersecurity requirements.[108] Nevertheless, global, omnipotent key digital service providers, including providers of social networks, search engines, and cloud computing, that also provide, among other things, financial-related services, have been ignored in the context of too-big-to-fail or critical infrastructure operators. Yet, there is no doubt that key digital service providers deliver essential services to our economy and social lives and should therefore be considered Critical Service Providers.

One reason that digital service providers have not been categorized as such could be the widespread belief that the technology industry has not been plagued by the too-big-to-fail issue. The assumption has been that technology companies come and go, acquiring each other, while their clients transition to other companies' products and services as needed.[109] Indeed, although major technology companies' products and services have failed, and there have even been technology companies that failed in their entirety, perhaps producing some type of ripple effects, no damage to the overall system has been recorded as a result as of yet. But this does not mean that such damage is not possible.

Another explanation could be that in many countries the private sector controls most of the cyber-relevant critical infrastructure. For example, in the United States, virtually all key internet services and vital digital service providers are private entities, and the private sector controls over 85% of cyber-relevant critical infrastructure.[110] Therefore, if global key digital service providers were to be defined as critical infrastructure entities, they would be subject to increased regulation. And although

---

efforts following the Sony hack); Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG TECH. (Dec. 10, 2014, 5:00 AM), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar [https://perma.cc/PD7R-GJCP] (destruction of a Turkish oil pipeline).

107. *See supra* note 19 and accompanying text.

108. Allison Grande, *EU's 1st Cybersecurity Rules Clear Final Hurdle*, LAW360 (July 6, 2016, 6:14 PM), http://www.law360.com/articles/814397/eu-s-1st-cybersecurity-rules-clear-final-hurdle [https://perma.cc/3EXD-USEY].

109. Win Treese, *Is Google Too Big To Fail?*, NETWORKER, June 2009, at 11, 11, https://www.researchgate.net/publication/242788788_Is_Google_too_big_to_fail [https://perma.cc/4KQY-W45Q].

110. Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 276 (2013).

some private entities do support "carefully crafted and narrowly tailored" legislation,[111] like the Cybersecurity Act of 2015,[112] the private sector in general is less inclined to adopt more laws or regulations that would require compliance with particular standards for technology.[113] The private sector uses four explanations to rationalize its objections: First, such requirements are likely to generate higher business expenses and misdirection of business resources.[114] Second, businesses would be required to comply with measures that rapidly become obsolete and futile at the expense of addressing current and future threats.[115] Third, such regulation would discourage public-private partnerships, which are presumably already covering the issue.[116] Fourth, more regulation is not guaranteed to enhance cybersecurity, and the public sector has not, historically, provided ideal protection against cyberattacks.[117]

But a megafailure or disastrous malfunctioning of key digital service providers, their services, or their products, could shock the country's security, economy, national public health, and safety.[118] And the likelihood of this happening as a result of a cyberattack is becoming more and more likely. In general, key digital service providers are exposed to failures that could be the result of various IT issues—from technical failures, which can include unnoticed or unresolved IT problems, or business interruption coverage, including systems failure, to malicious attacks, such as attacks exploiting online vulnerabilities as well as physical infrastructure. Differently, failures could be the result of financial issues or governance matters, including decisions regarding cyber extortion and digital asset management and restoration. But, either way, all types of failures can lead to more, different, new, and critical IT failures, financial failures, or governance failures that have extreme negative consequences that go beyond the scope of the entity in which they arose. This is because any of these failures can result in consumers losing confidence in the digital

---

111. Letter from R. Bruce Josten, Exec. Vice President of Gov. Affairs, U.S. Chamber of Commerce, to Sen. Harry Reid & Sen. Mitch McConnell 1–2 (Jan. 30, 2012), https://www.uschamber.com/sites/default/files/documents/files/120130_ComprehensiveCybersecurityLegislation_Reid_McConnell.pdf [https://perma.cc/X54T-CRJY].

112. Carey, Gerver & Wainstein, *supra* note 98.

113. JONES DAY, THE CYBERSECURITY DEBATE: VOLUNTARY VERSUS MANDATORY COOPERATION BETWEEN THE PRIVATE SECTOR AND THE FEDERAL GOVERNMENT 2, 5 (2013); *see also* Gautham Nagesh, *FCC Urges Industry-Led Approach on Cybersecurity*, WALL ST. J. (June 12, 2014, 1:37 PM), http://www.wsj.com/articles/fcc-urges-an-industry-led-approach-on-cybersecurity-to-protect-u-s-communications-networks-1402594627 [https://perma.cc/NDW3-8VBD].

114. Josten, *supra* note 111, at 1.

115. Larry Clinton, *Federal Red Tape Increases Threat of Cyberattacks*, STARS & STRIPES (Apr. 25, 2012), http://www.stripes.com/federal-red-tape-increases-threat-of-cyberattacks-1.175540 [https://perma.cc/2VEH-8HKF].

116. Josten, *supra* note 111, at 1.

117. Jody Westby, *The Government Shouldn't Be Lecturing the Private Sector on Cybersecurity*, FORBES (June 15, 2015, 2:05 PM), http://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity [https://perma.cc/V7R3-4SRN].

118. For a definition of critical infrastructure, see Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, *supra* note 5.

world, businesses losing massive amounts of money, e-government initiatives becoming ineffective, and even national security being put at stake.

By launching a cyberattack, cyberattackers can make prominent websites unavailable, causing severe damage to those relying on them. For example, according to estimates, a recent four-hour outage of Amazon's S3 cloud storage system that was not the result of a cyberattack, cost S&P 500 companies at least $150 million.[119] Accordingly, losses resulting from a large-scale attack on a cloud service are estimated in the billions. Otherwise, a cyberattack on traditional physical infrastructure, like the one that took out a large parts of the grid in Kiev, Ukraine, in December 2016, is also a concern.[120]

Realizing this, one would expect the potential IT, financial, corporate, and governance issues that can cause massive services, products, and even entity-wide failures to be closely regulated and monitored, but in reality that is not the case. The reason is that it is very difficult to model a cyber disaster, in part because one has not happened yet, and in part because it is challenging to try to quantify cyber risks. Additionally, understanding the geography of the internet, which is also important to evaluating the risk of big cyberattacks, is also quite complex. One needs a "map" of the locations where valuable data are stored, as well as information about how well the owners of those assets protect them.

Either way, identifying key digital service providers as Critical Service Providers whose potential failures should be closely monitored is justified based on such entities' (i) size, (ii) power, importance, and lines of business, and (iii) impact on internet services, which qualify as critical infrastructure.

A. Size

First, size does matter. Size is a proxy for power, and large entities have significant effects on the ecosystems and societies in which they operate. Large companies enjoy bargaining power in many areas, not just with customers. They can also refuse to comply with or even push back against governmental requests. In 2016, for example, the FBI was unable to force Apple and Amazon to cooperate with requests for information and resorted to taking the issues to court.[121] Larger businesses enjoy far greater access to capital than smaller ones, have high market value, and are arguably valued at higher multiples, everything else being equal.

The technology sector is responsible for approximately 6% of the U.S. economy and was valued at nearly $1 trillion in GDP for 2014 alone, helped in no small part

---

119. Mike Orcutt, *Insurers Scramble To Put a Price on a Cyber Catastrophe*, MIT TECH. REV. (Apr. 6, 2017), https://www.technologyreview.com/s/603937/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe [https://perma.cc/GE9F-JR7H].

120. *Id.*

121. Eric Lichtblau & Katie Benner, *Apple Fights Order To Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html [https://perma.cc/65YS-CVRH]; Amy B Wang, *Can Alexa Help Solve a Murder? Police Think So—But Amazon Won't Give Up Her Data*, WASH. POST (Dec. 28, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/?utm_term=.0a73a3683c1b [https://perma.cc/CZ57-FDMB].

by the contributions of the biggest digital service providers.[122] The "frightful five"—Amazon, Facebook, Apple, Microsoft, and Alphabet, Google's parent company (collectively, AFAMA)—control nearly everything of value in the digital world, including operating systems, application stores, browsers, cloud storage infrastructure, and oceans of data from which to spin new products. Alphabet, Apple, Facebook, and Amazon generated together $433 billion in revenues in 2015, placing them at the same level as a mid-sized economy in terms of financial volume and economic strength.[123] Moreover, experts have long said that if Apple, which is the number one firm in the NASDAQ in terms of market cap and revenue,[124] takes a big hit, the markets will sink drastically and everyone will feel the pain.[125] Indeed, in 2015, it was estimated that Apple accounted for 0.5% of the U.S. GDP, and 0.15% of the global GDP, and in May 2017, Apple shares hit an all-time high, putting the company's market value at more than $800 billion.[126] Similarly, Alphabet's Google, as of October 2016, was responsible for 90% of the worldwide search market[127]—and gave Apple a fight in early 2016, when Alphabet became the world's most valuable public company,[128] even if only for a short period of time.[129] Apple's massive market

---

122. Geof Wheelwright, *Strong-Arm Apple and Tax China Bigly: A Guide to Trump's Possible Tech Policies*, GUARDIAN (Nov. 17, 2016, 7:16 AM), https://www.theguardian.com/technology/2016/nov/17/trump-tech-policy-industry-leaders-apple-china-tax [https://perma.cc/9F2W-PQP6].

123. *See* Ghez, *supra* note 12.

124. David Saito-Chung, *Small Caps Lead Stocks Down; Apple Holds Firm, Finisar Soars*, INV. BUS. DAILY (Nov. 28, 2016), http://www.investors.com/market-trend/stock-market-today/small-caps-lead-stocks-down-apple-holds-firm-but-still-below-50-day [https://perma.cc/QX6L-BMYQ].

125. Stacey Vanek Smith, *Apple's Size Can Move Markets Up—and Down*, MARKETPLACE (Sept. 21, 2012, 3:41 PM), http://www.marketplace.org/2012/09/21/business/apple%E2%80%99s-size-can-move-markets-%E2%80%93-and-down [https://perma.cc/R6US-V5GR].

126. Tomi Kilgore, *Apple Is First To Cross $800 Billion Barrier*, MARKETWATCH (May 10, 2017, 9:54 AM), http://www.marketwatch.com/story/apple-is-first-to-cross-800-billion-barrier-2017-05-09 [https://perma.cc/MVV6-7NXN]; Tim Worstall, *Apple Is 0.5% of US GDP, 0.15% of Global GDP*, FORBES (Jan. 30, 2015, 4:53 AM), http://www.forbes.com/sites/timworstall/2015/01/30/apple-is-0-5-of-us-gdp-0-15-of-global-gdp [https://perma.cc/M39U-S5PT] ("If we say that the US economy is $17 trillion (inaccurate but close enough) then Apple is equal in size to 0.5%, half a percent, of the US economy. And if the global economy is $60 trillion (again, inaccurate, but close enough) then Apple is 0.15% of that global economy. And given that Apple operates globally that's probably the right comparison to make.").

127. Treese, *supra* note 109. For a general discussion on the importance and practice of search engines, see, for example, Tal Z. Zarsky, *Assessing Alternative Compensation Models for Online Content Consumption*, 84 DENV. U.L. REV. 645 (2006).

128. Ari Levy, *Google Parent Alphabet Passes Apple Market Cap at the Open*, CNBC (Feb. 2, 2016, 5:56 PM), http://www.cnbc.com/2016/02/01/google-passes-apple-as-most-valuable-company.html [https://perma.cc/B4XM-PKXE].

129. By late 2016, Alphabet was second to Apple again. As of November 29, 2016, Apple was valued at $595 billion, *Apple Inc.*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:AAPL [https://perma.cc/DY75-RM23], and Alphabet at $545 billion, *Alphabet Inc.*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:GOOGL [https://perma.cc/9ZVG-GJ57].

cap is still trailed by Microsoft ($476.9 billion),[130] Amazon ($358 billion),[131] and Facebook ($350 billion).[132]

Recognizing the size of key digital service providers, Senator Elizabeth Warren argued in summer 2016 against their growing impact on our society and economy and the unfair advantages and incentives they receive.[133] "[The] idea of "too big to fail" in the financial sector gets a lot of attention . . . . But the problem isn't unique to the financial sector," she said.[134] "It's hiding in plain sight all across the American economy."[135] Giants like Google, which asserted in 2012 that it had boosted the economy by $80 billion through its advertising functionality alone and transformed the world in ways that transcend economic analysis, should not be treated as favorably as the biggest banks following the 2008 financial crisis.[136]

B. Political and Financial Influence

The power and importance of key digital service providers, including AFAMA, can stretch far beyond their mere size, impressive market level, or relationships with consumers. These entities have become political and even geopolitical as they reach levels of influence and impact forbidden to even the largest financial institutions.[137] In fact, AFAMA's influence now derives from the ability of these companies to redefine a broad spectrum of political and societal realities. And while several governments, including the U.S. government, have threatened implausibly to break up the biggest banks if they do not comply with new laws and requirements,[138] it is even less likely that any state power will threaten to break up a company like Alphabet.[139]

---

130. *Microsoft Corp.*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:MSFT [https://perma.cc/AXT8-M9AR].

131. *Amazon.com, Inc.*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:AMZN [https://perma.cc/28CY-PMXT].

132. *Facebook Inc.*, GOOGLE FIN., https://www.google.com/finance?q=NASDAQ:FB [https://perma.cc/VH5K-4EES].

133. Hope King, *Elizabeth Warren: Have Tech Companies Become "Too Big To Fail"?*, CNN (July 1, 2016, 1:39 PM), http://money.cnn.com/2016/06/30/technology/elizabeth-warren-google-apple-amazon [https://perma.cc/Z57E-ZZTB].

134. *Id.* (alteration in original).

135. *Id.*

136. Eric Lieberman, *Apple Is Too Successful, Liz Warren Says*, DAILY CALLER (June 30, 2016, 4:36 PM), http://dailycaller.com/2016/06/30/apple-is-too-successful-liz-warren-says [https://perma.cc/FW5U-68XL].

137. *See* Ghez, *supra* note 12. For a discussion on how Internet market developments have introduced "new control points and dimensions of power into the Internet as a social-cultural-economic platform" and how certain companies "are jostling to acquire power over, and appropriate value from, networked activity," see, for example, Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, DÆDALUS, Winter 2016, at 18.

138. Nathaniel Popper & Peter Eavis, *Regulators Warn 5 Top Banks They Are Still Too Big To Fail*, N.Y. TIMES (Apr. 13, 2016), http://www.nytimes.com/2016/04/14/business/dealbook/living-wills-of-5-banks-fail-to-pass-muster.html [https://perma.cc/7PTQ-TQB4].

139. *See* Ghez, *supra* note 12.

AFAMA's influence in today's world also redefines the very notion of politics and governance.[140] After the recent U.S. elections, many individuals wondered about the impact of Alphabet[141] and Facebook—with its 1.79 billion monthly active users and 1.18 billion daily active users[142]—on the news ecosystem, questioning whether these companies have too much power and might be too big.[143] These questions became especially relevant after it became clear that 64% of U.S. internet users who read the news on social media sites do so on only one site, mainly Facebook.[144] Moreover, the death of distribution-based economic power has led media companies and other businesses to rely on powerful intermediaries such as Facebook and Google, which own the customer experience and commoditize their suppliers.[145] These companies immerse users in their sites rather than driving traffic elsewhere; consequently, in some developing countries users are not even aware of using the internet—to them it is all Facebook.[146]

AFAMA's influence even redefines geographical organization and structure.[147] AFAMA actively promotes libertarian values as they relate to encryption,[148] for

---

140. *See* Epstein, *supra* note 13; Fiegerman, *supra* note 13; Lapowsky, *supra* note 13.

141. Scholars found that Google could "easily shift the voting preferences of undecided voters by 20 percent or more—up to 80 percent in some demographic groups—with virtually no one knowing they are being manipulated." Epstein, *supra* note 13.

142. *See Company Info*, FACEBOOK NEWSROOM (Sept. 30, 2016), http://newsroom.fb.com/company-info [https://perma.cc/3KJ7-EN2H].

143. *See, e.g.*, Thomas Euler, *Is Facebook Too-Big-To-Fail?*, MEDIUM (Nov. 27, 2016), https://medium.com/@thomase/is-facebook-too-big-to-fail-ae6415245bd9 [https://perma.cc/MJ6R-3CE3].

144. JEFFREY GOTTFRIED & ELISA SHEARER., NEWS USE ACROSS SOCIAL MEDIA PLATFORMS 2016, at 5 (2016), http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/pj_2016-05-26_social-media-and-news_0-07 [https://perma.cc/M9GT-FY7J].

145. Ben Thompson, *Aggregation Theory*, STRATECHERY (July 21, 2015), https://stratechery.com/2015/aggregation-theory [https://perma.cc/SQ3N-YTUZ].

146. *Id.*; *see also* Rajat Agrawal, *Why India Rejected Facebook's "Free" Version of the Internet*, MASHABLE (Feb. 9, 2016), http://mashable.com/2016/02/09/why-facebook-free-basics-failed-india [https://perma.cc/GVD6-D25Y] (explaining one of the main arguments against Facebook's Free Basics initiative in India, which was rejected in 2016); Leo Mirani, *Millions of Facebook Users Have No Idea They're Using the Internet*, QUARTZ (Feb. 9, 2015), http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet [https://perma.cc/Z765-TQ54].

147. *See, e.g.*, Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 26–27 (2017) ("Digital markets suffer from a high level of concentration. Currently a handful of digital intermediaries with megaplatforms control effective points of access to potential users. These include smart devices (iPhone and Kindle), operating systems (iOS and Android), application stores (Apple Store and Google Play) and browser entry points (such as Google Search and Facebook). The high level of concentration is largely due to network effects, created when the value for each consumer of using the platform rises in parallel with the number of others using the system. These network effects are further increased by the network effects of big data. By converging control of content, access, and online distribution channels, large networks enjoy inherent competitive advantages in access to an immense volume of users' personal online data." (footnotes omitted)); Ghez, *supra* note 12.

148. *See* Ghez, *supra* note 12; Sean Keane, *Apple, Amazon, Facebook and Google Take*

example, whether or not these values clash with the goals of other organizations that AFAMA presumably supports.[149] AFAMA also redefines notions of community: Facebook rewrote the definitions of "friend," "group," and what it means to "like" something or sympathize with someone, while Amazon may forever change the concept of geographical distance by attempting to reduce it to the bare minimum through ever-faster delivery.[150]

Moreover, AFAMA and similar companies have made it clear in the last few years that they are interested in disrupting and reshaping the financial industry and have started to compete with traditional financial service providers; aided by the enormous success and rapid growth of financial technology,[151] they have already captured a portion of the sector's financial profits.[152] Offering products that range from payment and money transfer systems and loans to credit assessment, funds management, and online trades, the digital service providers have captured the attention of consumers, especially younger ones who prefer to bank with them, as well as competitors, academics, and regulators.[153] Moreover, in November 2015, Google, Amazon, and Apple started a financial regulation lobbying group, Financial Innovation Now, and in December 2016, Facebook unveiled its "newly acquired licenses for e-money and payment services out of Ireland," approximately a year after securing a patent for a new financial credit-scoring system.[154] As a result, commentators have already

---

Stand Against Encryption Law in Australia, CNET (Oct. 3, 2018), https://www.cnet.com/news/apple-amazon-facebook-and-google-take-stand-against-encryption-law-in-australia [https://perma.cc/6FDV-ZFKA].

149. *See* Ghez, *supra* note 12.

150. *Id.*

151. *See generally* Packin & Lev-Aretz, *supra* note 15.

152. Jim Marous, *Google, Apple, Facebook and Amazon Should Terrify Banking*, FIN. BRAND (Aug. 6, 2014), http://thefinancialbrand.com/41484/google-apple-facebook-amazon-banking-payments-big-data [https://perma.cc/3BXC-Q9CA]. In fall 2015, technology industry leaders Apple, Amazon, Google, Intuit, and PayPal formed Financial Innovation Now, a lobbying coalition advocating for greater innovation in financial services and more lenient regulation. Maggie McGrath, *A Peek Inside Apple, Google and Amazon's New Capitol Hill Lobbying Coalition*, FORBES (Nov. 9, 2015, 5:50 PM), http://www.forbes.com/sites/maggiemcgrath/2015/11/09/a-peek-inside-apple-google-and-amazons-new-capitol-hill-lobbying-coalition [https://perma.cc/FA8P-9S75].

153. A recent study revealed that American millennials increasingly regard banks as irrelevant, and 73% would prefer to have Google, Amazon, Apple, PayPal, or Square provide their financial services than their own banks. SCRATCH, VIACOM MEDIA NETWORKS, THE MILLENNIAL DISRUPTION INDEX (2013), https://www.bbva.com/wp-content/uploads/2015/08/millenials.pdf [https://perma.cc/MHH6-L56Y]; *see also* Shane Ferro, *33% of Millennials Don't Think They'll Need a Bank Five Years from Now*, BUS. INSIDER (Mar. 20, 2015, 9:15 AM), http://www.businessinsider.com/millennials-dont-think-they-will-need-a-bank-2015-3 [https://perma.cc/8XHD-E3A4]. Another study found that 72% of consumers eighteen to thirty-four years old would be likely to bank with major technology players if they offered financial services. ACCENTURE, THE DIGITAL DISRUPTION IN BANKING 5 (2014), https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_5/Accenture-2014-NA-Consumer-Digital-Banking-Survey.pdf [https://perma.cc/QL8W-45SZ].

154. *Financial Innovation Now: Recoding the Future of Commerce*, FIN. INNOVATION NOW, https://financialinnovationnow.org [https://perma.cc/8J5Y-KL2K]; Christoffer O.

started advocating for such institutions to be viewed as financial institutions and the biggest ones as SIFIs.[155]

C. A Society Dependent on Cloud Computing

Additionally, some have expressed fear regarding the damage that could be done to government operations, financial infrastructure, and cyber-social systems if cyberattacks were to take place against one of these key digital service providers.[156] For example, "in addition to its digital media prowess, fashion lines, hardware sales," and marketplace lending services, Amazon "is also the dominant player in the cloud services segment," which now hosts everything from television shows to financial information and even the CIA's intelligence data[157]—a significant change from a few years ago, when government agencies, including the CIA, were reluctant to use cloud services, particularly those provided by private companies.[158] However, two trends have pushed institutions towards the cloud, even as some agencies remain unclear on its complexities: (i) increasing specialization in technology's functionality and operation and difficulty of local installation and management and (ii) increasingly reliable and dependable cloud-based networks.[159] Realizing this, some government agencies initially attempted to own the entire cloud process and create homegrown enterprise cloud systems, but those proved harder to execute than imagined, which led the agencies to outsource their cloud strategy. The Department of Defense (DoD) created various cloud security policies and established procedures in the event of cyber incidents; in December 2014, it issued a memorandum allowing DoD agencies to

---

Hernæs, *What Facebook's European Payment License Could Mean for Banks*, TECHCRUNCH (Jan. 12, 2017), https://techcrunch.com/2017/01/12/what-facebooks-european-payment-license-could-mean-for-banks [https://perma.cc/4789-PRDB].

155. "The growing influence of nonbank companies poses a risk to the financial system, and perhaps a national security threat . . . . [B]ankers should recognize the potential dangers posed by nonbank players, particularly in the payments industry." Kristin Broughton, *Apple Pay a Systemic Risk? Banker Warns About Nonbank Players*, AM. BANKER (Nov. 21, 2014, 11:43 AM), http://www.americanbanker.com/news/bank-technology/apple-pay-a-systemic-risk-banker-warns-about-nonbank-players-1071357-1.html [https://perma.cc/4CQY-YM2K].

156. At least a few banks expressed concerns about the amount of personal and financial information Apple is collecting about the banks' customers, fearing that the same data "could serve as a beachhead for an invasion of the banking industry." Christopher Williams, *UK Banks in Talks over Apple "Wave and Pay,"* TELEGRAPH (Dec. 27, 2014, 7:29 PM), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/11312574/UK-banks-in-talks-over-Apple-wave-and-pay.html [https://perma.cc/UUJ8-WEWR].

157. *See* Neiger, *supra* note 16 (emphasis omitted).

158. *See* Hannah Moss, *DoD and the Cloud*, GOVLOOP (June 24, 2015), https://www.govloop.com/dod-and-the-cloud [https://perma.cc/HMS9-N54Q].

159. *Id.*

purchase cloud computing services directly from private cloud service providers,[160] while trying to make it as easy and safe as possible to use the cloud services.[161]

As mentioned, Amazon is currently the biggest cloud services company, but it is not the only key digital service provider offering such services to critical infrastructure operators. Google, for example, is doing the same thing.[162] According to experts, however, Amazon's share of the market will increase even more; along with Microsoft, it is predicted to take over 76% of the cloud business, which the financial industry is becoming extremely dependent on, and that will be worth about $32.9 billion in 2017.[163]

In the years following the 2008 financial crisis, it has become clear that major nonbank institutions could also pose risks to the financial system and therefore should be monitored similarly to SIFIs.[164] By the end of 2014, regulators went so far as to designate several nonbanks as SIFIs.[165] Similarly, the Federal Reserve has recently announced that it will soon issue rules for insurance companies—which by nature also provide financial services, as was clearly demonstrated by AIG's involvement in the 2008 crisis—deemed too big to fail that will minimize risks to U.S. financial stability.[166]

---

160. Memorandum from Terry A. Halvorsen, Acting Chief Info. Officer, U.S. Dep't of Def., to Sec'ys of the Military Departments et al., Updated Guidance on the Acquisition & Use of Commercial Cloud Computing Servs. 1 (Dec. 15, 2014), http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Serviices_20141215.pdf [https://perma.cc/A5D4-YMWU].

161. David Gallacher & Townsend Bourne, *Federal Cloud Security*, *in* CLOUD COMPUTING LEGAL DESKBOOK § 11:11, Westlaw (database updated June 2018).

162. Neiger, *supra* note 16.

163. *Id.* In addition to the large financial scale of this business, it is important to note that the main entities offering cloud computing services also get exposed to much more data than other businesses. Indeed, research shows "that cloud computing does result in the collection of more private information, but this mostly happens voluntarily." Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Term*s, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 594 (2010).

164. In the case of nonbanks, section 113 of the Dodd–Frank Act left the question of which entities qualify as SIFIs to the FSOC. 12 U.S.C.A. § 5323 (West 2014). Nonbanks identified as SIFIs are subject to consolidated supervision by the Federal Reserve and enhanced prudential standards in a manner similar to the Bank Holding Company Act model of regulation and supervision. *Id.* §§ 5325(a), 5365(i)–(j).

165. Thus far, such entities include: AIG; Prudential Financial; GE Capital, which was able to restructure itself to no longer qualify; and Metlife, which has argued against this designation. *Financial Stability Oversight Council: Designations*, U.S. DEP'T TREASURY (June 29, 2016, 9:48 AM), http://www.treasury.gov/initiatives/fsoc/designations/Pages/default.aspx [https://perma.cc/QW3F-SPTB].

166. Lisa Lambert, *Rules for "Too Big To Fail" Insurance Firms Coming Soon: Fed Official*, REUTERS (May 20, 2016, 9:35 AM), http://www.reuters.com/article/us-usa-fed-insurance-idUSKCN0YB1M9 [https://perma.cc/8WLY-NVBK].

D. The Internet as Critical Service

The internet can and probably should be viewed as a critical infrastructure. Over the last few years its importance as a critical infrastructure for national defense activities, energy resources, finance, transportation, and fundamental daily life pursuits for billions of individuals has become greater than ever.[167] So much of U.S. infrastructure is online that "gaining control of or disrupting" the country's key digital service providers is likely to "become a critical goal in future conflicts."[168] Experts have "varying opinions about the likely extent of damage and disruption [to cyberinfrastructure] at the nation-state level," but many predict that the "current cyber arms race dynamic will expand as nations and other groups . . . ceaselessly work to overcome security measures."[169] Given the potential extreme damage of a lethal cyberattack, some have questioned if a voluntary framework will be sufficient to ensure that private companies, including the world's leading digital service providers, adequately protect our critical infrastructure sectors.[170]

Recognizing this, in 2016 the EU Parliament announced its NIS Directive, which aims to cover two types of entities. First, it concerns "essential service operators" within the energy, transport, banking, financial market infrastructure, health, drinking water, and digital infrastructure sectors, arguing that "digital infrastructures'" or "e-infrastructures'" activity aims at empowering researchers with easy and controlled online access to facilities, resources, and collaboration tools, bringing to them the power of ICT for computing, connectivity, data storage, and access to virtual research environments.[171] According to the NIS Directive, the criteria for identifying the operators of essential services are: (i) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities, (ii) the provision of that service depends on network and information systems, and (iii) an incident would have significant disruptive effects on the provision of that service.[172] Second, and more importantly for this Article's purpose, "digital service providers," including entities such as online marketplaces, online search engines, and cloud computing service providers,[173] appear in the NIS Directive, even if they are subject to a lighter regulatory touch than essential service operators. This European inclusion is partly the result of more and more European data moving online and a presumed attempt by the European Union to ensure that networks such as Amazon Web

---

167. *See* PEW RESEARCH CTR., *supra* note 104, at 5. Needless to say, what regulators should and would require of critical infrastructure, too-big-to-fail financial institutions, and too-big-to-fail banks vary depending on the industry and type of institutions involved, and hence the different rules for the insurance firms.

168. *Id.* at 11 (internal quotation marks omitted).

169. *Id.* at 9.

170. JONES DAY, *supra* note 113, at 2; *see also* Nagesh, *supra* note 113.

171. *See Digital Infrastructures*, EUR. COMMISSION (Aug. 17, 2017), https://ec.europa.eu/digital-single-market/en/digital-infrastructures [https://perma.cc/LSQ3-7UBH].

172. "[O]perator of essential services" means a public or private entity of a type referred to in Annex II of the NIS Directive, which meets the criteria laid down in Article 5(2) of the NIS Directive. NIS Directive, *supra* note 19, at 14, 28–29.

173. *Id.* at 7.

Services (AWS) and Google Drive, which store vast amounts of data, are not compromised and suffer minimal downtime.[174] Moreover, this inclusion is meant to help identify and monitor "key operators of essential services and networks, such as online banking," given the potential harm to society and the economy that could result from their collapse or severe breach.[175] This inclusion of digital service providers did not go uncontested. An earlier proposal agreed upon by the EU Parliament in March 2014 did not include "enablers of key internet services" such as Google, Amazon and Facebook—so-called over-the-top companies.[176] Later on, however, policy makers agreed to include them,[177] as reflected in the NIS Directive.[178]

According to media reports, the considerable disagreement regarding the inclusion of digital service providers in the NIS Directive was due to the objections of many of the entities falling under the definition of digital service provider. In particular, these opponents argued that cyberattacks on digital service providers were insignificant, and that additional regulation would potentially detract from innovation. But policy makers insisted on precautions to guarantee the security of digital infrastructure, requiring companies like Google to report key breaches to data protection authorities.[179]

Given all of the above, key digital service providers should be viewed as Critical Service Providers, as in some respects they bear similar responsibility and liability to the ones SIFIs and critical infrastructure operators do. Indeed, while the type of damages and their impact greatly varies, society is reliant on these institutions, and their potential failure, or the failures of some of their key services or products, can cause a massive ripple effect. This makes these institutions extremely important and their potential failures will be referred to herein as Too-Big-To-Fail 2.0.

---

174. Roi Perez, *Industry Sceptical of New NIS Directive Passed Today*, SC MAG. UK (Jan. 14, 2016), https://www.scmagazineuk.com/industry-sceptical-new-nis-directive-passed-today/article/1477756 [https://perma.cc/LDG9-SCEB].

175. Kelly Fiveash, *Google, Amazon, Other Giants May Soon Have To Notify EU Nations of Big Security Leaks*, ARS TECHNICA UK (Jan. 14, 2016, 10:39), http://arstechnica.co.uk/security/2016/01/google-amazon-prepare-to-warn-eu-nations-of-big-security-gaffes [https://perma.cc/KEB4-BQ57].

176. Allison Grande, *EU Parliament Frees Google, Others from Cybersecurity Plan*, LAW360 (Mar. 13, 2014, 6:47 PM), https://www.law360.com/articles/518254/eu-parliament-frees-google-others-from-cybersecurity-plan [https://perma.cc/5TD4-LQYU]. Apparently, "Ireland, Sweden, and the UK—all countries which host large US-based internet concerns—are leading efforts to minimi[z]e the involvement of such companies within the scope of the directive," while "France, Germany[,] and Spain, amongst others are opposed" to the efforts and pushing to scrutinize these companies more. Jeremy Fleming, *Cyber Security Directive Held Up in Face of "Wild West" Internet*, EURACTIV (Apr. 1, 2015, 4:05 AM), https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet [https://perma.cc/3ZBV-7GR3].

177. Allison Grande, *EU Cybersecurity Rules Increase Liability for Multinationals*, LAW360 (Dec. 8, 2015, 11:22 PM), https://www.law360.com/articles/735622/eu-cybersecurity-rules-increase-liability-for-multinationals [https://perma.cc/357J-JFYM].

178. Grande, *supra* note 108.

179. *Id.*

IV. RISKS AND CHALLENGES

A. Cybersecurity and Threats

Considering the importance of cybersecurity, baseline requirements for risk management and mitigation are long overdue—particularly in the financial industry, which has suffered from many attacks in recent years. In February 2016, for example, cyber criminals stole more than $81 million from the Bangladesh central bank's holdings in the New York Federal Reserve Bank.[180] They did so using the credentials of the Society for Worldwide Interbank Financial Telecommunication (SWIFT), whose network enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized, and reliable environment. The 2016 cyberattack was concerning given that the majority of international interbank messages use the SWIFT network.[181] Likewise, the FDIC has suffered dozens of cyberattacks since 2010 which have infected the computers of former Chairwoman Sheila Bair and other officials.[182] In an attack in October 2015, a massive cybersecurity breach affected more than 40,000 individuals and 30,000 banks.[183] Unwilling to disclose the scale of the breach, the FDIC grossly misrepresented the number of affected individuals and entities.[184]

But while attacks on cybersecurity with substantial long-term physical effects are less likely to materialize, other threats involving information infrastructures are quite possible. Certainly, there is a substantial danger during many conventional catastrophes that a supportive information infrastructure will become overloaded and crash, thus preventing societal recovery. The absence of a clear governmental response in such situations may cause public panic if there appears to be no clear path back to normalcy.

It is not surprising, therefore, that both the media and government officials have been paying more attention to the potential scenarios that could result from lethal

---

180. Victor Mallet & Avantika Chilkoti, *How Cyber Criminals Targeted Almost $1bn in Bangladesh Bank Heist*, FIN. TIMES (Mar. 18, 2016), https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8 [https://perma.cc/BXU6-6VDH].

181. Kalev Leetaru, *What the Bangladesh SWIFT Hack Teaches About the Future of Cybersecurity and Cyberwar*, FORBES (Apr. 30, 2016, 4:08 AM), http://www.forbes.com/sites/kalevleetaru/2016/04/30/what-the-bangladesh-swift-hack-teaches-about-the-future-of-cybersecurity-and-cyberwar [https://perma.cc/D37L-Z5JT] ("The attackers initially attempted to loot the bank of a grand total of 951 million dollars, but most transfers were blocked, leaving the robbers with just 81 million which was routed through bank accounts and casinos in the Philippines and remain missing.").

182. Lalita Clozel, *FDIC's Gruenberg Admits Mistakes in Cybersecurity Hearing*, AM. BANKER (July 14, 2016, 10:57 AM), http://www.americanbanker.com/news/law-regulation/fdics-gruenberg-admits-mistakes-in-cybersecurity-hearing-1090187-1.html [https://perma.cc/V3W7-ADRL].

183. Lalita Clozel, *FDIC Created False "Narrative" on Cybersecurity Incident, Lawmakers Charge*, AM. BANKER (July 13, 2016, 4:09 PM), http://www.americanbanker.com/news/law-regulation/fdic-created-false-narrative-on-cybersecurity-incident-lawmakers-charge-1090170-1.html [https://perma.cc/DPF8-S6UX].

184. *Id.*

cyberattacks.[185] In August 2015, for the first time, U.S. regulators advised financial institutions to include cyber risk analysis in their Dodd-Frank Act mandated living wills, as part of their general strategic planning. The FDIC stressed that "[i]n addition to preparing for natural disasters and other physical threats, continuity now also means preserving access to customer data and the integrity and security of that data in the face of cyberattacks."[186] Then, in June 2016, SEC Chair Mary Jo White described cybersecurity as "one of the greatest risks facing the financial services industry and will be for the foreseeable future."[187] Several months later, in fall 2016, the state of New York[188] and a number of federal agencies proposed new regulations to

---

185. For example, regulators focused on the financial system have repeatedly expressed deep anxiety about data hackings, which "represent a systemic risk to our financial markets. . . . [W]ithin the next decade—or perhaps sooner—we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time—what some have termed a 'cyber 9/11.'" Young Ha, *N.Y.'s Lawsky: Cybersecurity Likely Most Important Issue DFS Will Face in 2015*, INS. J. (Feb. 26, 2015), https://www.insurancejournal.com/news/east/2015/02/26/358751.htm [https://perma.cc/8A67-T9WV].

186. Ian McKendry, *Cyber Risk Should Be Standard Part of Disaster Planning: FDIC*, AM. BANKER (Aug. 24, 2015, 3:12 PM), http://www.americanbanker.com/news/law-regulation/cyber-risk-should-be-standard-part-of-disaster-planning-fdic-1076279-1.html [https://perma.cc/7UQQ-UMCB] (quoting an article authored by a division of the FDIC).

187. Mary Jo White, Chair, Sec. & Exch. Comm'n, Testimony on "Oversight of the U.S. Securities and Exchange Commission" Before the Committee on Banking, Housing, & Urban Affairs, United States Senate 14 (June 14, 2016), https://www.sec.gov/news/testimony/testimony-white-oversight-sec-06-14-2016.html [https://perma.cc/2FV3-WDQL]. Not long after, the SEC created a new position—Senior Advisor to the Chair for Cybersecurity Policy—to better handle cyber threats. Press Release, Sec. & Exch. Comm'n, SEC Names Christopher Hetner as Senior Advisor to the Chair for Cybersecurity Policy (June 2, 2016), https://www.sec.gov/news/pressrelease/2016-103.html [https://perma.cc/G372-NS4J]. The SEC described Hetner's senior adviser responsibilities as threefold: (1) "coordinating efforts across the [SEC] to address cybersecurity policy," (2) "engaging with external stakeholders," and (3) "further enhancing the SEC's mechanisms for assessing broad-based market risk." *Id.*

188. The New York State Department of Financial Services (NYDFS) was the first to propose cybersecurity regulation for financial companies. The proposed New York requirements are designed to address what the NYDFS describes as an "evergrowing threat posed to information and financial systems" and require covered entities to develop a Cybersecurity Program that can (i) identify internal and external risks, (ii) use defensive infrastructure, (iii) detect predefined cybersecurity events, (iv) respond to and mitigate such events, (v) recover and restore normal operations and services, and (vi) fulfill reporting obligations. The requirements also delve into some technical areas: they mandate that financial services companies implement a written Cybersecurity Policy and create official notice procedures, and require corporate governance and risk management changes in covered entities. *See* N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR (2014), https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_banking_report_052014.pdf [https://perma.cc/CRR2-7YRT]; N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE INSURANCE SECTOR (2015), https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_insurance_report_022015.pdf [https://perma.cc/G3TJ-L4ZB]; N.Y. STATE DEP'T OF FIN. SERVS., UPDATE ON CYBER SECURITY IN THE BANKING SECTOR: THIRD PARTY SERVICE PROVIDERS (2015), https://www.dfs.ny.gov/reportpub/cyber/dfs_rpt_tpvendor_042015.pdf [https://perma.cc/PS9T-SUNL].

address cybersecurity challenges to financial service institutions.[189] Among the proposed regulations are provisions suggesting that entities that provide a sector-critical system should be required to "substantially mitigate the risk of a disruption due to a cyber event."[190] Similarly, the regulators are considering whether it might be appropriate to determine which entities should be covered under some of these cybersecurity initiatives based on the number of connections that a particular entity, its affiliates, and third-party service providers have with other entities throughout the financial sector—as opposed to doing so based on asset size. Furthermore, the regulators are considering whether such enhanced cyber risk management standards should apply directly to third-party service providers of financial entities that are covered under the new initiatives, rather than placing oversight responsibility for service providers on the financial entity itself, in an effort to ensure consistent application and oversight of such standards regardless of whether it is a third-party service provider of the financial entity that works with it that performs a relevant operation. Finally, regulators are contemplating requiring domestic and international covered entities with sector critical systems, as well as relevant third parties, which provide

---

189. Attempting to curb systemic cyber threats, the Federal Reserve Board, the FDIC, and the Office of the Comptroller of the Currency approved an advance notice of proposed rulemaking (ANPR) regarding potential "enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that these entities receive from third parties" on October 19, 2016. *See* Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (proposed Oct. 26, 2016) (to be codified at 12 C.F.R. pts. 30, 364 & ch. II). The ANPR is intended to address "cyber contagion"—that is, the risk that "a cyber incident or failure at one interconnected entity may not only impact the safety and soundness of the entity, but also other financial entities with potentially systemic consequences." *Id.* at 74,316, 74,324. The ANPR proposes that all covered institutions meet a minimum standard and that "those entities that are critical to the functioning of the financial sector" meet "more stringent standards." *Id.* at 74,315. The enhanced cyber risk management standards described in the ANPR would apply on an enterprise-wide basis to banking organizations and financial institutions with U.S. $50 billion or more in total consolidated assets—including, among others, financial market utilities designated as systemically important by the FSOC, financial market infrastructures for which the Board exercises primary supervisory authority, and nonbank financial companies subject to enhanced supervision and prudential standards under Section 165 of the Dodd-Frank Act. Similarly, in September 2016, the Federal Financial Institutions Examination Council (FFIEC) updated its Information Technology Handbook to incorporate revised examination expectations with respect to information security. FFIEC Information Technology Examination Handbook, Information Security, Sept. 2016, http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf [https://perma.cc/CCY5-379C]. Additionally, in late 2016, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) published guidance on financial institutions' reporting of cyber events in connection with their submission of Suspicious Activity Reports (SARs), as required under the Bank Secrecy Act and FinCEN's Anti-Money Laundering regulations. Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, FinCEN, Oct. 25, 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf [https://perma.cc/S23W-3AXA] (stating that the "proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system").

190. Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 74,319, 74,320.

sector-critical systems, to establish procedures regarding returning to full operational ability within two hours of a cyber event.[191]

B. Preparedness and Awareness?

The 2008 crisis resulted in large part from the regulatory financial system, which was flawed, fragmented, and out of touch with current technology and financial mechanisms. Considering the state of the regulatory cyber risk management system, the present situation is not much different. Most institutions have traditionally viewed cybersecurity as an IT problem despite current awareness that cybersecurity constitutes a broader risk management issue necessitating risk-based decision making.[192] Technology's evolution is constantly outpacing regulators, and the speedy growth we have witnessed in financial technology markets such as payments and marketplace lending is often tricky to understand, monitor, and regulate. Similarly, the rapid growth and advancement of cloud computing services, search engines, and data processing features, and social networks' related products, have also proved difficult to standardize legally, ethically, and socially.

As a result of the 2008 crisis, U.S. financial institutions enhanced their risk management, following the Dodd-Frank Act's requirements, which are not ideal but at least included the creation of risk management committees and the preparation and submission of disaster plans. This exercise, which is not bulletproof, does not really mention cyber risks and only applies to financial institutions, not digital service providers. And the fragmented global patchwork of laws that imposes varying and often incoherent rules on business institutions, such as data security and breach reporting mandates, is in place only in some jurisdictions, while in others there are no specific requirements. And until 2016, when New York State issued its Cybersecurity Regulations for Financial Service Companies, which was the first of its kind in the United States,[193] no state laws mandated that major institutions internalize cyber-related risks, test their own cybersecurity, prepare for disastrous consequences, or purchase cyber insurance. But New York's new laws do not relate to nonfinancial private-sector companies or to key digital service providers, and that might be problematic. New York's new measures only require banks, insurance companies, and other financial services institutions regulated by the state's Department of Financial Services (DFS) to establish and maintain a cybersecurity program designed to protect consumers' private data and ensure the safety and soundness of the state's massive financial services industry. This legislation was not created in a vacuum. According

---

191. *Id.* at 74,325; *see also* Jeff C. Dodd, Sean S. Wooden & Ross Campbell, *New York Proposes First State Cybersecurity Regulations for Financial Services Companies; Federal Agencies Push for Enhanced Standards to Prevent "Cyber Contagion,"* NAT'L L. REV. (Nov. 4, 2016), http://www.natlawreview.com/article/new-york-proposes-first-state-cybersecurity-regulations-financial-services-companies [https://perma.cc/C8EJ-WTF7]; David F. Freeman, Ronald D. Lee & Michael A. Mancusi, *Banking Agencies Considering Enhanced Cyber Risk Management Standards for Larger Enterprises*, LEXOLOGY (Nov. 9, 2016), http://www.lexology.com/library/detail.aspx?g=b58421c3-8a06-4ef1-ad66-5d9d9d74c35b [https://perma.cc/PV8A-NAZ2].

192. SAS INST. INC., *supra* note 23.

193. *See* Dewald et al., *supra* note 191.

to a study conducted in 2016 by the Ponemon Institute, 66% of the 2400 security and IT professionals interviewed said that their organization was not prepared to recover from cyberattacks.[194] Moreover, 75% of respondents admitted that no formal cybersecurity incident response plan (CSIRP) was applied consistently across their organizations; of those with a CSIRP in place, 52% had either not reviewed or updated it since it was put into place or had no set plan for doing so.[195] Even more concerning, most entities participating in this study had experienced a data breach in the past year, and 57% of respondents reported that their entities had suffered from a data breach involving the loss or theft of more than 1000 records, including sensitive or confidential professional information, in the past two years. And while legislative initiatives have been made to encourage public companies to appoint cybersecurity experts to their boards of directors, such legislative attempts have yet to be successful.[196]

Key digital service providers, despite their size and importance to our economy, are not legally required to manage their business risks, including cyber risks. Indeed, U.S. cybersecurity laws and regulations date back to the 1980s, but historically focused almost exclusively on punishing hackers or penalizing companies that failed to secure sensitive information. And, despite digital service providers' presumed technical expertise, much like other businesses, they have also been exposed to cyberattacks. For example, in 2016–2017 alone, most key digital service providers suffered from significant cyberattacks. In 2018, scandalous reports came out about Facebook's handling of user information that resulted in Cambridge Analytica's access to the data of 50–90 million Facebook users, which may have impacted the 2016 presidential election.[197] Prior to that, Facebook also proved vulnerable to breaches when the company admitted that links and malicious files had been sent through its program to hack into users' accounts, and even the U.S. president Donald Trump was informed of these risks and their potential impact, given his extensive use of social media.[198] In addition, data hacks and leaks dating back to 2012 had caused technical

194. Michael Cooney, *IBM: Many Companies Still Ill-Prepared for Cyber Attacks*, NETWORKWORLD (Nov. 16, 2016, 11:25 AM), http://www.networkworld.com/article/3142316/security/ibm-many-companies-still-ill-prepared-for-cyber-attacks.html [https://perma.cc/S4CX-QAP9].

195. *Id.*

196. *Id.* U.S. Senators Mark Warner (D-VA), Jack Reed (D-RI), and Susan Collins (R-ME) have joined together to introduce such a bill. *See* The Cybersecurity Disclosure Act of 2017, S. 536, 115th Cong. (2017) (introduced March 7, 2017); Michael Greene, *Senators Focus on Board Cyber Skills in Disclosure Bill*, BLOOMBERG (Mar. 16, 2017), https://www.bna.com/senators-focus-board-n57982085274 [https://perma.cc/XM66-QMGY].

197. The Facebook–Cambridge Analytica data scandal exploded in 2018, after it was revealed that Cambridge Analytica had harvested the personal information of millions of people's Facebook profiles without their consent in order to exploit it for political purposes. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/A28H-B8FL]; *see also* Issie Lapowsky, *What Did Cambridge Analytica Really Do for Trump's Campaign*, WIRED (Oct. 26, 2017), https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign [https://perma.cc/F38G-5PSN].

198. Bogdan Popa, *President Donald Trump's Android Phone Could Easily Be Hacked,*

glitches in Facebook's massive archive of contact information that was collected from 1.1 billion users worldwide.[199] As a result of the glitches, Facebook users who downloaded contact data for their list of friends obtained additional private information.[200]

Similarly, in December 2018, reports came out about a new Google+ blunder, which exposed data from 52.5 million users.[201] In November 2016, reports came out disclosing that a new variant of Android malware was responsible for the theft of what was believed to be more than 1.3 million Google accounts.[202] And, in July 2016, Google's parent company, Alphabet, revealed that it was subject to approximately 4000 state-sponsored cyberattacks on users per month.[203]

Similarly, the non-key but nonetheless famous digital service provider Yahoo, a search engine that also provides email services, admitted in September 2016 that hackers had stolen data on 500 million users in 2014;[204] in December 2016, the world learned that in 2013 one billion Yahoo accounts were compromised.[205] Other major digital service providers, including Amazon, also endured cyberattacks in 2016.[206] Likewise, in 2016, Apple not only had to ascertain how the U.S. government had cracked its iPhone,[207] but it also had to release a patched version of its latest mobile

---

Experts Warn, SOFTPEDIA (Nov. 28, 2016, 1:42 PM), http://news.softpedia.com/news/president-donald-trump-s-android-phone-could-easily-be-hacked-experts-warn-510553.shtml [https://perma.cc/FGE5-UL6R].

199. Gerry Shih, *Facebook Admits Year-Long Data Breach Exposed 6 Million Users*, REUTERS (June 21, 2013, 7:08 PM), http://www.reuters.com/article/net-us-facebook-security-idUSBRE95K18Y20130621 [https://perma.cc/5BA3-JK4Z].

200. *Id.*

201. Ben Tobin, *Google To Shut Down Google+ Early Due To Bug that Leaked Data of 52.5 Million Users*, USA TODAY (Dec. 11, 2018, 8:02 AM), https://www.usatoday.com/story/tech/2018/12/11/google-plus-leak-social-network-shut-down-sooner-after-security-bug/2274296002 [https://perma.cc/SG57-GZPS].

202. Thomas Fox-Brewster, *Android "Gooligan" Hackers Just Scored the Biggest Ever Theft of Google Accounts*, FORBES (Nov. 30, 2016), http://www.forbes.com/sites/thomasbrewster/2016/11/30/gooligan-android-malware-1m-google-account-breaches-check-point-finds [https://perma.cc/BPZ3-ZNVE].

203. Jonathan Chadwick, *4,000 Cyber Attacks on Users Per Month: Alphabet*, ZDNET (July 12, 2016), http://www.zdnet.com/article/4000-cyber-attacks-on-users-per-month-alphabet [https://perma.cc/2GJP-JM3F].

204. Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html [https://perma.cc/L9YL-JMB5].

205. Sam Thielman, *Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History*, GUARDIAN (Dec. 15, 2016), https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached [https://perma.cc/TEL6-7VCF].

206. *See, e.g.*, Agan Uzunovic, *Amazon Suffers Security Breach; 80,000 Login Credentials Leaked*, HACKREAD (July 8, 2016), https://www.hackread.com/amazon-suffers-security-breach [https://perma.cc/3B2U-PVV9] (reporting that, in July 2016, a hacker leaked 80,000 Amazon login credentials because the company would not respond to his security report).

207. Katie Benner, John Markoff & Nicole Perlroth, *Apple's New Challenge: Learning How the U.S. Cracked Its iPhone*, N.Y. TIMES (Mar. 29, 2016), http://www.nytimes.com/2016/03/30/technology/apples-new-challenge-learning-how-the-us-cracked-its-iphone.html [https://perma.cc/TKC4-GLPY].

software, iOS 9.3.5, after one of the world's most evasive digital arms dealers allegedly took advantage of several security vulnerabilities in its products to spy on dissidents and journalists.[208] Apple also dealt with security breaches relating to the usernames, passwords, and other information for thirteen million users of MacKeeper, a performance-optimizing software for Apple computers.[209] Finally, as previously discussed, in May 2017, attackers took advantage of Microsoft software vulnerabilities and over the course of several days disrupted operations in more than 150 countries.[210]

While these cyberattacks and hacks on the largest global digital service providers vary in their severity and scope, it is clear that these entities are neither safe nor any more resilient than the largest financial institutions or other critical infrastructure operators. Moreover, unlike some other industries' entities, such as financial institutions, which are now legally required to at least try to enhance their risk management efforts, it is unclear how much U.S. digital service providers are improving their risk management procedures in an attempt to prevent the potentially dire consequences of cyberattacks.[211]

In the EU, the regulatory landscape is a bit stricter for digital service providers; the July 2016 NIS Directive attempted to formalize what used to be considered best practices into actual legal obligations. Yet, even in the EU, the legal standards regarding risk internalization and management are still vague and interpretations of them vary among the member states, producing a patchwork of mismatched adoptions of the law.

C. Expectations and Public Choice Theory

As mentioned above, the U.S. private sector controls over 85% of cyber-relevant critical infrastructure. And if key digital service providers were to be defined as Critical Service Providers, they would be subject to more scrutiny and regulation, which the private sector is less inclined to adopt given its opposition to cybersecurity regulations that would mandate compliance with specific principles or technology.[212] Within a risk-based cybersecurity approach, private businesses assess the probability

---

208. Nicole Perlroth, *iPhone Users Urged To Update Software After Security Flaws Are Found*, N.Y. TIMES (Aug. 25, 2016), http://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html [https://perma.cc/T545-L3P7] ("Investigators discovered that . . . [t]he NSO Group's software can read text messages and emails and track calls and contacts. It can even record sounds, collect passwords and trace the whereabouts of the phone user.").

209. Brian Krebs, *13 Million MacKeeper Users Exposed*, KREBS ON SECURITY (Dec. 14, 2015), https://krebsonsecurity.com/2015/12/13-million-mackeeper-users-exposed [https://perma.cc/6MV2-BTXL].

210. *See* Volz & Auchard, *supra* note 1.

211. *See* Alan Murray, *Google vs Microsoft*, FORTUNE (Nov. 1, 2016, 8:03 AM), http://fortune.com/2016/11/01/google-microsoft-vulnerability-cyberattacks-breach [https://perma.cc/AK4G-SZLW] (describing how the existence of a "zero day vulnerability" in Microsoft Windows software was disclosed, meaning that there is a hole in the software that can be exploited by hackers).

212. JONES DAY, *supra* note 113; *see also* Nagesh, *supra* note 113.

of cyberattacks at different levels of magnitude and the costs and methods needed to prevent each type of attack.[213] Businesses may not be inclined to allocate a great deal of funds and effort to protect against such attacks;[214] some may simply buy insurance to cover these unlikely threats.[215] Private-sector businesses also lack incentive to invest in protection against successful and disruptive critical infrastructure cyberattacks if they do not internalize their negative and positive externalities.[216] For example, if cyberattackers ruin a power generation facility, the operator may need to spend funds on a new digital infrastructure and may lose some revenue from its customers.[217] But because such a facility is viewed as part of the critical infrastructure, the government will pick the lesser evil and step in to help with purchasing the systems and catching the attacker.[218] Thus, the consumers will ultimately suffer the consequences—albeit reduced due to the intervention—of this attack while they remain without power.[219]

Thus, financial considerations may be the largest obstacle preventing companies from protecting themselves from cyber threats. However, the government should not simply dispense money when private businesses are not investing for their own protection. The private sector should better manage the risks related to cybersecurity issues even if doing so results in financial gains that do not surpass the expense of guarding against these threats.[220] The government should offer assistance and encouragement to help businesses offset these expenses. Yet the fear remains that "[d]amages in the billions will occur to manufacturing and/or utilities but because it ramps up slowly, it will be accepted as just another cost (probably passed on to taxpayers through government rebuilding subsidies and/or environmental damage), and there will be little motivation for the private sector to defend itself. . . . The primary issue is a lack of policy/political/economic incentives and willpower to address the problem."[221]

Addressing this problem could also be done using public choice theory tools, which apply concepts from economics to an analysis of political behavior. In the traditional "public interest" view, public officials are "public servants" who devot-

---

213. Teplinsky, *supra* note 110, at 311.

214. *See* INTERNET SEC. ALL., THE ADVANCED PERSISTENT THREAT: PRACTICAL CONTROLS THAT SMALL AND MEDIUM-SIZED BUSINESS LEADERS SHOULD CONSIDER IMPLEMENTING 4 (2013), http://isalliance.org/publications/2013-06-06-ISA_APT_Paper-Practical_Controls_for_SMBs.pdf [https://perma.cc/U6ER-7B5A].

215. Matthew Cohen, Opinion, *Comment: Cybersecurity Lessons from the Financial Sector*, INFOSECURITY MAG. (Jan. 9, 2014), http://www.infosecurity-magazine.com/opinions/comment-cybersecurity-lessons-from-the-financial [https://perma.cc/R3SC-W746].

216. Sales, *supra* note 84.

217. *Id.* at 1507–08.

218. *Id.* at 1508.

219. "A targeted cyber-attack . . . on the power system could lead to huge costs, with sustained outages over large portions of the electric grid and prolonged disruptions in communications, health care delivery and food and water supplies." Hayden et al., *supra* note 100; *see also* HAYDEN ET AL., *supra* note 89.

220. Describing how in 2012, cybercrimes cost U.S. companies millions of dollars. JONES DAY, *supra* note 113.

221. *See* PEW RESEARCH CTR., *supra* note 104, at 10 (quoting Jeremy Epstein).

edly perform the will of the people. In promoting the public's interest, voters, politicians, and legislators are believed to be capable somehow of ignoring their own narrow concerns and promoting the greater good. But in modeling the behavior of individuals as driven by the goal of utility maximization, public choice theory transfers the rational actor model of economic theory to the realm of politics. Public choice theorists assume that individuals care about their own interests and are led mainly by those interests in the political process, just as these interests steer their other daily functions.[222] As such, voters vote for candidates that they believe will better their own lives, and politicians seek to advance their own careers or get reelected to office.[223] Thus, public and private choice processes differ, not because the motivations of actors are different, but because of stark differences in the incentives and constraints that channel the pursuit of self-interest in the two settings.[224] But public choice scholars have identified even deeper problems with democratic decision-making processes. The logic of collective action reinforces lawmaking that caters to the interests of the minority at the expense of the majority. Small groups with strong communities of interest are more successful suppliers of political pressure and political support than big groups whose interests are more dispersed.[225] After all, members of smaller groups have more individual stake in advantageous policy decisions, can organize at lower cost, and can more easily control issues that might challenge the accomplishment of their shared goals.[226] Because the vote incentive motivates politicians seeking reelection to respond to the demands of small, well-organized groups, representative democracy frequently leads to this tyranny of the minority.

The logic of collective action explains how digital service providers have leveraged their size to secure favorable government treatment and advantages such as too-

---

222. "We learn from Public Choice theory that theory for which James Buchanan won the Nobel prize in economics in 1986 that public servants act in their own interest just as much as corporate moguls do." Hon. Daniel Oliver, Chairman, Fed. Trade Comm'n, Remarks Before the U.S. Chamber of Commerce (Feb. 18, 1988), 1988 WL 1025382, at *4.

223. *See* Zachary J. Gubler, *Public Choice Theory and the Private Securities Market*, 91 N.C. L. REV. 745, 750 (2013) (noting that regulators can pursue their own interests when their actions and legislation are not scrutinized by the electorate).

224. *See, e.g.*, Melissa Waters & William J. Moore, *The Theory of Economic Regulation and Public Choice and the Determinants of Public Sector Bargaining Legislation*, 66 PUB. CHOICE 161 (1990).

225. For more on special interest groups and their power, see generally EAMON BUTLER, PUBLIC CHOICE THEORY—A PRIMER, THE INSTITUTE OF ECONOMIC AFFAIRS 34–39 (2012), https://iea.org.uk/wp-content/uploads/2016/07/IEA%20Public%20Choice%20web%20complete%2029.1.12.pdf [https://perma.cc/9ZJY-Z22N]; WILLIAM H. RIKER, THEORY OF POLITICAL COALITIONS (1962); Amitai Etzioni, *Special Interest Groups Versus Constituency Representation*, 8 RES. SOC. MOVEMENTS, CONFLICTS & CHANGE 171 (1985).

226. "Under the public choice theory, public policies with broad benefits and concentrated costs, like the Dodd-Frank Act, generally have well-organized opposition, as was the case with the Wall Street lobby. The resulting policy, then, tends to be only as strong as the minority bearing the costs is willing to pay . . . . Main Street demanded action, but the Wall Street Lobby made it nearly impossible for Congress to come to agreement on many details of the bill." Alison K. Gary, Comment, *Creating a Future Economic Crisis: Political Failure and the Loopholes of the Volcker Rule*, 90 OR. L. REV. 1339, 1366–67 (2012).

big-to-jail status. Apple, Amazon, and Google's lobbying group, Financial Innovation Now, is defined as "an alliance of technology leaders working to modernize the way consumers and businesses manage money and conduct commerce."[227] The group's goal is to promote policies that enable these innovations.[228] By trading votes in favor of protectionism for pledges of support from politicians, representatives of the technology industry ensure that these policies are approved. Many programs of this sort are also packaged in omnibus bills that policy makers support in order to pass their pet projects. And the results are apparent. Today's biggest digital service providers, in addition to operating based on a cost-benefit analysis and a risk-based approach to cybersecurity, enjoy market supremacy and governmental backing. Despite reports that Google paid Apple approximately $1 billion in 2015 to be the default search engine in its operating system, for example, federal regulators have shown no interest in pursuing the company, reinforcing the validity of public choice theory and antitrust enforcement.[229] Politically appointed FTC commissioners have declined to take any action beyond extracting settlements,[230] and the DOJ has not taken a stand; state attorneys continue to probe Google's conduct, but given the disinterest of federal regulators, Google may already be too-big-to-jail[231]—considered unstoppable by the market and hence the safest investment.

D. Should We Care About Failure?

The elevated probability of some kind of failure or disastrous malfunctioning of key digital service providers, their services, or their products as a result of cyberattacks, the risks and potential damages of such attacks to our economy and society,

---

227. *Financial Innovation Now*, *supra* note 154.

228. *Id.*; *see also* McGrath, *supra* note 152.

229. Daniel Crane, *Rethinking Merger Efficiencies*, 110 U. MICH. L. REV. 347, 379 (2011) ("Public choice literature suggests that antitrust enforcers are not merely detached public servants on a truth-seeking expedition."); Gideon Parchomovsky & Philip J. Weiser, *Beyond Fair Use*, 96 CORNELL L. REV. 91, 112 (2010) ("[P]ublic choice theory explains how and why agencies set up to regulate a certain industry or economic sector will sometimes act to advance the narrow interests of the regulated industry or sector.").

230. *See, e.g.*, Press Release, Fed. Trade Comm'n, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns in the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search (Jan. 3, 2013), http://www.ftc.gov/opa/2013/01/google.shtm [https://perma.cc/3XC8-5X7D]; Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm [https://perma.cc/F2R2-EZ7B].

231. Farhad Manjoo, *The Case Against the Case Against Google*, SLATE (July 28, 2009, 5:02 PM), http://www.slate.com/articles/technology/technology/2009/07/the_case_against_the_case_against_google.html [https://perma.cc/BT8B-P9TV] ("Ever since Barack Obama appointed her to head the DoJ's antitrust division, Varney has been promising a tough line against firms that dominate their industries."); Andrew Orlowski, *Is Alphabet-Google "Too Big To Jail"? The Lords Find Out*, REGISTER (Oct. 28, 2015, 1:03 PM), http://www.theregister.co.uk/2015/10/28/house_lords_eu_platform_enquiry [https://perma.cc/2A5Y-USNU].

and the lack of transparent, binding, and much-needed cyber-related risk internalization and management principles make Too-Big-To-Fail 2.0 a bigger problem than many may want to believe.

1. Innovation and Competition

Too-Big-To-Fail 2.0 may not appear to be a valid concern given that failure, in the way it manifests itself in the financial sector, is not necessarily a problem in the technology industry. Arguably, in the tech sector, competitors can always disrupt the industry by targeting existing services or goods and adapting them to a new digital reality using new technologies or a platform approach.[232] Moreover, history teaches us that in fast-moving industries, driven by fast-changing technologies, barriers to entry may be less significant. The nature of the business means that technology companies are vulnerable to the "next big thing," and that concept promotes entrepreneurship and innovation. For example, Airbnb, Uber, Netflix, and Tesla all rose to power by creating markets inconceivable to their predecessors. The NASDAQ landscape may be considerably different in several years, with new brands dominating different sub-industries. This was the case with Microsoft. In the 1970s, IBM held a monopoly on the hardware of computers. Deciding to outsource the development of the operating system to Microsoft, and the development of chips to Intel, both outside and small-business entities, IBM ended up ceding control of the software industry to those two new players.[233] Then, a few years down the line, a similar story happened again when Microsoft, which grew to rule the technology world, seemed unstoppable until the natural course of the market slowed it down. Indeed, for years, Microsoft's monopoly in computer software leveraged tremendous influence that challenged regulators[234] and appeared to be unparalleled. Eventually, however, creativity, innovative ideas, and corporate reinvention resulted in major market changes that curbed

---

232.

> "Technological innovation can also limit the power of distributors by creating the opportunity to support a limited interest market, thereby lessening the production and distribution expenses required to support mass appeal product and lowering barriers to entry for new production and distribution organizations. . . . New technologies also lessen the power of existing major distributors by creating additional sources of income to help offset the high risk that production and distribution expenses will not be recovered, thereby inducing new entrants into the production and distribution field."

Impact of Technological Innovation, *in* 1 ENTERTAINMENT LAW 3D: LEGAL CONCEPTS AND BUSINESS PRACTICES § 6:12, Westlaw (database updated Dec. 2016) (footnotes omitted); *see also* Ghez, *supra* note 12.

233. *See, e.g.*, DAVID I. ROSENBAUM, MARKET DOMINANCE: HOW FIRMS GAIN, HOLD, OR LOSE IT AND THE IMPACT ON ECONOMIC PERFORMANCE 139–56 (1998); Sandra Salmans, *Dominance Ended, I.B.M. Fights Back*, N.Y. TIMES (Jan. 9, 1982), http://www.nytimes.com/1982/01/09/business/dominance-ended-ibm-fights-back.html [https://perma.cc/9CTC-H3MJ].

234. *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001); Probir J. Mehta & Ryan J. Harris, Recent Decisions, United States v. Microsoft*: The Application of Antitrust Law to Technologically Dynamic Markets*, 70 GEO. WASH. L. REV. 287, 287 (2002).

Microsoft better than any regulator could.[235] Massive institutions routinely attempt to force a new economic and societal paradigm in the name of efficiency and connectedness; ultimately, however, consumers determine whether this paradigm will take hold.[236]

The too-big-to-fail-related issues, if any, that plagued digital service providers in the past were antitrust cases, such as the ones brought decades ago against IBM and Microsoft, and questioned whether they were abusing their monopolistic power in the marketplace. Some of these antitrust-related issues, as well as others, are still very relevant today in connection with the biggest tech companies. In particular, a key issue with the tech giants' monopolistic power results from the fact that they have been allowed to simply acquire and absorb any potential future competitors. And, this has been their strategy in recent decades in order to stay dominant – halting competitors before they get too big. So, for example, when Facebook purchased Instagram for about $1 billion and WhatsApp for $21.8 billion, we as a society lost the ability to have these two businesses grow to be a company that can actually compete with Facebook.[237] Similarly, when Google bought Android for $50 million, Waze for $1 billion, or YouTube for $1.65 billion to prevent them from further growing and competing with it, Google was able to remain dominant.[238] And Amazon killed much of its competition with purchases such as the Whole Foods acquisition, which was entirely aligned with Amazon's desire to deliver more aspects of its customers' daily lives. Groceries are one of the few goods that are purchased with high regularity, and Whole Foods was the gateway to this new market.[239] Likewise, in addition to acquiring the competition, the tech giants' size and business models also hurt competition and reduce innovation as they create a chilling effect on funding of small startups. Indeed, investors are aware of the tech giants' potential ability to outman, out-fund, and immediately compete with any new innovative player, and are wary of that. So, these new players have a hard time getting financial support, and we should not be surprised of the continued dominance of a very few companies like Facebook, Google, Amazon, Apple and Microsoft.

---

235. Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1666–67 (2013) (stating that some believe that "underenforcement will more likely lead to short-term harm that the market will correct as firms innovate and compete for their chance to reap the rewards of temporary dominance").

236. *See* Ghez, *supra* note 12.

237. Steven Davidoff Solomon, *Tech Giants Gobble Start-Ups in an Antitrust Blind Spot*, N.Y. TIMES (Aug. 16, 2016), https://www.nytimes.com/2016/08/17/business/dealbook/expect-little-antitrust-challenge-to-walmarts-bid-for-jet-com.html [https://perma.cc/U7QT-TGNP] ("Facebook's acquisition of WhatsApp [is] . . . another example of an upstart internet company being swallowed up to preserve the stranglehold of a giant. This happens because antitrust regulators are stuck in an outdated view of the world, while the internet giants are more attuned to their nascent competitive threats. . . . Facebook and its elite brethren will do anything to make sure they are not the next Yahoo or Radio Shack, killed by disruption and failure to innovate. This translates into paying obscene sums for technology that might challenge their dominance one day.").

238. *Id.*

239. Clark Boyd, *GAFA: What Can We Learn from Their Acquisition Strategies?*, MEDIUM (Dec. 9, 2017), https://medium.com/swlh/gafa-what-can-we-learn-from-their-acquisition-strategies-ac4523be70e5 [https://perma.cc/5L6W-X73J].

But in addition to the antitrust issues, there are other negative, economic-wide externalities caused by the technology industry, including systemic risks related to critical infrastructure. It would undoubtedly be more than inconvenient for most individuals, institutions, and businesses if Google were to disappear, and it would probably take a long time before internet infrastructure—especially services related to emails, searches, and maps—regained the same levels of usefulness and productivity. But that is not the worst that could happen. Inherent risk is involved when government agencies, businesses, and individuals move increasing amounts of computing and data to shared services. Individually, the changes to outsourced services may represent low risk. Taken together, the stored financial or government information, dependent on a few too-big-to-fail entities, could represent a tremendous risk to the overall economy.[240] This was not the case with Microsoft or IBM. It is clear why the EU subjects digital service providers—of online marketplaces, online search engines, and cloud computing services—to critical infrastructure's legal security requirements, while excluding, per the NIS Directive, "hardware manufacturers and software developers"[241] such as IBM or Microsoft.

The speed of change in computer and communications technologies and its impact on economic, social, and cultural structures make a difference as well. Past events may not offer the best guidance regarding the future,[242] as both technology and cyber threats are evolving quickly. Reliable internet, digital services, and other network and IT facilities are essential in recovering from most large-scale disasters. As a society, we must prioritize detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate.[243]

2. Financial Links and Contagion

The inextricable links between physical and cyberinfrastructures also validate Too-Big-To-Fail 2.0 as a concern. Infrastructure has become increasingly interdependent with essential services, increasing the possibility of cascading effects if a single sector is disrupted. This is especially demonstrated by the financial sector's reliance on the key digital service providers' cloud services, as well as other services. Understanding and mitigating these risks is key to our national security, resilience, and economic prosperity.

Indeed, businesses across different industries today are so interconnected and interdependent that hackers attack the advanced cybersecurity systems of bigger businesses by turning to smaller companies without vigorous protection.[244] These smaller businesses may be contractors for larger entities or third- party vendors, may be directly responsible for critical infrastructure, or may hold data that could be valuable

---

240. *See* Treese, *supra* note 109.

241. *See* JONES DAY, THE NEW EU CYBERSECURITY DIRECTIVE: WHAT IMPACT ON DIGITAL SERVICE PROVIDERS? (2016) (internal quotation marks omitted).

242. PETER SOMMER & IAN BROWN, REDUCING SYSTEMIC CYBERSECURITY RISK 5 (2011), https://www.oecd.org/gov/risk/46889922.pdf [https://perma.cc/EB88-F5ER].

243. *Id.*

244. *Introduction to Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity [https://perma.cc/HD3G-JJUF].

to hackers. For example, the hack into the Office of Personnel Management (OPM) was the result of IT system access through a third party.[245]

Additionally, and unrelatedly, in recent years, the key digital service providers have started to situate themselves as instrumental financial service providers, offering more and more consumers, especially millennials and underbanked and unbanked populations, access to financial services. These services have included credit and creditworthiness evaluations, loans, payment transfers, cash alternatives, and even money accounts of different sorts. Some, including Facebook, for example, have even gone as far as acquiring regulatory banking licenses.[246]

V. REGULATORY MEASURES AND POTENTIAL RESPONSES

The increasing sophistication and scope of data breaches in general have caused federal and state regulators to pay closer attention to cybersecurity. In the United States, several federal agencies have started issuing guidelines for avoiding these dangers. A notable example is the Securities and Exchange Commission (SEC), which in 2014 hosted a Cybersecurity Roundtable where it emphasized the significance of cybersecurity to the integrity of the market system and customer-data protection.[247] A month later, the SEC began its cybersecurity initiative, stressing its objectives: to gain a better understanding of the cybersecurity risks in the securities industry and to help firms prepare for and respond to these risks. Similarly, the Office of Compliance Inspections and Examinations (OCIE) published a Risk Alert with a series of assessments to identify cybersecurity risks[248] and measure cybersecurity preparedness in the securities industry. In 2015, the OCIE published summary observations of the results.[249] Because of the extreme and constantly growing importance of cybersecurity and the affirmative response from broker-dealers and advisers to OCIE's efforts, the OCIE announced a focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities.[250]

---

245. *See* Laughlin, *supra* note 88, at 361.

246. *See generally* Packin & Lev-Aretz, *supra* note 15; Steve O'Hear, *Facebook Just Secured an E-money License in Ireland, Paving the Way for Messenger Payments in Europe* TECHCRUNCH (Dec. 7, 2016), https://techcrunch.com/2016/12/07/facebook-just-secured-an-e-money-license-in-ireland-paving-way-for-messenger-payments-in-europe [https://perma.cc/E4F3-TBP9].

247. *Cybersecurity Roundtable*, U.S. SEC. & EXCH. COMM'N (Mar. 26, 2014), https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml [https://perma.cc/SC9V-WGMV].

248. 4 OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, OCIE CYBERSECURITY INITIATIVE (2014), https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf [https://perma.cc/J24K-SSGM].

249. 4 OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, CYBERSECURITY EXAMINATION SWEEP SUMMARY (2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf [https://perma.cc/W2YF-8M5V].

250. 4 OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE (2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf [https://perma.cc/FBB3-H292].

Similarly, as discussed above, President Obama issued presidential policy directives and signed executive orders tackling this issue—admittedly following discussions in recent years of the government's involvement in preventing cybersecurity attacks, and its responsibility for fixing the damage they cause. Additionally, lawmakers have tried, not always successfully, to advance the issues of cybersecurity, regularly introducing information-sharing bills in both the Senate and the House; in October 2015, the Senate passed the Cybersecurity Information Sharing Act,[251] attempting to encourage the flow of cyber threat data between the private sector and the government.[252]

These regulatory attempts are not surprising. Changes must be made to the existing fundamental regulatory framework to ensure that undesired risks relevant to key digital service providers are monitored, minimized, and mitigated. In the financial sector, the Dodd-Frank Act attempted to make SIFIs safer and solve the too-big-to-fail problem.[253] Nevertheless, several years after its enactment, it seems that it has failed, allowing the government to give financial support, which might be similar to bailouts, framed in a general fashion.[254] Also, as noted earlier, entities beyond SIFIs can cause a too-big-to-fail impact.[255]

In the case of Too-Big-To-Fail 2.0 resulting in a national emergency, different forms of government intervention are possible. For example, in Netflix's third season of *House of Cards*, President Underwood (played by Kevin Spacey) invoked the (real) Stafford Act[256] to declare unemployment a disastrous national emergency and use funds from the Federal Emergency Management Agency (FEMA) for his job-creation program—a (fictional) stretch, to be sure, but one that might inform responses to cybersecurity-related catastrophes.

One thing is clear, however: all legal responses must be carefully designed. After all, even initiatives such as the EU's NIS Directive, meant to institute the first set of baseline cybersecurity requirements for Critical Service Providers, are likely to have unintended consequences. The Directive's impact, for example, is likely to go less noticed in the near future: member states have twenty-one months to transpose the Directive's new rules into their national laws and six more to identify operators of essential services by each member state. At that point, each member state crafts an interpretation of the legislation to be incorporated into its laws. Just as the Dodd-Frank Act's SIFI designation was interpreted as governmental approval of SIFIs as too big to fail, entities that the EU would identify as critical digital service providers might *de facto* be seen as too big to fail. This market perception could then lead to the creation of all sorts of undesired and unethical incentives.

---

251. S. 754, 114th Cong. (2015).

252. *See* Kimberly Peretti & Lou Dennig, *What In-House Counsel Should Know About Cybersecurity Information Sharing*, CORP. COUNSEL (July 7, 2016), http://www.corpcounsel.com/id=1202761997713/What-InHouse-Counsel-Should-Know-About-Cybersecurity-Information-Sharing?mcode=0&curindex=0&curpage=ALL [https://perma.cc/E5HE-7CBW].

253. *See generally* Packin, *supra* note 9.

254. *Id.*

255. *See, e.g.*, Azgad-Tromer, *supra* note 42.

256. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707, 102 Stat. 4689 (codified as amended at 42 U.S.C. §§ 5121–5208 (2012)).

CONCLUSION

From the standpoint of domination and power, a central problem in today's political economy is what Brandeis famously called the "curse of bigness"[257]—in particular, the concentrated private power of digital service providers in the information economy. Currently, key digital service providers increasingly control the terms of access and distribution for major cyber-social systems and services.[258] This power, in combination with cybersecurity threats to which such entities are exposed, and the potential consequences, is worrisome.

In the past several years, public discussions of too-big-to-fail have asked the following questions: If a specific entity fails, would the effects of the failure on our technological, economic, and social lives be so dire that the government would be required to get involved? What consequences would there be for the ecosystem of customers, service providers, competitors, employees, and others parties partaking in the marketplace? The goal is to prevent a situation where there is a risk of damage to the larger system from the breakdown of one participant in the system.

Traditionally, the technology industry has not faced this issue, as the assumption has been that technology companies come and go, acquiring others or being acquired, their clients transitioning as needed.[259] Damages resulting from failures of one company's products or services, which could impact the entire company's stability and business, have yet to produce ripple effects, and the impact on the overall system has been limited. This Article argues, however, that this may no longer be the case, considering the key digital service providers' size, power, and importance; horizontal and vertical integration; overall impact on our technological, economic, and cyber-social systems; and the damaging potential of cyberattacks. Indeed, when taking advantage of Microsoft's software vulnerabilities in May 2017, attackers were able to disrupt operations in more than 150 countries, lock up more than 200,000 computers, and cause damage that was estimated in the billions of dollars[260]—and much worse attacks exposing the big digital service providers' vulnerabilities still await.

Arguing that the too-big-to-fail concept may be relevant to key, albeit nonfinancial, digital service providers, given the massive externalities on the general public that their failure would impose, this Article seeks to draw attention to the entities that might constitute Critical Service Providers. It also calls for the private sector and scholars to help regulators advance initiatives to address this problem, create guidelines as to how to better manage the risk at such entities, and determine the best measures to increase the stability and safety of the relevant entities, as well as the overall economy. But in order for such a systemic approach to take place, the consequences for designating entities as Critical Service Providers should also be clearly

---

257. Louis D. Brandeis, *A Curse of Bigness*, HARPER'S WKLY., Jan. 10, 1914, at 18, 18.

258. *See* K. Sabeel Rahman, *Domination, Democracy, and Constitutional Political Economy in the New Gilded Age: Towards a Fourth Wave of Legal Realism?*, 94 TEX. L. REV. 1329, 1345 (2016) (describing how some of these firms are monopolies in the conventional sense, while others exhibit a different form of "platform power," centralizing control over key conduits of economic activity such as Amazon's control of its logistics and marketplace).

259. Treese, *supra* note 109.

260. *See* Volz & Auchard, *supra* note 1.

defined and include further scrutiny and regulation conducted by some type of a supervisory body, which should be the product of a collaborative private-public initiative.

The private sector must be involved in designing this systemic approach for several reasons. First, in the United States, the private sector controls most of the critical infrastructure, although the government has a national security interest in safeguarding those assets. And there is a gap between the public sector's desire to safeguard the critical infrastructure from low-probability catastrophe and the private sector's desire to spend a lot of money to minimize the likelihood of it happening, without utilizing a cost-effective, risk-based approach to defend against threats. In order to guarantee that the private sector properly manages risks against all cyber threats, the input of lawmakers and experts in such initiatives is key, despite the private sector's persuasive argument against overregulation.[261] Second, the challenge lies in fostering the right set of economic, political, and societal checks and balances that could curb key digital service providers' influence while not overregulating them. In the aftermath of the 2008 financial crisis, a wide range of financial-technology companies have emerged to offer alternative services and investments to consumers demanding more transparency, with the blessing of regulators. The same consumer-driven revolution in the technology industry would severely undermine AFAMA's ability to rule the sector, as many worry they are aiming to do,[262] without overburdening them. Third, although the Dodd-Frank Act's living wills are mainly a costly disclosure requirement that is difficult to effectively implement[263] rather than a substantive regulatory solution that solves the too-big-to-fail problem, the living wills do add some value by requiring entities to enhance their risk management and plan better for the unknown,[264] including in connection with cybersecurity, as advocated recently by former Pentagon cybersecurity expert, Dr. Michael Sulmeyer.[265] Finally, and most

---

261. *See* Laughlin, *supra* note 88, at 359–60.

262. *See* Ghez, *supra* note 12.

263. *See* DAVID SKEEL, THE NEW FINANCIAL DEAL: UNDERSTANDING THE DODD-FRANK ACT AND ITS (UNINTENDED) CONSEQUENCES 185 (2010).

264. Daniel Bryant, *Too Big To Fail: Lessons Learnt from Google and HealthCare.gov*, INFOQ (June 14, 2015), https://www.infoq.com/news/2015/06/too-big-to-fail [https://perma.cc/V9XT-8LF5] (reporting that Nori Heikkinen, an engineer at Google, discussed SARs, and shared "stories of failures and lessons learnt . . . at Google" that demonstrated that "preparedness is an important element of handling failure," explaining that "[m]odelling ahead of time is essential").

265. Discussing the process of prioritizing and organizing the business lines and data and then working out a business strategy to match it, a process that resembles the living will plans, Dr. Michael Sulmeyer, who left the Pentagon and heads up the cybersecurity project at the Harvard Kennedy School's Belfer Center recently stated that

> the thing that companies and law firms need to be thinking about is, what is the most important data that needs to be protected? That's where this analysis has to begin for almost everyone . . . . Once a company or a firm is able to get greater clarity on its own priorities, then you can think about how to better defend it. But I think any company that tries to say "I just want more cybersecurity" or "I just want to buy more defenses," that's not a smart strategy to pursue.

Dr. Sulmeyer argued that "[w]ith a list of priorities . . . comes the ability to strategize, be it through internal safeguards, contracting out security, and coming up with contingency plans

importantly, across the technology sector, companies are already racing to provide stronger cybersecurity protection for customers, including from nation-states, but they cannot successfully do so on their own, especially as governments are increasing their investments in offensive cyber capabilities. Therefore, it must be recognized that this is not a problem that the public sector or the private sector can solve acting alone.[266]

Pushing for this type of a collaboration between the private and the public sectors was also a presidential cybersecurity commission's preferred course of action, as indicated in the commission's report. Action Item 1.1.1 begins: "The President should direct senior federal executives to launch a private-public initiative, including provisions to [enable] agile, coordinated responses and mitigation of attacks on the users and the nation's network infrastructure."[267] The report repeatedly emphasizes the need for collaborative public-private partnership, rather than plain rulemaking.[268]

If the process of planning is well conceived,[269] risk management can give entities a competitive advantage, become a profit center,[270] and help focus efforts on areas where business strategies fall short of best practice,[271] while preventing a Too-Big-To-Fail 2.0 situation.

---

in the event of a breach." Bryan Koenig, *Trump Faces Tough Challenges in Bolstering Cybersecurity*, LAW360 (Feb. 6, 2017), https://www.law360.com/aerospace/articles/885597?utm_source=rss&utm_medium=rss&utm_campaign=section [https://perma.cc/6GXE-KL38].

266. *See* Smith*, supra* note 103. This argument was also made in connection with the May 2017 cyberattack on Microsoft's software. Thomas Fox-Brewster, *Microsoft Just Took a Swipe at NSA over the WannaCry Ransomware Nightmare*, FORBES (May 14, 2017, 5:14 PM), https://www.forbes.com/sites/thomasbrewster/2017/05/14/microsoft-just-took-a-swipe-at-nsa-over-wannacry-ransomware-nightmare/#425281f43585 [https://perma.cc/NMK5-MPFK].

267. COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY 14 (2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf [https://perma.cc/M5QW-4D4A].

268. *Id.* For a discussion on the public-private cybersecurity system and how it stands with public law values, see Kristen Eichensehr*, Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017).

269. *See* Thomas F. Huertas, Dir. of Banking Sector, U.K. Fin. Servs. Auth., Speech at the Wharton School of the University of Pennsylvania: Living Wills: How Can the Concept Be Implemented? (Feb. 12, 2010), http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2010/0212_Th.Shtml https://perma.cc/DF89-PDYR].

270. *See* James Fanto, *Anticipating the Unthinkable: The Adequacy of Risk Management in Finance and Environmental Studies*, 44 WAKE FOREST L. REV. 731, 735–36 (2009).

271. Daniel K. Tarullo, Speech at the Institute of International Bankers Conference on Cross-Border Insolvency Issues: Supervising and Resolving Large Financial Institutions (Nov. 10, 2009), http://www.federalreserve.gov/newsevents/speech/tarullo20091110a.htm [https://perma.cc/Y4GH-SD3A].